Connecting. The. Dots.

The Behavioral Threat Assessment Unit's

College & University

School Resource Guidebook

Connecting. The. Dots.

Connecting. The. Dots.

The Behavioral Threat Assessment Unit

College & University

School Resource Guidebook

Compiled by J. M. Marks

NC State Bureau of Investigation

April 2019

Table of Contents

Table of Contents

What is the North Carolina Behavioral Threat Assessment Unit?

The North Carolina Behavioral Threat Assessment (BeTA) Unit was developed by the North Carolina State Bureau of Investigation in 2018 to take a **proactive** approach to **prevent violence** in our communities.

Staffed by law enforcement officers, intelligence analysts and mental health professionals, the primary objective of a BeTA Unit investigation is to gather and evaluate information about persons who exhibit concerning behaviors associated with the pathway to violence. Behavioral Threat Assessment (BeTA) Unit investigations receive high priority and begin immediately upon receipt of information of any threat or unusual behavior directed toward an individual associated with an educational property, place of worship, or other mass gathering of the public.

PURPOSE

Between 2016 and 2017, there have been 50 shootings characterized by the FBI as active shooter incidents. These 50 incidents resulted in 943 casualties (Active Shooter Incidents in the United States in 2016 and 2017, the Advanced Law Enforcement Rapid Response Training (ALERRT) Center at Texas State University and the Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC 2018). After the February 14, 2018 attack at the Marjory Stoneman Douglas High School in Parkland, Florida, the SBI, in consultation with the University of North Carolina System, decided that the traditional reactive approach of law enforcement to attacks is not sufficient to address this issue. Partnering with University Police, and state and federal law enforcement agencies, the SBI formed the Behavioral Threat Assessment (BeTA) Unit to take a proactive approach focusing on threat assessment and management to address threats of mass violence.

The BeTA Unit is a statewide threat assessment and management program meant to follow persons of concern throughout the State and to ensure information about persons of concern is shared with other states should the person of concern move outside of North Carolina.

PREVENTION IS POSSIBLE

Findings of the Safe School Initiative conducted by the U.S. Secret Service and the U.S. Department of Education suggest that some future attacks may be preventable. "The fact that most attackers engaged in pre-incident planning behavior and shared their intentions and plans with others, suggests that those conducting threat assessment inquiries or investigations could uncover these types of information." (Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates, Washington, DC, May 2002, p. 30). The primary purpose of threat assessment is the prevention of targeted violence. The threat assessment and management process involves the proactive work of a trained multi-disciplinary threat management team charged with the responsibility to seek out and thwart potential attackers before they strike. As such, threat management is integral to the work of the BeTA Unit. Threat assessment is the process of gathering and assessing information about persons who may have the interest, motive, intention, and capability of mounting attacks against identified targets. The BeTA Unit uses this methodology but also incorporates key investigative principles and relies on relationships with other entities to gather information critical to informing the threat assessment process and formulating viable mitigation plans. Threat assessment is one component in the overall strategy to reduce violence.

THIS RESOURCE GUIDE

The Behavioral Threat Assessment (BeTA) Unit has compiled this resource guide to support Colleges and Universities in North Carolina that might be new to behavioral threat assessments, and/or are looking to implement threat assessment teams in their school district. In the pages to follow, you will find literature from nationwide leading experts in behavioral threat assessments, landmark studies and publications that have shaped the world of behavioral threat assessment, current best practices, legal considerations and some additional resources to explore. While this guide is certainly not an all-encompassing or all-answering publication, we hope it serves as a strong sounding board for educating you, your college or university, your institution administrators and policy makers on the importance of implementing school-based threat assessment teams.

The BeTA Unit is not intended to replace or duplicate the threat assessment duties of school threat assessment teams, other state and local law enforcement agencies, the Federal Bureau of Investigation Behavioral Analysis Unit, the United States Secret Service Protective Intelligence Division, or any other threat assessment group or agency.

Targeted Violence

"The **conscious decision** to kill or physically harm **specific or symbolic** victims in a workplace or on a campus is now categorized as targeted or intended violence. In contrast to affective or impulsive violence, targeted violence is by definition **planned**, emotionless, and predatory." *WAVR-21*

"Targeted violence" is defined as an incident of violence where a known or knowable attacker selects a particular target prior to their violent attack.

Perpetrators don't "snap" …they *decide*

Pathway to Workplace and Campus Targeted or Intended Violence
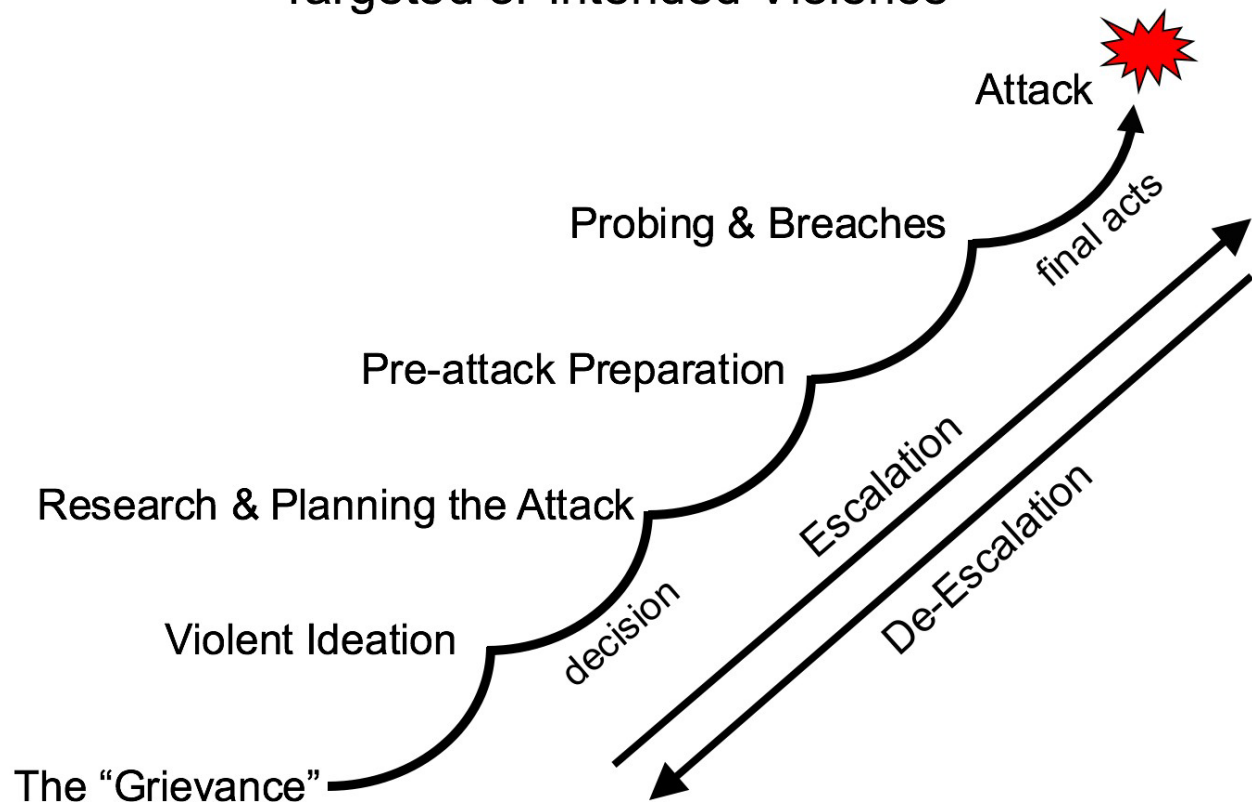
Attack

Probing & Breaches

final acts

Pre-attack Preparation

Escalation

Research & Planning the Attack

decision

De-Escalation

Violent Ideation

The "Grievance"

A Study of Pre-Attack Behaviors of Active Shooters in the United States Between 2000 and 2013; USDOJ, FBI, Published July 2018: 77% spent a week or longer **planning***; 46% spent a week or longer actually* **preparing***; In 64% of cases, at least one of the victims was* **specifically targeted**

A Study of Pre-Attack Behaviors of Active Shooters in the United States Between 2000 and 2013; USDOJ, FBI, Published July 2018

U.S. Department of Justice
Federal Bureau of Investigation
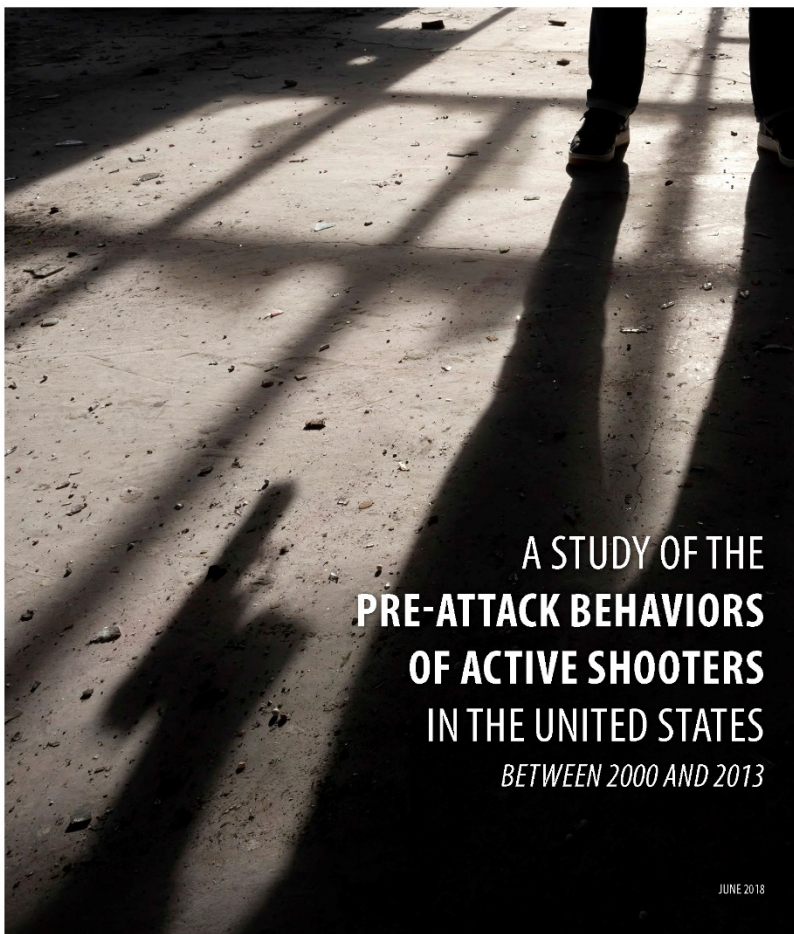
A STUDY OF THE
PRE-ATTACK BEHAVIORS OF ACTIVE SHOOTERS
IN THE UNITED STATES
BETWEEN 2000 AND 2013

JUNE 2018

- 56% had a first instance of concerning behavior **25 months or more before the incident**

- On average, each shooter displayed **4 to 5 observable concerning behaviors** over time

Behavioral Threat Assessment

Identifies individuals who
pose a threat of targeted violence
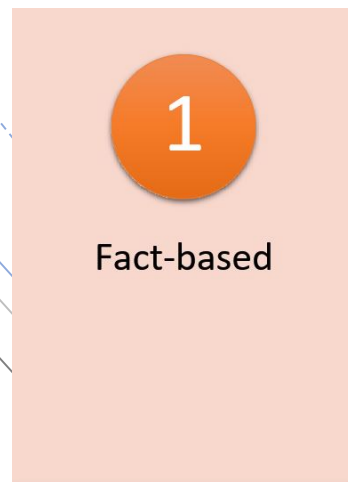
Mitigate/manage those individuals
before they strike

PREVENTION vs. RESPONSE

PROACTIVE vs. REACTIVE

1 Fact-based

2 Behaviorally driven

3 Pathway to violence model

4 Only one part of **comprehensive law enforcement approach**

Recognizing and Supporting Students of Concern

Who Could Be a Student of Concern?

A student who is exhibiting the following behaviors of concern which are impacting their well-being and/or the well-being of others.

- ► Decline in school performance
- ► Increased absenteeism/tardiness
- ► Withdrawal from friends/social activities
- ► Sudden change in behavior or appearance
- ► Drug or alcohol use
- ► Bullying/harassing others
- ► Threatening or engaging in violence
- ► Bringing weapons to school
- ► Discloses thoughts of violence to others through writing, art, online activities or statements to others

NC SBI's Behavioral Threat Assessment (BeTA) Unit

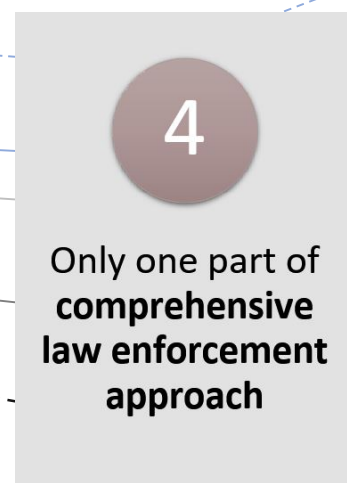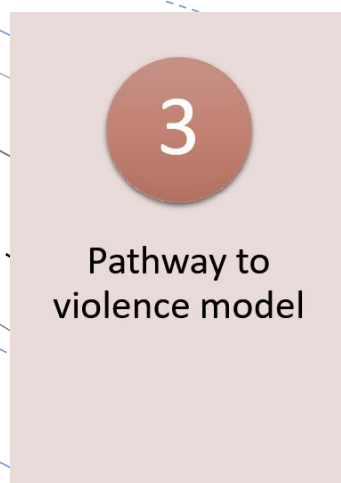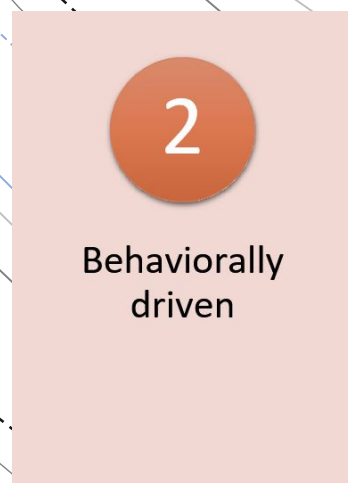- ► Developed by the North Carolina State Bureau of Investigation (SBI) to take a proactive approach to prevent violence in our communities
- ► Staffed by law enforcement officers, intelligence analysts and mental health professionals
- ► Mission is to identify, investigate, evaluate and manage person(s) of concern within North Carolina who are recognized as having motive and means to develop, or act on an opportunity to commit a targeted attack
- ► Compliments work being done by your school threat assessment team
- ► Assessment will provide recommendations for reducing a student's risk factors for committing a violent act
- ► Goal is to enable the student to remain positively engaged in the learning environment

Privacy Concerns

The **Family Education Rights and Privacy Act (FERPA)** permits communication about a student of concern in connection with a health and safety emergency. Observations of a student's conduct or statements made by a student are not FERPA protected. Such information should be shared with appropriate consideration for student privacy. **If you feel there is an imminent risk of danger, please call 911 or your local law enforcement agency. To make a BeTA Unit referral, contact 1-888-624-7222 or ncbeta@ncsbi.gov.**

THE NATIONAL THREAT ASSESSMENT CENTER (NTAC) 2018 REPORT ON MASS ATTACKS IN PUBLIC SPACES:

SCHOOLS ARE THE THIRD MOST COMMON TARGET

BEHAVIORAL THREAT ASSESSMENT UNIT

BETA UNIT

SBI

NORTH CAROLINA

STATE BUREAU OF INVESTIGATION

United States Secret Service
NATIONAL THREAT ASSESSMENT CENTER

MASS ATTACKS IN PUBLIC SPACES – 2018

U.S. Department of Homeland Security

This report was prepared by the staff of the
U.S. Secret Service National Threat Assessment Center (NTAC)

Lina Alathari, Ph.D.
Chief

Ashley Blair, M.A.
Social Science Research Specialist

Arna Carlock, Ph.D.
Social Science Research Specialist

Steven Driscoll, M.Ed.
Lead Social Science Research Specialist

Diana Drysdale, M.A.
Supervisory Social Science Research Specialist

Jeffrey McGarry, M.A.
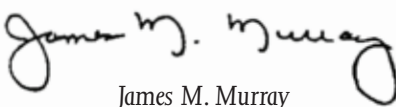Social Science Research Specialist

MESSAGE FROM THE DIRECTOR

In response to the acts of targeted violence occurring in this Nation, the U.S. Secret Service National Threat Assessment Center (NTAC) has published this research report titled, **Mass Attacks in Public Spaces – 2018**. The study was conducted for the specific purpose of identifying key information that will enhance efforts to prevent these types of attacks. The report is NTAC's second analysis of mass attacks carried out in public spaces, building upon the findings identified in its 2017 report.

These acts have impacted the safety and security of the places where we work, learn, dine, and conduct our daily activities. Each new tragedy, including the attack on a bank in Sebring, FL; a synagogue in Poway, CA; a university in Charlotte, NC; and the municipal center in Virginia Beach, VA; serves as a reminder that we must continue to research and provide robust training and awareness to help prevent these tragic outcomes.

NTAC's research and publications directly support our agency's protective mission, as well as the missions of those responsible for keeping our communities safe. Through this report, NTAC aims to assist law enforcement, schools, public agencies, private organizations, and others in understanding the motives, behavioral indicators, and situational factors of those who carry out mass attacks.

Empowering public safety professionals to combat this ever-evolving threat is a priority for our agency. I commend our community partners for their continued efforts, commitment, and determination to prevent targeted violence within the Homeland.

James M. Murray
Director

The U.S. Secret Service's National Threat Assessment Center (NTAC) was created in 1998 to provide guidance on threat assessment both within the U.S. Secret Service and to others with criminal justice and public safety responsibilities. Through the Presidential Threat Protection Act of 2000, Congress formally authorized NTAC to conduct research on threat assessment and various types of targeted violence; provide training on threat assessment and targeted violence; facilitate information-sharing among agencies with protective and/or public safety responsibilities; provide case consultation on individual threat assessment investigations and for agencies building threat assessment units; and, develop programs to promote the standardization of federal, state, and local threat assessment processes and investigations.

United States Secret Service
NATIONAL THREAT ASSESSMENT CENTER

INTRODUCTION

On May 31, 2019, 12 innocent people were killed at the Virginia Beach Municipal Center in Virginia Beach, VA by an attacker who had reportedly resigned from his position at the municipal center earlier that day. While little else is yet known publicly about the attacker or his motive, this act of mass violence is the most recent example of targeted violence affecting a public space in the United States. Mitigating the risk of mass casualties from such an event requires the efforts of everyone with a role in public safety, a responsibility that is not limited to law enforcement. Other community stakeholders may also be in a position to intervene, including workplace managers, school administrators, local officials, and the mental health community, each of whom has a unique role to play in keeping communities safe.

To support these prevention efforts, the Secret Service National Threat Assessment Center (NTAC) is tasked with delivering research, training, consultation, and information sharing on threat assessment and the prevention of targeted violence, including targeted attacks directed at workplaces, houses of worship, schools, and other public spaces. The research and information produced by NTAC guides not only the Secret Service's approach to preventing assassinations, called **threat assessment**, but also informs the communitywide approach needed to prevent incidents of targeted violence.[1]

This report is NTAC's second analysis of mass attacks that were carried out in public spaces, and it builds upon *Mass Attacks in Public Spaces – 2017* (MAPS-2017). In MAPS-2017, NTAC found that attackers from that year were most frequently motivated by grievances related to their workplace or a domestic issue. All of the attackers had recently experienced at least one significant stressor, and most had experienced financial instability. Over three-quarters of the attackers had made threatening or concerning communications, and a similar number had elicited concern from others. Further, most had histories of criminal charges, mental health symptoms, and/or illicit substance use or abuse.

With this latest report, *Mass Attacks in Public Spaces – 2018* (MAPS-2018), the Secret Service offers further analysis and operational considerations to our partners in public safety.[2] Between January and December 2018, 27 incidents of mass attacks – in which three or more persons were harmed – were carried out in public spaces within the United States.[3] In total, 91 people were killed and 107 more were injured in locations where people should feel safe, including workplaces, schools, and other public areas.[4] The loss of life and traumatic nature of these attacks had a devastating impact on the victims and their families, local communities, and the entire nation.

> ### What is Threat Assessment?
>
> In the 1990s, the U.S. Secret Service pioneered the field of threat assessment by conducting research on the targeting of public officials and public figures. The agency's Threat Assessment Model offered law enforcement and others with public safety responsibilities a systematic investigative approach to identify individuals who exhibit threatening or concerning behavior, gather information to assess whether they pose a risk of harm, and identify the appropriate interventions, resources, and supports to manage that risk.

Regardless of whether these attacks were acts of workplace violence, domestic violence, school-based violence, or inspired by an ideology, similar themes were observed in the behaviors and circumstances of the perpetrators,[5] including:

- Most of the attackers utilized *firearms*, and half *departed the site on their own* or *committed suicide*.
- Half were motivated by a *grievance* related to a domestic situation, workplace, or other personal issue.
- Two-thirds had histories of *mental health symptoms,* including *depressive, suicidal, and psychotic symptoms*.
- Nearly all had at least one *significant stressor* within the last five years, and over half had indications of *financial instability* in that timeframe.
- Nearly all made *threatening or concerning communications* and more than three-quarters *elicited concern* from others prior to carrying out their attacks.

The violence described in this report is not the result of a single cause or motive. The findings emphasize, however, that we can identify warning signs prior to an act of violence. While not every act of violence will be prevented, this report indicates that targeted violence may be *preventable*, if appropriate systems are in place to identify concerning behaviors, gather information to assess the risk of violence, and utilize community resources to mitigate the risk.

THE INCIDENTS

THE WEAPONS: Though most of the attacks were carried out using a firearm ($n = 24$, 89%), three attackers used vehicles to cause harm (11%).[6] Of the 24 who used firearms, at least 10 possessed their weapon illegally at the time of the incident. Two of those ten were minors. The remaining eight had felony convictions, were the subjects of protective orders, or had some other factor present that would have prohibited them from purchasing or possessing a firearm based on federal or state laws.[7]

THE PUBLIC SITES: The 27 incidents were carried out in 18 states, at 28 different sites, with most ($n = 20$, 70%) occurring at places of business (see Figure 1). Those that took place in open spaces ($n = 4$) represented 14% and included such locations as a public sidewalk, street, and parking lot. Three attacks (11%) were carried out at high schools. One attack (4%) took place in a house of worship.

Figure 1.

Sites of the Attacks

Places of Business — 2018: 20, 2017: 13
Open Spaces — 2018: 4, 2017: 9
Schools — 2018: 3, 2017: 4
Transportation — 2018: 0, 2017: 3
Houses of Worship — 2018: 1, 2017: 2

Legend: ■ 2018 ■ 2017
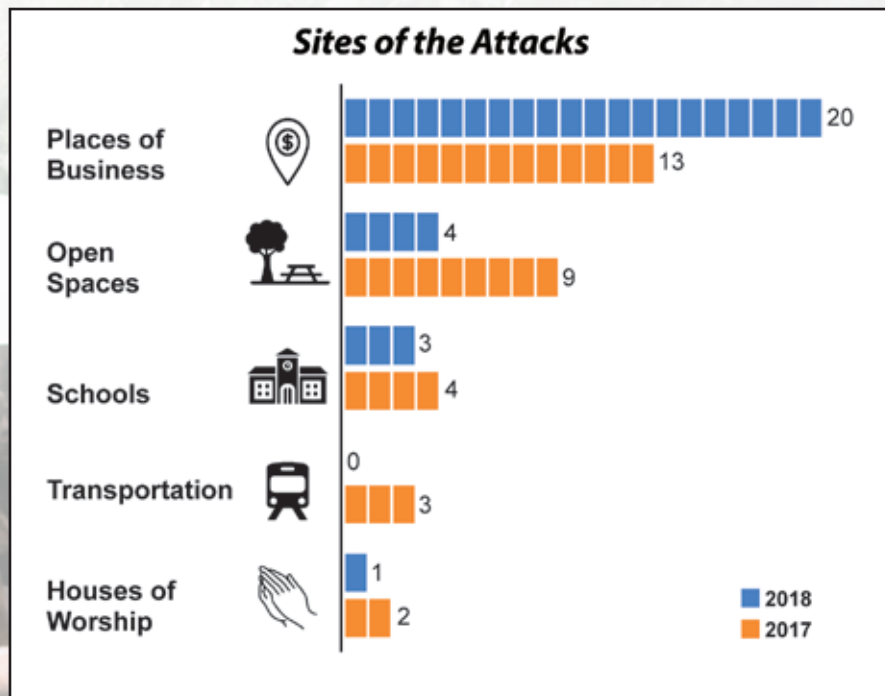
Places of Business Affected

Bars / Restaurants	Bank
Office Buildings	Municipal Center
Warehouses	Yoga Studio
Treatment Facility	Hospital
Health Center	

THE TIMING: The attacks took place in every month except December and occurred on every day of the week (see Figure 2). Over half ($n = 16$, 59%) took place between the hours of 7:00 a.m. and 3:00 p.m. More than half ($n = 17$, 63%) of the attacks ended within 5 minutes from when the incident was initiated (see Figure 3).

END OF THE ATTACKS: The most common ways the attacks ended were either by the attacker committing suicide at the scene ($n = 7$, 26%) or departing on their own ($n = 7$, 26%). Three of those who departed the scene on their own committed suicide soon after. Law enforcement intervention at the site brought six attacks to an end (22%). In four of these incidents, the attacker was killed. Other attacks ended when the weapon used became inoperable ($n = 4$, 15%) or due to bystander intervention ($n = 2$, 7%).

Figure 2.

Day of the Week				
Mon	Tues	Wed	Thurs	Fri
3	2	7	6	4

	Sat	Sun	
	1	4	

Figure 3.

Duration of the Attacks

Less than 5 min. 63%

5-14 min. 22%

15 min. or more 15%
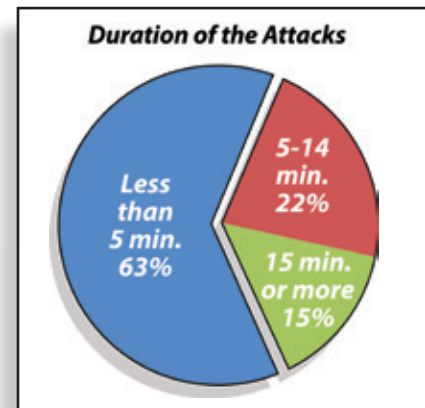
Attacks Perpetrated By Current Employees

On September 12, 2018, an employee shot and killed his ex-wife and two co-workers near his workplace. Though divorced that April, the ex-wife had recently filed for additional support. The attacker fled the scene and later committed suicide when confronted by police.

On September 19, 2018, an employee opened fire inside his employer's offices, injuring four before being fatally shot by police. The attacker's targets appeared to be random, and his motive is unknown.

On September 20, 2018, a temporary employee opened fire at a distribution center, killing three people and injuring three others before committing suicide. The attacker's motive may have been related to a grievance with co-workers.

On November 12, 2018, an employee shot and injured three individuals at a food distribution warehouse. After fleeing the scene, the attacker called police and reported that his actions were motivated by mental illness. He later committed suicide.

THE ATTACKERS

GENDER AND AGE: While most of the attackers were male (*n* = 25, 93%), there was one female and one individual in the process of gender reassignment. Their ages ranged from 15 to 64, and the average age was 37 (see Figure 4).

YOUNGEST: On January 23, 2018, a 15-year-old sophomore began shooting students randomly in a common area at his high school, killing two and injuring ten. When the attacker ran out of bullets, he abandoned his gun and joined other students who had been hiding. After the students were moved to another room, police identified the attacker and arrested him. The student had planned the attack for about a week, and he did not target any particular students, describing his attack as "an experiment."

OLDEST: On March 7, 2018, a 64-year-old male walked into a local cafe and asked to see the owner, with whom he had a disagreement weeks prior. When the owner appeared, the attacker shot him several times with a rifle, killing him. He then proceeded to shoot cafe patrons, injuring two and killing one. After the attacker ran out of bullets, he fled to his nearby home and barricaded himself inside. He eventually surrendered to police.

Figure 4.

Ages of the Attackers

	2018	2017
15-24	5	5
25-34	9	6
35-44	6	8
45-54	2	7
55+	5	2

SUBSTANCE USE: Nearly one quarter of the attackers (*n* = 6, 22%) were found to have a history of illicit drug use and/or substance abuse.

CRIMINAL CHARGES AND DOMESTIC VIOLENCE: Approximately half of the attackers (*n* = 13, 48%) had histories of criminal charges beyond minor traffic violations. Those charges included both non-violent (*n* = 10, 37%) and violent (*n* = 6, 22%) offenses.

Looking specifically at the issue of domestic violence, eight attackers (30%) were found to have had such histories, with only some of those instances resulting in criminal charges or arrests.[8]

On September 19, 2018, a man shot and injured his wife, two bystanders, and a police officer in a municipal building. At the time of the attack, he was subject to a protective order resulting from incidents in which he assaulted and threatened to kill his wife because she wanted a divorce. About a month prior to his attack, he was arrested after he threatened to kill his wife and choked her with a belt. A judge agreed to issue a protective order; however, he denied the wife's request that her husband be ordered to relinquish his firearms.
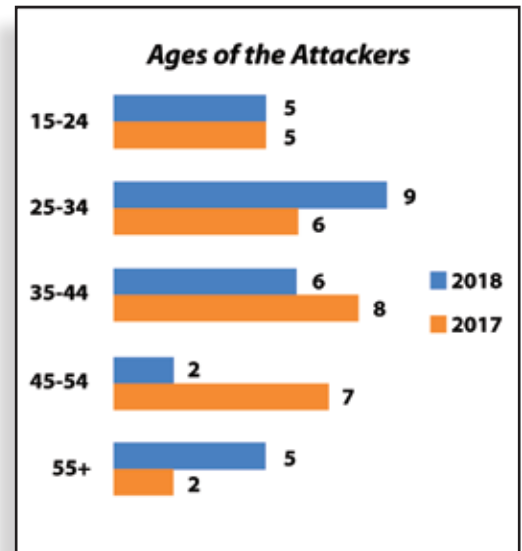
MENTAL HEALTH: Two-thirds of the attackers (n = 18, 67%) experienced mental health symptoms prior to their attacks. The most common symptoms observed were related to depression and psychotic symptoms, such as paranoia, hallucinations, or delusions. Suicidal thoughts were also observed (see Table 1). Nearly half of the attackers (n = 12, 44%) had been diagnosed with, or treated for, a mental illness prior to their attacks.

On May 24, 2018, a man opened fire on the patrons of a restaurant, injuring one adult and two children. His motive for the attack is not known, but he was demonstrating symptoms of a mental illness, including suicidal thoughts and paranoid delusions about being taunted by demons and watched by a drone. In videos posted online shortly before the attack, the man said that everyone was against him and he felt tortured and alone. He said, "My life is in danger…Satan is after me."

Table 1.

Mental Health Symptoms	2017	2018
	n	*n*
Depression	4	10
Psychotic Symptoms	9	10
Paranoia	6	9
Delusions	2	5
Hallucinations	6	1
Suicidal Thoughts	6	8

MOTIVES, BELIEFS, & TARGETING

MOTIVES: The violence in this study resulted from a range of motives, with some attackers having multiple motives. In half of the incidents (*n* = 14, 52%), grievances appeared to be the main motivating factor. In these cases, the attackers were retaliating for perceived wrongs related to their domestic situations (*n* = 6, 22%), workplaces (*n* = 3, 11%), or other personal issues (*n* = 6, 22%), for example, losing a video game competition or having an argument with an owner of a retail establishment (see Table 2).[9]

Beyond grievances, some motives were related to the attackers' mental health symptoms (*n* = 5, 19%), while others were connected to ideological beliefs (*n* = 2, 7%). Of the two perpetrators motivated by an ideology, one was motivated by anti-abortion beliefs while the other was motivated by anti-Semitic beliefs. Additionally, one attacker appeared to have been motivated by the desire for fame or notoriety. For the remaining incidents (*n* = 6, 22%), a motive was not identifiable given information that was publicly available.

Table 2.

Components to Motive	2017	2018
Grievances	46%	52%
Domestic	18%	22%
Personal	7%	22%
Workplace	21%	11%
Mental Health/Psychosis	14%	19%
Ideological	21%	7%
Fame	4%	4%
Political	4%	0%
Unknown	14%	22%

*Percentages exceed 100 as some attackers had more than one motive.

BELIEFS: While only two of the attacks were primarily motivated by an ideology, nearly one-third of the attackers (*n* = 8, 30%) appeared to have subscribed to a belief system that has previously been associated with violence. Often the attackers' beliefs were multifaceted and touched on a range of issues, including white supremacy, anti-Semitism, conspiracy theories, sovereign citizens, animal rights, and the "incel" movement. Incels, or involuntarily celibates, are members of an Internet-based subculture of heterosexual males who view themselves as undesirable to females and therefore unable to establish romantic or sexual relationships to which they feel entitled.

FIXATIONS: Two-fifths of the attackers (*n* = 11, 41%) exhibited a fixation, defined as an intense or obsessive preoccupation with a person, activity, or belief to the point that it negatively impacted aspects of their lives. The focuses of these fixations included an ex-girlfriend, wife, or other females in the subjects' lives; perceived injustices; delusions; sociopolitical ideologies; and video games. The behaviors that demonstrated these fixations included, but were not limited to, posting written material or videos online, stalking or harassing others, and filing lawsuits or complaints to police.

> *On June 28, 2018, a man shot and killed five employees in a newspaper office. Six years prior, he had sued the newspaper and some of its employees for alleged defamation. He became fixated on the case, stating in 2013 that it had "become [his] life." He created social media profiles to impersonate people involved in the court proceedings. After the lawsuit was dismissed, he continued to file related court documents.*

TARGETING: In 11 cases (41%), the attacker appeared to have pre-selected targets in mind. Seven of those attacks resulted in harm to both the targeted person and random bystanders, and in three cases the harm was restricted to just those specifically targeted. In the remaining case, when the attacker could not find his intended targets at their workplaces, he randomly fired at other people associated with the office. In nearly two-thirds of the attacks (*n* = 16, 59%) harm was directed at persons indiscriminately.

> *On October 27, 2018, a man opened fire indiscriminately inside a synagogue. Eleven people were killed and six more were wounded before he was shot and apprehended by police. The attacker had previously accused a Jewish-founded refugee advocacy group of helping to transport refugees, whom he referred to as "invaders," from Central America into the United States. When he later attacked the synagogue, he reportedly targeted a specific Jewish congregation in the building that had previously partnered with that refugee aid group.*

KEY INVESTIGATIVE THEMES

SIGNIFICANT STRESSORS WITHIN FIVE YEARS: Most (n = 23, 85%) attackers had at least one significant stressor occur in their lives in the five years preceding the attack. For three-quarters of the attackers (n = 20, 74%), the stressors they experienced occurred within one year of the attack. Beyond the criminal charges described earlier, the stressors most often faced by the attackers were related to:

LIFE STRESSORS

- *Family/romantic relationships*, such as the death of a loved one, divorce, a broken engagement, or physical or emotional abuse.
- *Work or school*, such as being denied a promotion, losing a job, or being forced to withdraw from school.
- *Contact with law enforcement that did not result in arrests or charges*, including law enforcement responding to reports of inappropriately touching women, domestic violence, or engaging in other violent acts towards others.
- *Personal issues*, such as homelessness or losing a competition.

Over half of the attackers (n = 15, 56%) experienced stressors related to *financial instability* in the five-year period prior to their attacks. These financial stressors were evidenced through the inability to sustain employment, losing civil judgements in court, filing for bankruptcy, loss of income, or having to rely on others for income.

> *On April 3, 2018, a female opened fire at the headquarters of a video sharing website, injuring three people. The attacker had supported herself financially using the ad revenue generated by videos that she posted to the company's website, some of which had received hundreds of thousands of views. Prior to the attack, the woman had expressed her anger at the company over recent policy changes that resulted in a loss of income. Following the attack, her father reported that she had been angry for weeks and complaining that the company had ruined her life.*

THREATS AND OTHER CONCERNING COMMUNICATIONS: Nearly all of the attackers (n = 25, 93%) engaged in prior threatening or concerning communications. One-third had threatened someone (n = 10, 37%), including threats against the target in six cases (22%). Most of those who made threats against the target had a direct relationship with them, as a co-worker, domestic partner, classmate, member of the same treatment facility, or peer in a competition. Though the presence of prior threats to the target is unusual for some forms of targeted violence (e.g., assassination), threats are often seen in cases motivated by domestic or workplace issues, which together represent one-third of these mass attacks (n = 9, 33%).

All but four attackers (n = 23, 85%) made some type of communication that did not constitute a direct threat, but should have elicited concern. Some of these concerning communications included expressing interest in previous attackers, racist and misogynistic comments, referencing a desire to purchase a gun, and comments that suggest an aspiration to commit future violence.

> *On February 14, 2018, a former student opened fire at his prior high school, killing 14 students and 3 staff, and wounding an additional 17. The attacker had a long history of behavioral problems and concerning communications. While enrolled at the targeted high school, he was known by classmates to make racist and anti-Semitic comments and to speak openly about*

his guns. A year prior to the attack, someone who knew the attacker contacted local law enforcement to report that the attacker had posted on Instagram a photo of himself holding a gun and a statement similar to, "I am going to get this gun when I turn 18 and shoot up the school." Another concerned individual notified law enforcement of the attacker's concerning social media posts about a month before the shooting.

HISTORY OF ELICITING CONCERN: Most of the attackers (*n* = 21, 78%) in this report exhibited behaviors that caused concern in others. Those who were concerned had various degrees of association with the attackers, from those who were close to them, to strangers in the community who may have never met the attacker before.

The Behaviors that Elicited Concern

- Social media posts with alarming content
- Escalating anger or aggressive behavior
- Changes in behavior and appearance
- Expressions of suicidal ideations
- Writing about violence or weapons
- Cutting off communications
- Inappropriate behavior toward females
- Stalking and harassing behaviors
- Increased depression
- Increased drug use
- Erratic behavior
- Purchasing weapons
- Threats of domestic violence
- Acting paranoid

The responses from others to these behaviors varied from more passive activities like avoiding the attacker, to more active efforts like transporting the person for a mental health evaluation. The ways in which people responded to their concerns included:

- Mothers and fathers seeking therapy for the attacker, calling police, confiscating weapons, or searching for the person when they could not be reached.
- Family and friends making efforts to spend more time with the attacker.
- Online community members calling police.
- Fellow students telling school staff about their concerns.
- Law enforcement getting the attacker to undergo a mental health evaluation, revoking firearms licenses, or asking family to consensually restrict access to weapons.
- Employers firing them or calling their family members to express concern.
- Co-workers checking on them or suggesting counseling.
- Members of the community asking them to leave business establishments or treatment programs, sometimes resorting to calling law enforcement.

Who Was Concerned

Mothers & Fathers
Romantic Partners
Siblings & Children

•

Friends & Neighbors

•

School Staff &
Classmates

•

Supervisors &
Coworkers

•

Mental Health
Professionals

•

Law Enforcement
Judges & Attorneys
Community Services

•

Community Members
Religious Leaders

•

Online Community

For the majority of the attackers (n = 19, 70%), the concern others felt was so severe that they feared specifically for the safety of the individual, themselves, or others. Some of those concerned for their own safety acted on that fear by filing for divorce, ceasing communications, filing for restraining or protection orders, asking loved ones to stay with them out of fear, changing their daily routines, moving, or warning their own family and friends about their concerns. In one case, a person shared photos of the attacker so that others could remain alert and call the police if needed.

On November 2, 2018, a man opened fire inside a yoga studio, killing two and injuring five. From adolescence, others had expressed concerns about his behavior around women and girls. According to police investigative records and other sources, his conduct had resulted in the man being discharged from the Army, fired from two teaching jobs, reported to law enforcement, arrested and investigated by police on multiple occasions, banned from a university campus, asked to leave a child's party, and avoided by acquaintances and former friends.

MASS ATTACKS IN PUBLIC SPACES
2017 & 2018

Many of the key findings in both the 2017 and 2018 reports reflect similarities among the incidents and the attackers. For example, attacks occurred across the country and attackers predominantly used firearms. The majority of attackers elicited concern in others and two-thirds had histories of mental health symptoms or treatment. A majority of the attackers had recently experienced significant stressors, with just over half of the attackers experiencing financial instability in that same timeframe.

Table 3.

General Backgrounds	2017	2018
Gender - Male	100%	93%
Age: Range	15-66	15-64
Average	37	37
Illicit drug use or substance abuse	54%	22%
History of criminal charge(s)	71%	48%
Non-violent	57%	37%
Violent	54%	22%
History of domestic violence	32%	30%
Overall history of violence	64%	44%
Mental health symptoms	64%	67%
Known treatment or diagnosis	25%	44%
Investigative Themes	2017	2018
Beliefs	25%	30%
Fixation	39%	41%
Stressors	100%	85%
Financial instability	57%	56%
Threatening or concerning communications	86%	93%
History of making threats	50%	37%
Threats specific to the target	36%	22%
Concerning communications	82%	85%
Elicited concern	79%	78%
Concern about safety	46%	70%

CONSIDERATIONS

Like the year before, 2018 saw incidents of mass violence impact the places where we work, learn, worship, or otherwise conduct our daily activities. Consistent with previous research from the Secret Service, these attacks were found to be motivated by a variety of goals, grievances, and ideologies. The attackers varied widely on demographic factors, and while there is no single profile that can be used to predict who will engage in targeted violence, focusing on a range of concerning behaviors while assessing threats can help promote early intervention with those rare individuals that pose such a risk.

- **Mental health and mental wellness** – Mental illness, alone, is not a risk factor for violence, and most violence is committed by individuals who are not mentally ill. Two-thirds of the attackers in this study, however, had previously displayed symptoms indicative of mental health issues, including depression, paranoia, and delusions. Other attackers displayed behaviors that do not indicate the presence of a mental illness, but do show that the person was experiencing some sort of distress or an emotional struggle. These behaviors included displays of persistent anger, an inability to cope with stressful events, or increased isolation. A multidisciplinary approach that promotes emotional and mental wellness is an important component of any community violence prevention model. For example, a robust employee assistance program (EAP) can help to promote mental wellness in the workplace, whether that involves facilitating mental health treatment or assisting with other personal problems, like substance abuse, financial struggles, or problems in a personal relationship.

- **The importance of reporting** – Since three-quarters of the attackers had concerned the people around them, with most of them specifically eliciting concerns for safety, the public is encouraged to share concerns they may have regarding coworkers, classmates, family members, or neighbors. Such reports could be made to workplace managers, school administrators, or law enforcement, as appropriate. While over-reporting is not the goal, a reasonable awareness of the warning signs that can precede an act of violence may prompt community members to share their concerns with someone who can help. Systems can be developed to promote and facilitate such reporting, and people should be encouraged to trust their instincts, especially if they have concerns for someone's safety. For example, several states have recently developed statewide reporting infrastructures that allow students and others to utilize a smartphone app to submit anonymous tips to a call center staffed by law enforcement. This type of program can facilitate not only a law enforcement response to reported threats, but also a community-level response to reports of bullying, suicidal ideation, self-harm, or depression.

- **"…Do Something"** – Since 2010, the Department of Homeland Security has effectively promoted the "If You See Something, Say Something®" national campaign, originally developed by New York City's Metropolitan Transportation Authority, which encourages the reporting of suspicious activity. In many of these cases from 2018, members of the general public successfully performed their role in the "See Something, Say Something" process, by reporting their concerns to someone with a role in public safety. At that point, the responsibility is on the public safety professionals to "Do Something," namely assessing the situation and managing as needed. By adopting a multidisciplinary threat assessment approach, that standardizes the process for identifying, assessing, and managing individuals who may pose a risk of violence, law enforcement and others are taking steps to ensure that those individuals who have elicited concern do not "fall through the cracks."

- **Law enforcement partnerships** – While law enforcement has a key role to play in the prevention of community violence, intervening with individuals who may pose a risk is not the responsibility of law enforcement alone. Particularly in those instances where a concerning individual has not broken a law, the relationships between law enforcement and other community resources become paramount. Law enforcement personnel are encouraged to continue developing close partnerships with the mental health community, local schools and school districts, houses of worship, social services, and other private and public community organizations. The mission of law enforcement in the United States is public service oriented, and that mission will be most effectively executed through multidisciplinary and collaborative community efforts.

Targeted violence has a profound and devastating impact on those directly involved and a far reaching emotional impact to those beyond. Because these acts are usually planned over a period of time, and the attackers often elicit concern from the people around them, there exists an opportunity to stop these incidents before they occur. *Threat assessment* is one of the most effective practices for prevention. Many of the resources to support this process are already in place at the community level, but require leadership, collaboration, and information sharing to facilitate their effectiveness at preventing violence.

The Importance of Threat Assessment

"Threat assessment" refers to a proactive approach to violence prevention. It is an investigative model originally developed by the U.S. Secret Service to prevent assassinations, but has since been adapted to prevent all forms of targeted violence, regardless of motivation. This includes K-12 school shootings and acts of workplace violence. When implemented effectively, a threat assessment generally involves three key components:

Identify → Assess → Manage

Research indicates that the majority of perpetrators of targeted violence elicit concern in others prior to the attack. We rely on those people who observe such concerns to *identify* the individual to law enforcement or to someone else with a public safety responsibility. In educational settings or workplaces, concerns may be reported to a multidisciplinary threat assessment team that works in conjunction with law enforcement when needed. The responsible public safety entity is then tasked to *assess* the situation to determine how they can *manage* any risk of violence posed by the individual. With a focus on early intervention, this systematic approach is an important component of any safety plan. It allows communities to respond appropriately to a broad range of situations, from those individuals who are displaying a low-level concerning behavior to those who may pose an immediate and imminent risk of violence.

THE INCIDENTS

1) On January 23, a student fatally shot two and injured ten at a high school in Benton, KY.

2) On January 28, a gunman fatally shot four in a parking lot in Melcroft, PA.

3) On February 14, a former student fatally shot 17 and injured another 17 at a high school in Parkland, FL.

4) On February 14, a man drove a truck into a clinic, injuring three in East Orange, NJ.

5) On March 7, a gunman fatally shot two and injured two inside a restaurant in Hurtsboro, AL.

6) On March 9, a gunman fatally shot three at a treatment facility in Yountville, CA.

7) On April 3, a woman shot and injured three at the headquarters of a video sharing website in San Bruno, CA.

8) On April 22, a gunman fatally shot four and injured four others in a restaurant in Antioch, TN.

9) On May 18, a student fatally shot 10 and injured 13 at a high school in Santa Fe, TX.

10) On May 20, a man drove a vehicle into a restaurant, killing two and injuring three in Bessemer City, NC.

11) On May 24, a gunman injured three in a restaurant in Oklahoma City, OK.

12) On May 25, a man drove a vehicle onto a sidewalk, injuring three in Portland, OR.

13) On June 1, a gunman killed two at a law firm, followed by one at a psychologist's office, in Scottsdale, AZ.

14) On June 28, a gunman killed five in a newsroom in Annapolis, MD.

15) On July 5, a gunman injured six in the street near the oceanfront in Virginia Beach, VA.

16) On August 26, a gunman fatally shot two and injured nine at a video game competition in Jacksonville, FL.

17) On September 6, a gunman fatally shot three and injured two at a bank in Cincinnati, OH.

18) On September 12, a gunman fatally shot three in front of a trucking company in Bakersfield, CA.

19) On September 19, a gunman injured four at a municipal center in Masontown, PA.

20) On September 19, a gunman injured four in an office building in Middleton, WI.

21) On September 20, a gunman fatally shot three and injured three at a warehouse in Aberdeen, MD.

22) On October 27, a gunman fatally shot 11 in a synagogue in Pittsburgh, PA.

23) On November 2, a gunman fatally shot two and injured five in a yoga studio in Tallahassee, FL.

24) On November 5, a gunman fatally shot one and injured two at a drug treatment center in San Rafael, CA.

25) On November 7, a gunman fatally shot 11 and injured at least two at a bar in Thousand Oaks, CA.

26) On November 12, a gunman injured three at a food distribution warehouse in Albuquerque, NM.

27) On November 19, a gunman fatally shot three at a hospital in Chicago, IL.

---

[1] Additional threat assessment resources and publications from the National Threat Assessment Center are available on the U.S. Secret Service website, located at https://www.secretservice.gov/protection/ntac/.

[2] The limitations of open source information should be considered when reviewing the findings contained in this report. Since information for a few of the offenders was limited, it is likely that a larger number than reported here may have displayed the behaviors, symptoms, and other background elements described here.

[3] The incidents included in this report were identified and researched through open source reporting (e.g., media sources and released law enforcement records); therefore, it is possible that more incidents took place than were discovered at the time of this writing. Though there is much debate as to what defines a *mass attack*, for the purpose of this report we included acts of intentional violence in public spaces (e.g., parks, community events, retail establishments) or semi-public places (e.g., workplaces, schools, religious establishments) during which significant harm was caused to three or more persons. We excluded violence related to criminal acts (e.g., gang or drug activity), failed attempts at a mass attack, and spontaneous violence.

[4] In two incidents, the attackers harmed additional persons that were not included in the total number killed and injured, based on the criteria for this report. In one case, the attacker killed two individuals at a private residence following his attack in a public space. In another case, the attacker had killed one person the day prior to the mass attack. Further, the total of those harmed only included individuals that were harmed as a direct result of the subject's actions. Injuries sustained while fleeing the scene, for example, were not included.

[5] This report was prepared for educational and research purposes. The background and behaviors reported herein are of those individuals who: 1) were arrested for the act; 2) died at the scene; or 3) died immediately following the attack. Actions attributed to individuals who have been arrested, indicted, or charged in these incidents are merely allegations, and all are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[6] In one attack, the attacker used a combination of a firearm and smoke/flash-bang grenades. In another attack, the subject brought explosives to the school, but they were not used in the attack and were determined to be inoperable.

[7] Though illegal drug use within the previous year is one of the disqualifying factors for possessing a firearm under federal law, it was not considered in this review as information was not available to confirm active use within one year of the incident.

[8] For the purpose of this report, *domestic violence* was defined as physical force or the threat of imminent bodily harm inflicted on a romantic partner, parent/guardian, or child (of the assailant or romantic partner). If an attacker was classified as having a history of domestic violence against a parent or child, the perpetrator and the victim must have resided at the same location.

[9] One subject had both domestic and personal grievances as part of his motive for the attack.

United States Secret Service
NATIONAL THREAT ASSESSMENT CENTER
Mass Attacks in Public Spaces - 2018

OBSERVING THE SIGNS
THE BYSTANDER STUDY
USSS & US DOE

PRIOR KNOWLEDGE OF POTENTIAL SCHOOL-BASED VIOLENCE:

INFORMATION STUDENTS LEARN MAY PREVENT A TARGETED ATTACK

UNITED STATES SECRET SERVICE AND
UNITED STATES DEPARTMENT OF EDUCATION

WASHINGTON, DC
May 2008

Prior Knowledge of Potential School-Based Violence:
Information students learn may prevent a targeted attack

UNITED STATES SECRET SERVICE
AND
UNITED STATES DEPARTMENT OF EDUCATION

by

William S. Pollack, Ph.D.
Director, National Violence Prevention and Study Center
Director, Centers for Men and Young Men, McLean Hospital
Assistant Clinical Professor of Psychology
Department of Psychiatry, Harvard Medical School

William Modzeleski
Associate Assistant Deputy Secretary
Office of Safe and Drug-Free Schools
U. S. Department of Education

Georgeann Rooney
Threat Assessment Specialist
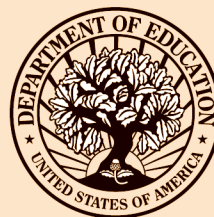National Threat Assessment Center
U. S. Secret Service

Acknowledgments

Prior Knowledge of Potential School-Based Violence:
Information students learn may prevent a targeted attack[1]

In the wake of several high-profile shootings at schools in the United States, most notably the shootings that occurred at Columbine High School on April 20, 1999, the United States Secret Service (Secret Service) and the United States Department of Education (ED) embarked on a collaborative endeavor to study incidents of planned (or *targeted*) violence in our nation's schools. Initiated in 1999, the study, termed the Safe School Initiative (SSI), examined several issues, most notably whether past school-based attacks were planned, and what could be done to prevent future attacks.

The SSI employed a method similar to an earlier Secret Service study, the Exceptional Case Study Project (ECSP), that examined targeted attacks on public officials and public figures (Fein & Vossekuil, 1999). In the ECSP the Secret Service coined the term *targeted violence* and defined it as any incident of violence where a known or knowable attacker selects a particular target prior to the violent attack (Fein, Vossekuil, & Holden, 1995). As with the ECSP, the SSI employed an operational focus to assist those involved with school safety to improve prevention efforts by increasing knowledge of targeted violence in schools. By studying past incidents of targeted violence in schools, the Secret Service and ED examined whether pre-attack behaviors of perpetrators could be identified to prevent future attacks.

The SSI identified specific incidents of targeted school violence and analyzed the attackers' behavioral pathways, from the initial idea of the attacks to the violent conclusions. This involved an in-depth study of 37 incidents of targeted school violence involving 41 perpetrators, which took place in the United States from January 1974 through May 2000. A full report of the findings as well as the significant implications for both practical application and further investigation may be found in two jointly published Secret Service/ED reports: *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States* (Vossekuil, Fein, Reddy, Borum, & Modzeleski, 2002) and *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates* (Fein et al., 2002). The reports focused on 10 key findings from the SSI:

- Incidents of targeted violence at schools rarely were sudden impulsive acts.
- Most attackers did not threaten their targets directly prior to advancing the attack.
- There was no useful or accurate "profile" of students who engaged in targeted school violence.
- Most attackers had difficulty coping with significant losses or personal failures. Moreover many had considered or attempted suicide.
- Many attackers felt bullied, persecuted or injured by others prior to the attack.
- Most attackers had access to and had used weapons prior to the attack.
- Despite prompt law enforcement responses, most shooting incidents were stopped by means other than law enforcement interventions.

---

[1] The study is on file with the McLean Hospital Institutional Review Board (IRB) under the title "A Systematic Pilot Study of Student Responses to Prior Knowledge of Potential School-Based Violence: What can we learn about life-sustaining prevention?"

- In many cases, other students were involved in some capacity.
- Most attackers engaged in some behavior prior to the incident that caused others concern or indicated a need for help.
- Prior to the incidents, other people knew about the attacker's idea and/or plan to attack.

While each of these findings is important and may be useful in detecting and preventing future attacks, the final two findings in particular highlight further areas of inquiry. First, the perpetrators exhibited concerning behavior prior to the attack in 93% of the incidents. This suggests that attacks might have been avoided with proper observation techniques and more open sharing of information. Second, and more significant, at least one other person had some type of knowledge of the attacker's plan in 81% of the incidents and more than one person had such knowledge in 59% of the incidents. Of those individuals who had prior knowledge, 93% were peers of the perpetrators – friends, schoolmates, or siblings (Vossekuil et al., 2002).

Study Purpose

The SSI findings highlight that in most targeted school-based attacks, individuals, referred to as *bystanders* in this report, had some type of advanced knowledge about planned school violence. Despite this advanced knowledge, the attacks still occurred. This study aimed to further the prevention of targeted school-based attacks by exploring how students with prior knowledge of attacks made decisions regarding what steps, if any, to take after learning the information.[2] The study sought to identify what might be done to encourage more students to share information they learn about potential targeted school-based violence with one or more adults.

Among the topics covered in semi-structured interviews with participants were the following key questions:
- What information was known by the bystander in advance of the attack?
- What relationship did the bystander have to the perpetrator(s)?
- Did the bystander share the information he or she learned of the planned violence with others?
- Was the bystander alone in his or her knowledge of the planned attack or was there discussion with other bystanders? If there was discussion among several bystanders, was there an agreement among them as to whether to report the information?
- How much did personal characteristics of the bystander as compared with issues related to the school climate influence the bystander's decision regarding whether to come forward with the information?
- What were the relationships and levels of interpersonal connections between the bystander and responsible adults?
- In retrospect, how did the bystander feel about his or her decision regarding whether to take action? What advice would the bystander give others?

---

[2] This study was conducted in partnership with McLean Hospital, a teaching affiliate of Harvard Medical School, and underwent human participants review through its IRB. The principal investigator was William S. Pollack.

Method

Study Participants
Initially, potential participants were identified in reference to two groups. One group included those students who had prior knowledge of planned school violence and were believed to have shared that knowledge to avert the planned attack. Participants in this group were identified through online searches of publicly available material, as well as through outreach to law enforcement and school personnel, for information about school shootings that were averted and individuals who had prior knowledge of the threatened targeted school violence. The second group included those students who had prior knowledge of planned targeted school violence and who attended a school where a shooting occurred. Participants in this group were drawn from the 37 cases originally studied in the SSI. Participants who indicated that they had some type of prior knowledge were identified from a review of media reports, law enforcement records, and court records contained in the SSI case files. In all, 198 bystanders were identified from the files with the number of bystanders identified per incident ranging from 0 to 28. Individuals who actively planned or encouraged the attack were omitted from the study.

Once potential participants were identified, researchers determined whether each participant met the study's inclusion criteria. Initially, participants were to be selected based on considerations related to the recency of the case, the participant's level of knowledge regarding the planned school attack, and the participant's relationship with the perpetrator of the attack. However, when recruitment for the study proved difficult more emphasis was placed on the participant's accessibility and willingness to be interviewed.

Researchers contacted 29 individuals who met the study's inclusion criteria. Fourteen of the individuals contacted either refused participation in the study or did not complete the informed consent process in spite of several outreach attempts. Thus, the final study participants consisted of 15 individuals, six of whom had prior knowledge of a potential threat and attended a school at which a school shooting was averted, and nine of whom had prior knowledge of a potential threat and attended a school at which a school shooting occurred. The six participants in the first group were drawn from four independent incidents in which a school attack was averted (two participants each from two incidents and one participant each from two separate incidents). The nine participants in the second group also were drawn from four independent incidents in which a shooting occurred at school (four participants from one incident, three participants from another incident, and one participant each from two separate incidents). In total, the participants represented eight school locations. At the time of the study, the participants ranged in age from 13 to 30 years.

Procedure
A member of the research team telephoned each participant (or legal guardian if the participant was a minor) and described the nature of the study and its benefits and risks. If the participant agreed, consent forms were mailed to the participant for review. The consent forms, approved by the McLean Hospital Institutional Review Board (IRB), included versions for adults and minors aged 13 to 17 years. The forms addressed two aspects of consent: consent to participate in the study interview and consent to have the study interview videotaped. Fourteen participants

consented to videotaping of their study interviews. Once the signed consent forms were returned, a confidential location was agreed upon for the interview.

Study data were gathered via review of SSI case files, public sources, and a semi-structured interview with each participant (n=15). The data were analyzed by researcher reviews of the taped interviews, first independently and later in conference. Case vignettes, included as an Appendix, were developed from the subject interviews.

In the process of reviewing the data, the researchers observed similarities as well as some differences between the group of students who had prior knowledge of planned targeted school violence and came forward with the information to avert the violence, and the group of students who had such prior knowledge but attended a school at which violence occurred. Due to the overlapping data and an emerging continuum between these two groups, which originally had been expected to be more distinct in nature, the groups were collapsed into one group for purposes of analysis.

Findings

Six key findings were identified. Given the small sample size and the exploratory nature of the study, generalization from these findings may be limited.

1. The relationships between the bystanders and the attackers, as well as when and how the bystanders came upon information about the planned attacks, varied.
From the original SSI case files, there was information available about the relationship between 119 of the bystanders and the attackers. Of those, 34% were friends with the attacker, 29% were acquaintances/co-workers/schoolmates, 6% were family members, and in 31% of the cases the relationship was of another type or unknown. Eighty-two percent of the bystanders received information directly from the attacker and 13% were told secondhand.[3] Details about when the bystander learned the information were available in 91 of the cases. A majority of those individuals received the information more than a day before the attack. Fifty-nine percent were told days or weeks in advance, 22% were told months or years prior, and 19% were told a few hours or less before the attack.

2. Bystanders shared information related to a threat along a continuum that ranged from bystanders who took no action to those who actively conveyed the information.
Participants displayed a range in their actions and willingness to come forward. A continuum emerged between bystanders who took no action and those bystanders who were proactive in conveying information related to the threat to others. For instance, while some came forward without external prompting and were entirely forthcoming, others revealed the information they knew only after repeated prodding from adults, including school safety officials. In addition, some bystanders did not share their information with anyone or attempt to come forward, while others discussed the information with, or sought the advice of, peers and adults. Information from the SSI case files indicated that only 4% of the individuals with prior knowledge attempted to dissuade the attacker from violence.

---

[3] It was unknown how the remaining 5% of the bystanders became aware of the potential threat.

3. School climate affected whether bystanders came forward with information related to the threats.

Some bystanders reported that the school climate influenced their decisions to share information with the school staff regarding the threats. Bystanders who came forward with information commented that they were influenced by positive relations with one or more adults, teachers, or staff, and/or a feeling within the school that the information would be taken seriously and addressed appropriately. Similarly, students who displayed a reluctance to come forward indicated that they anticipated a negative response from the school had they shared information.

- One student who knew of a weapon on school property was reluctant to come forward because he expected a negative reaction: "When you say something, you get in trouble or interrogated by teachers."

4. Some bystanders disbelieved that the attacks would occur and thus did not report them.

A number of bystanders reported not disclosing information related to the threat to a responsible adult because they did not believe the event would ever occur. Several factors contributed to this belief, to include:

- The student made the threat or voiced the plan repeatedly and over a long period of time, had been engaged in what might be considered attention-seeking behaviors, and had made peculiar comments.
- The described threat seemed unbelievable because it was so extreme. In one case, a bystander who had overheard some of the conspirators discussing their plans in great detail "didn't think anything of it . . . [didn't] think they would really do it" and therefore the bystander did not tell anyone.
- The student's tone when making the threat did not seem serious or it was thought he was joking. For instance, bystanders made comments such as "he kept eating his pizza while discussing the event" and "he'd say it violently but then laugh about it."
- The threats or statements were overt, repetitive, and/or clearly overheard by school personnel. This led the students to mistakenly believe that the threateners (and therefore the threats) were not serious.

5. Bystanders often misjudged the likelihood and immediacy of the planned attack.

Bystanders reported that often they did not come forward with information related to the potential attack because they felt they had more time to decide on an appropriate action. Whether the potential attacker shared specific or vague information with the bystander was not a determinant of the bystander's assessment of the likelihood of an attack or its imminence.

6. In some situations, parents and parental figures influenced whether the bystander reported the information related to the potential attack to school staff or other adults in positions of authority.

Bystanders were questioned regarding the influence parents and other adults in their lives may have had on their decision to share information related to the potential attack. For example, one bystander felt comfortable sharing her concerns with other adults because her parents reassured her it was the correct thing to do. In contrast, another bystander consulted a parent figure in his life and was advised to "mind his own business." The bystander did not share information related to the potential attack, and the following day a shooting occurred at his school.

Implications

Although the generalizability of this study's findings is limited due to the exploratory nature of the study and the small number of participants, several implications were derived from a review of its data and findings. These implications may impact whether a shooting at a school is prevented by encouraging students to come forward when they learn of an event that may cause harm to themselves, other students, or faculty. Further, these implications may help faculty, staff, and other adults take appropriate action when they become aware of a threatening situation.

1. Schools should ensure a climate in which students feel comfortable sharing information they have regarding a potentially threatening situation with a responsible adult.
One factor that contributed to a bystander's decision to share knowledge of planned school violence was the student's positive emotional connection to the school and to its staff (see also Fein et al., 2002). Bystanders who did not share information related to the planned attack reported no connection to the school or a negative perception of the school climate. They also expressed discomfort speaking to anyone, or believed that if they did speak to someone they either would not be believed or would get into trouble. Further, bystanders were reluctant to come forward if they felt that school officials would not keep the source of the information confidential, which would open the bystander to potential ridicule and retribution.

Conversely, in those instances where bystanders with information about a possible attack felt a positive emotional connection with the school or with someone on the staff, they were comfortable coming forward and reporting what they knew. If the bystanders knew they would be believed and the information they provided would be protected, they were more likely to come forward with that information.

Developing meaningful social and emotional connections with students and creating a climate of mutual respect are essential to keeping schools safe. Such a climate encourages all students with information about threats against the school or its students to share the information with a responsible adult. Students in this study felt connected to the school when they believed someone in the school knew them and cared for them. Schools demonstrate their commitments to such climates by promoting social and emotional connections between students, staff, and teachers in everyday interactions and activities. Simple and genuine measures, such as regularly greeting students, talking to students, and addressing students by name, help to make students feel connected and part of the school.

Law enforcement officers and educators need to convey clearly to students that merely reporting information about potential threats will not subject the student to negative consequences and/or liability. In this study, many bystanders feared negative consequences would result if they were to bring information forward. Schools and law enforcement need to counter this negative preconception by emphasizing the value of the information that the students may hold and reassuring them that sharing will not cause harm. Because attackers sometimes communicate vague information prior to an attack, a student may be wary of overreacting and getting someone in trouble. It should be explained to students that any reported information or threats will be investigated and appropriate action will be taken.

Creating a school climate in which students believe the school staff wants to hear from them about threats or possible attacks is critical to ensuring that students come forward. Students should be encouraged to come forward regardless of the amount of information they have, and school staff should convey to the students that if they do share information about potential school violence they will be supported. If students do not feel that they will be treated with respect and listened to in a non-judgmental manner, or that the information will not be protected, they will not come forward and the school will lose an opportunity to intervene in a possible attack, as well as assist a troubled student.

2. School districts are encouraged to develop policies that address the many aspects of reporting a threat.
While many schools have policies that address threatening behavior, these policies do not always attend to all aspects of reporting threats, such as what procedure a student should follow in reporting a threat and what the school's role is when such information is received. School policies should:

- Encourage students, staff, faculty, parents, and others to report all apparent threats or threatening or disturbing behaviors.
- Provide several options for the reporting of threats, including reporting anonymously if necessary.
- Ensure that all those who report a threat or threatening situation will be treated with respect and that the information they provide will be closely guarded.
- Emphasize that the school will take appropriate action on all reports and will, within the confines of privacy laws, provide feedback to the reporting student that the information was received, and that appropriate action was taken.
- Articulate what types of student information and knowledge can be shared, with whom it can be shared, and under what conditions it can be shared.
- Be clear as to who is responsible for acting on information received regarding threats.
- Where the law permits, include law enforcement and mental health officials in the review process.
- Track threats over time so that the information collected regarding threats can be used in the decision-making process.

To prevent crime and violence effectively and intercede when necessary, it would be helpful for schools to know what types of criminal acts occur and the frequency of those acts. While many school districts have some mechanisms to track incidents that occur in schools, few of them track threats made against other students or the school (especially if the event did not result in official law enforcement intervention). The result of this failure to collect and maintain records regarding threats is that very little is known about the extent or nature of the problem. Collecting more data about threats will permit law enforcement officials and educators to learn more about what students or groups of students have previously engaged in these behaviors, the manner in which they threatened others, the actions taken by the school and law enforcement in response, and the outcome. Analysis of this information can lead to the development of a more effective targeted violence prevention strategy.

3. Teachers, administrators, and other faculty should be trained on how to properly respond to students who provide them with information about a threatening or disturbing situation, as well as how to deal with actual threats.

Students talk among themselves in lunchrooms, hallways, and classrooms about a wide variety of topics, including inappropriate behaviors (such as bullying, harassment, and name calling) and criminal activities (such as drug sales, possession of weapons, and threats or plots against other students or the school). Staff and faculty may hear this information but sometimes discount it as typical youthful talk that does not warrant concern. However, staff and faculty would be advised to take these conversations seriously and investigate further when the situation suggests such action.

Schools are encouraged to train their faculty and staff to listen to what students are saying and, if they hear information about a potentially dangerous act, report it to the designated authority or committee within the school so that an inquiry may be initiated.

Conclusion

This examination into why some students who knew of planned school attacks came forward and reported what they knew, while others did not, is meant to be an exploratory pilot study. Although the number of participants was expected to be relatively small, it was not anticipated that recruiting study participants would be as difficult. The low number of participants is attributable to a variety of factors, to include the length of time since some of the incidents occurred (e.g. some cases occurred 20 to 30 years ago) and that some bystanders were reluctant to speak of their experiences. Despite the relatively small sample size, the information gained from this pilot study provides some insight for those involved with the prevention of school violence. Additional research that builds upon the findings of this pilot study should be conducted so that additional barriers to reporting information may be identified and overcome.

The data gathered as part of this study support several of the findings of the SSI. For example, many bystanders did not assess threats of violence made by other students as serious because they did not believe the person posed a real danger. The SSI recognized that a single individual, whether a student or adult, is often not equipped to adequately assess if a particular person poses a threat of targeted violence. The SSI recommended the creation of school threat assessment teams to examine all threats to make an initial determination as to whether the threat is valid. This initial review would then be followed by a law enforcement-led investigation. A team approach would allow students to share information related to threats with adults in the school and allow a more formal assessment as to whether the student(s) posed a danger.

Further, the SSI found that while what a person *said* was an important part of any inquiry or investigation, even more important was an examination of that person's *behavior*. The SSI revealed that some shooters made inappropriate words or statements over a long period of time, resulting in their statements being disregarded as idle chatter. While words alone are not always indicative of a potential attack, when viewed in the context of one's behavior they provide insight into one's potential or probable actions.

This study also highlights the importance of a school climate where adults encourage students to come forward with information about threats and other concerning behavior, without fearing punishment, ridicule, or not being taken seriously. All communities should develop school policies and practices to ensure students come forward when they have information about a threat or possible attack.

Appendix: Case Studies

In one interview, the bystander noted that the incident at his school occurred before the "wake-up call" of the shooting at Columbine High School. In retrospect, he described being concerned when, prior to the shooting, the shooter aimed a gun at him in response to an action by the bystander. Also, the bystander spoke to the shooter the day before the incident and he recalled that something about the conversation concerned him enough that he sought the advice of a trusted adult. After some questioning, the adult advised the bystander that he did not need to tell anyone about his concerns. The bystander accepted the advice and the following day his friend carried out a shooting at the school resulting in the deaths of some of his peers.

In addition to accepting the adult's advice to not share his concerns, the bystander shared two additional reasons he did not share the information with others. First, he said it was "hard to believe [a school shooting] could happen" in his own community. Although the bystander recalled that he did not take the possibility of an actual shooting seriously, he mentioned that he, along with several friends and the shooter, discussed how the techniques used to carry out a recent school shooting that was widely covered in the media, could have been improved. Since the bystander felt, from his own perspective, that he was only engaging in fanciful teenage bravado ("kidding around"), he assumed all of his friends also were engaging in the same joking behavior, including the soon-to-be attacker. Second, some reluctance was clearly related to his lack of a positive connection to anyone in a position of authority in his own school. He said he found adults at the school "too judgmental."

The bystander's advice to other students, now younger than he, is: "Don't take [such threats or jokes about potential violence] lightly. Come to . . . an adult for help, before it's too late."

* * * * *

In the same incident discussed in the first case study, two other students shared their experiences.

One bystander expressed that he thought the teachers in the school were aware of the shooter's "violent temper and direct threats." He described how the shooter had read papers aloud in front of the teacher and students, in which he spoke directly of harming the bystander and/or the school, and in which he outlined his fascination with bombs and killing. Given the openness of the shooter's threats in front of responsible adults and school authorities, the bystander thought school officials were aware of any danger the shooter posed and that they "had everything under control." Consequently, he believed there was no need for active intervention on his behalf. Prior to the incident, the school disciplined the shooter for possessing a gun on school property; however, the students were not notified. In retrospect, the bystander mentioned that he wished students had been notified as this information, combined with the information he and others had regarding the shooter's prior threatening statements and behaviors, may have altered the outcome.

Another bystander also reported that the shooter made numerous threats of violence at school in the presence of teachers and administrators. As a young adolescent, the bystander did not know what to make of her concerns or what to do. Since adults were aware of the problems, and given

her "trust for authority," the bystander assumed that the school staff was adequately addressing the issue. Looking back on the shooting, the bystander stated that children cannot afford to be passive about remarks they hear: "Don't take things said for granted." In addition, she said adults in schools "need to network more with the students, and bring various groups together."

* * * * *

In an example of an averted school shooting, a bystander reported that he had heard rumors about possible violence in his high school. He stated that the potential attackers did not seem to be the usual outcasts described in newspaper reports of previous school shootings across the United States. It was more "like they fit in with their own bad crowd within the school," he explained.

The bystander stated that certain factors were crucial in providing him the support and courage to avert what could have become another school shooting. First, he reported that he was not close friends with the potential attackers so that allowed him to be more objective when he learned of a possible attack plan. Second, the impact of the shooting at Columbine High School weighed heavily upon him: "If not for Columbine, I might have thought twice about coming forward, but I couldn't be one of those who sat by." The bystander stated that the potential incident seemed too similar to the events in Colorado. Third, he noted that he felt an obligation to come forward: "I thought of my friends and just couldn't say nothing. It was the right thing to do." In describing what happened after he came forward with the information, the bystander stated that "Everybody was nice and understanding, and that helped." In addition, he mentioned that his "mother supported" him in coming forward. He offered advice to others who might find themselves in a similar situation: "Make sure to tell somebody before something dangerous can happen."

References

Fein, R. A., & Vossekuil, B. V. (1999). Assassination in the United States: An operational study of recent assassins, attackers, and near-lethal approachers. *Journal of Forensic Sciences, 44,* 321-333.

Fein, R. A., Vossekuil, B., & Holden, G. (1995). Threat assessment: An approach to prevent targeted violence. *Research in Action.* U.S. Department of Justice, Office of Justice Programs, National Institute of Justice: Washington, D.C., at 1-7.

Fein, R., Vossekuil, B., Pollack, W., Borum, R., Modzeleski, W., & Reddy, M. (2002). *Threat assessment in schools: A guide to managing threatening situations and to creating safe school climates*. U.S. Department of Education, Office of Elementary and Secondary Education, Safe and Drug-Free Schools Program and U.S. Secret Service, National Threat Assessment Center, Washington, D.C.

Vossekuil, B., Fein, R., Reddy, M., Borum, R., & Modzeleski, W. (2002). *The final report and findings of the safe school initiative: Implications for the prevention of school attacks in the United States*. U.S. Department of Education, Office of Elementary and Secondary Education, Safe and Drug-Free Schools Program and U.S. Secret Service, National Threat Assessment Center, Washington, D.C.

OBSERVING THE SIGNS

A STUDY OF PRE-ATTACK BEHAVIORS OF ACTIVE SHOOTERS IN THE UNITED STATES BETWEEN 2000 AND 2013

USDOJ & FBI

REMINDERS

- There is no one "profile" of an active shooter.
- There is no single warning sign, checklist, or algorithm for assessing behaviors that identifies a prospective active shooter.
- While impossible to predict violent behavior, it is possible to prevent some attacks via effective threat assessment and management strategies.

ACTIVE SHOOTER DEMOGRAPHICS

The **63** active shooters in the sample did not appear to be readily identifiable prior to the attack *based on demographics alone*.

The youngest active shooter was 12 yoa and the oldest was 88 yoa with an average age of **37.8** years.

94% were male and only **6%** were female.

Among active shooters age 18 and older, **44%** were employed and **38%** were unemployed.

24% had at least some military experience.

57% were single at the time of the offense.

13% were married; **13%** were divorced; **11%** were partnered but not married; **6%** were separated.

35% had adult criminal convictions prior to the event.

62% had a history of acting in an abusive, harassing or oppressive way (e.g., bullying).

16% had engaged in intimate partner violence.

11% had engaged in stalking-related conduct.

PLANNING AND PREPARATION

73% of active shooters had a known connection with the attack site.

35% of active shooters age 18 and older targeted their workplace or former workplace.

88% of active shooters age 17 and younger targeted their school or former school.

Active shooters with no known connection to the site were more likely to conduct pre-attack site surveillance as compared to those with a connection to the targeted site.

21% of active shooters researched or studied past attacks by others.

In cases where the amount of time spent *planning* could be determined (n=34), **77%** (n=26) of the active shooters spent a week or longer planning their attack.

In cases where the amount of time spent *preparing* could be determined (n=46), **46%** (n=21) of the active shooters spent a week or longer preparing (procuring the means) for the attack.

In the four cases where active shooters took less than 24 hours to plan and prepare, all had at least one concerning behavior and three had an identifiable grievance.

FIREARMS ACQUISITION

40% of active shooters purchased a firearm legally and specifically for the purpose of the attack.

35% of active shooters already possessed a firearm and did not obtain it for the express purpose of the attack.

11% of active shooters borrowed or took a firearm from a person known to them.

6% of active shooters stole a firearm.

2% of active shooters purchased a firearm illegally.

STRESSORS

Active shooters experienced multiple stressors (with an average of **3.6** separate stressors) in the year prior to the attack. The stressors reported included:

62% Mental health

49% Financial strain

35% Job-related stressors

29% Conflict with friends/peers

27% Marital problems

22% Abuse of illicit drugs/alcohol

22% Other (e.g., caregiving responsibilities)

22% Conflict at school

21% Physical injury

18% Conflict with parents

16% Conflict with other family members

13% Sexual stress/frustration

11% Criminal problems

10% Civil problems

6% Death of friend/relative

2% No stressors

MENTAL HEALTH

25% of active shooters had a diagnosed mental illness prior to the offense.

Of the 25% (n=16), **12** had a mood disorder, **4** had an anxiety disorder, **3** had a psychotic disorder, and **2** had a personality disorder. One active shooter was diagnosed with Autism spectrum disorder, one with a developmental disorder, and one described as "other."

It could not be determined if a diagnosis had been given in **37%** (n=23) of the cases in this study.

SOCIAL CONNECTIONS

All active shooters either: a) lived with someone or b) had significant in-person or online social interactions.

68% of all active shooters lived with someone else.
- **64%** of active shooters 18 yoa or older lived with someone else.

86% of active shooters had significant in-person social interactions with at least one person in the year prior to the attack.

27% of active shooters had significant online interactions with another person within a year of the attack.

For this study, the FBI used data that has been verified to the greatest possible extent, relying almost exclusively on information contained in official law enforcement investigative files. Active shooting events which appeared to be spontaneous reactions to situational factors were excluded. The final sample of 63 active shooting incidents was included in this study.

CONCERNING BEHAVIORS

Concerning behaviors are *observable* behaviors, with an average of **4.7** concerning behaviors displayed by the active shooters in this sample. The concerning behaviors observed by others included:

62% Mental health

57% Interpersonal interactions

56% Leakage

54% Quality of thinking or communication

46% Work performance

42% School performance

35% Threats/confrontations

33% Anger

33% Physical aggression

21% Risk-taking

21% Firearm behavior

19% Violent media usage

13% Weight/eating

13% Drug abuse

11% Impulsivity

10% Alcohol abuse

10% Physical health

8% Other (e.g., idolizing criminals)

6% Sexual behavior

5% Quality of sleep

3% Hygiene/appearance

HOW WERE THE CONCERNING BEHAVIORS NOTICED

95% Verbal communication

86% Physical actions

27% Written communication

16% Online behavior

89% Demonstrated concerning behaviors that were observed in multiple ways

WHO NOTICED THE CONCERNING BEHAVIORS

92% Schoolmate *(if a student)*

87% Spouse/domestic partner *(if in a relationship)*

75% Teacher/school staff *(if a student)*

68% Family member

51% Friend

40% Co-worker

37% Other (e.g., neighbors)

25% Law enforcement

10% Online individual

5% Religious mentor

COMMON RESPONSES TO OBSERVED CONCERNING BEHAVIORS

83% Communicated directly to the active shooter

54% Did nothing

51% Reported the active shooter to a non-law enforcement authority

49% Discussed the behavior with a friend or family member

41% Reported the active shooter to a law enforcement authority

CONCERNING COMMUNICATIONS

55% of 40 active shooters who had a specific target made threats or had a prior confrontation.

When threats or confrontations occurred, **95%** were in person and only infrequently in writing or electronically **(14%)**.

88% of active shooters age 17 and younger leaked an intent to commit violence.

51% of active shooters leaked an intent to commit violence.

No instances of observed leakage were reported to law enforcement.

30% of active shooters created a legacy token prior to the attack.

PRIMARY GRIEVANCE

The majority of active shooters **(79%)** appeared to be acting in accord with a grievance of some kind, including:

33% Adverse interpersonal action against the active shooter

16% Adverse employment action against the active shooter

10% Other (e.g., general hatred of others)

5% Adverse governmental action against the active shooter

3% Adverse academic action against the active shooter

3% Adverse financial action against the active shooter

3% Domestic

3% Hate crime

3% Ideology/extremism

21% Unknown/no grievance identified

Even the active shooters with no identifiable grievance demonstrated at least two concerning behaviors (with an average of **5.4** behaviors) that were observed by others.

PRECIPITATING EVENT

Of the 50 active shooters who had an identifiable grievance, nearly half of them **(44%)** experienced a precipitating or triggering event related to the grievance.

TARGETING

While approximately **one-third** of active shooters in this sample victimized only random members of the public, most active shooters arrived at a targeted site with a specific person or persons in mind.

SUICIDE: IDEATION AND ATTEMPTS

48% (n=30) of active shooters had suicidal ideation or engaged in suicide-related behaviors at some point prior to the attack.
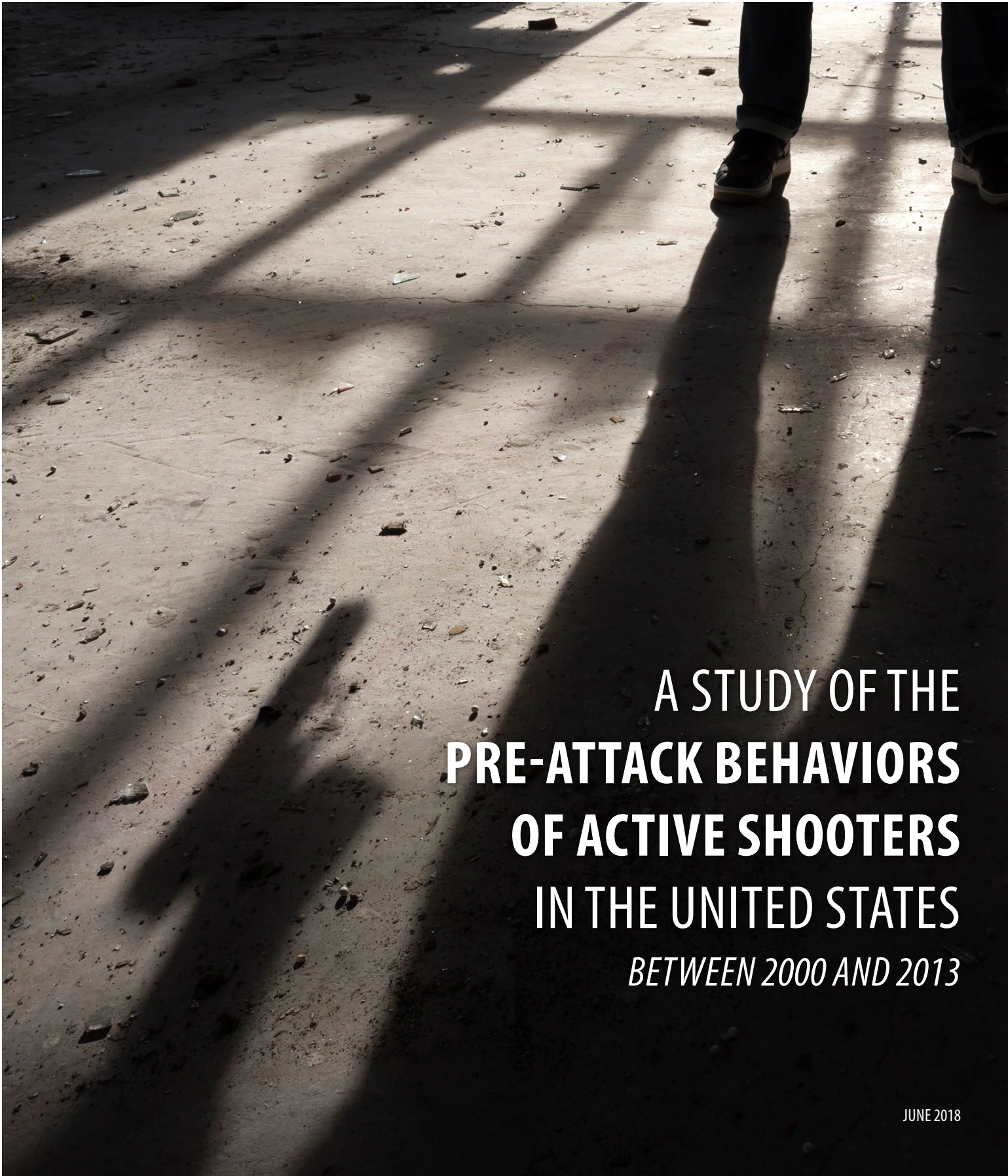
- Of the 30 suicidal active shooters, **90%** showed signs of suicidal ideation and **23%** made actual suicide attempts.
- **70%** of these behaviors occurred within one year of the shooting.

RESOURCES

Persons suspected of planning an active shooting should be immediately reported to local law enforcement or to a threat assessment team.

The BAU's Behavioral Threat Assessment Center (BTAC) is the only multi-agency behavioral threat assessment and threat management team in the U.S. Government. Requests for BTAC assistance can be made via the BAU Coordinator in your local FBI Field Office.

A Study of the Pre-Attack Behaviors of Active Shooters in the United States is available for download at www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view

A STUDY OF THE
PRE-ATTACK BEHAVIORS
OF ACTIVE SHOOTERS
IN THE UNITED STATES

BETWEEN 2000 AND 2013

Authors

James Silver, Ph.D., J.D., Worcester State University

Andre Simons, Supervisory Special Agent, Behavioral Analysis Unit, FBI

Sarah Craun, Ph.D., Behavioral Analysis Unit, FBI

A Study of the Pre-Attack Behaviors of Active Shooters in the United States
Between 2000 and 2013

Click on a link above to jump to a page.

Acknowledgments

The authors wish to thank the many dedicated members and former members of the FBI's Behavioral Analysis Unit (BAU) who supported this study, including Crime Analyst Kristen Solik, BAU; Unit Chief John Wyman, BAU; Unit Chief Kristen Slater, BAU; Unit Chief Kevin Burton, BAU; Unit Chief Shawn VanSlyke, BAU (ret.); Research Coordinator Kristen Lybert, BAU; Supervisory Special Agents (SSAs) Karie Gibson and Adrienne Isom, BAU; Mr. Bryan Czako; Mr. Davis Moore; and Mr. James Russell. The authors also offer special thanks and gratitude to our colleagues in the BAU's Behavioral Threat Assessment Center (BTAC).

Further, the authors express their appreciation to Assistant Director Kerry Sleeper, Section Chief Katherine Schweit (ret.), Unit Chief James Green, and Supervisory Intelligence Analyst Deborah Cryan of the FBI's Office of Partner Engagement for their past and ongoing support of this project. Special thanks as well to Visual Information Specialist Erin Kim of the FBI's Office of Public Affairs.

The authors are exceptionally grateful to our many threat assessment colleagues who have partnered with and supported the BAU over several years. These professionals quietly and tirelessly work each day to prevent active shootings in our schools, universities, houses of worship, and businesses.

The authors and researchers from the FBI's Behavioral Analysis Unit involved in preparing this report are aware of the horrific impact these shootings have had on victims, survivors, families, and communities. We extend our deepest sympathies to those who have suffered the unimaginable tragedy of an active shooting, either personally or as a family member. We know that behind the statistics and numbers presented here are thousands of individuals with personal stories of grief, bravery, and resilience. In partnership with other law enforcement and threat assessment professionals, we remain committed to doing everything possible to prevent future attacks. Although much work remains, we present this report as a step towards disrupting those who would seek to inflict catastrophic harm.

Introduction

In 2017 there were 30 separate active shootings in the United States, the largest number ever recorded by the FBI during a one-year period.[1] With so many attacks occurring, it can become easy to believe that nothing can stop an active shooter determined to commit violence. "The offender just snapped" and "There's no way that anyone could have seen this coming" are common reactions that can fuel a collective sense of a "new normal," one punctuated by a sense of hopelessness and helplessness. Faced with so many tragedies, society routinely wrestles with a fundamental question: can *anything* be done to prevent attacks on our loved ones, our children, our schools, our churches, concerts, and communities?

There is cause for hope because there *is* something that can be done. In the weeks and months before an attack, many active shooters engage in behaviors that may signal impending violence. While some of these behaviors are intentionally concealed, others are observable and — if recognized and reported — may lead to a disruption prior to an attack. Unfortunately, well-meaning bystanders (often friends and family members of the active shooter) may struggle to appropriately categorize the observed behavior as malevolent. They may even resist taking action to report for fear of erroneously labeling a friend or family member as a potential killer. Once reported to law enforcement, those in authority may also struggle to decide how best to assess and intervene, particularly if no crime has yet been committed.

By articulating the concrete, observable pre-attack behaviors of many active shooters, the FBI hopes to make these warning signs more visible and easily identifiable. This information is intended to be used not only by law enforcement officials, mental health care practitioners, and threat assessment professionals, but also by parents, friends, teachers, employers and anyone who suspects that a person is moving towards violence.

In 2014, the FBI published a report titled *A Study of Active Shooter Incidents in the United States Between 2000 and 2013*.[2] One hundred and sixty active shooter incidents in the United States occurring between 2000 and 2013 were included in the sample. In this first report, the FBI focused on the circumstances of the active shooting events (e.g., location, duration, and resolution) but did not attempt to identify the motive driving the offender, nor did it highlight observable pre-attack behaviors demonstrated by the offender. The 2014 report will be referred to as the "Phase I" study.

The present study ("Phase II") is the natural second phase of that initiative, moving from an examination of the parameters of the shooting events to assessing the pre-attack behaviors of the shooters themselves. This second phase, then, turns from the vitally important inquiry of "what happened during and after the shooting" to the pressing questions of "how do the active shooters behave *before* the attack?" and, if it can be determined, "why did they attack?" The FBI's objective here was to examine specific behaviors that may precede an attack and which might be useful in identifying, assessing, and managing those who may be on a pathway to deadly violence.

---

1   https://www.fbi.gov/file-repository/active-shooter-incidents-us-2016-2017.pdf/view
2   https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1.pdf/view

Key Findings of the Phase II Study

1. The **63** active shooters examined in this study did not appear to be uniform in any way such that they could be readily identified prior to attacking *based on demographics alone*.

2. Active shooters take time to plan and prepare for the attack, with **77%** of the subjects spending a week or longer planning their attack and **46%** spending a week or longer actually preparing (procuring the means) for the attack.

3. A majority of active shooters obtained their firearms legally, with only very small percentages obtaining a firearm illegally.

4. The FBI could only verify that **25%** of active shooters in the study had ever been diagnosed with a mental illness. Of those diagnosed, only three had been diagnosed with a psychotic disorder.

5. Active shooters were typically experiencing multiple stressors (an average of **3.6** separate stressors) in the year before they attacked.

6. On average, each active shooter displayed **4 to 5** concerning behaviors over time that were observable to others around the shooter. The most frequently occurring concerning behaviors were related to the active shooter's mental health, problematic interpersonal interactions, and leakage of violent intent.

7. For active shooters under age 18, school peers and teachers were more likely to observe concerning behaviors than family members. For active shooters 18 years old and over, spouses/domestic partners were the most likely to observe concerning behaviors.

8. When concerning behavior was observed by others, the most common response was to communicate directly to the active shooter (**83%**) or do nothing (**54%**). In **41%** of the cases the concerning behavior was reported to law enforcement. Therefore, just because concerning behavior was *recognized* does not necessarily mean that it was *reported* to law enforcement.

9. In those cases where the active shooter's primary grievance could be identified, the most common grievances were related to an adverse interpersonal or employment action against the shooter (**49%**).

10. In the majority of cases (**64%**) at least one of the victims was specifically targeted by the active shooter.

*All percentages in this report are rounded to the nearest whole number.

Methodology

With the goal of carefully reviewing the pre-attack lives and behaviors of the active shooters, the FBI developed a unique protocol of 104 variables covering, among other things:

- Demographics

- Planning and preparation

- Acquisition of firearms in relation to the attack

- Stressors

- Grievance formation

- Concerning pre-attack behaviors and communications

- Targeting decisions

- Mental health

Whereas Phase I analyzed event circumstances that are typically well documented both in law enforcement incident reports and reliable open sources[3], this second phase is substantially based on observations of what are often nuanced behavioral indicators demonstrated by the active shooter prior to the attack. Given the subtle nature of many of the factors relevant to the inquiry, the FBI decided to use data that have been verified to the greatest possible extent, relying almost exclusively on information contained in official law enforcement investigative files.[4] For this reason, Phase II includes only those cases where the FBI obtained law enforcement investigative files that contained "background" materials (e.g., interviews with family members, acquaintances, neighbors; school or employment records; writings generated by the subject) adequate to answer the protocol questions.[5] In addition, as Phase II focused on identifying pre-attack behaviors of those on a trajectory to violence, active shooting events which appeared to be spontaneous reactions to situational factors (e.g., fights that escalated) were excluded. This resulted in a final sample of 63 active shooting incidents included in the Phase II study.

The use of law enforcement investigative case files as the primary source of data makes this study unique in comparison to other reports that typically rely upon unverified data derived from open sources. The comprehensive evaluation of law enforcement case files for suitability and completeness also contributed to the substantial time it has taken to prepare and publish this study.

The FBI examined whether the 63 cases included in Phase II are representative of the entire Phase I sample ($N = 160$). To identify the differences in the samples between Phase I and Phase II ($N = 160$ versus $N = 63$), the FBI compared those cases that were *only* in Phase I ($n = 97$) to those cases included in Phase II ($N = 63$), assessing potential differences between the active shooters (e.g., race, gender, age, and whether the offender committed suicide subsequent to the attack), as well as potential differences in the characteristics of the incidents (number of victims killed, number of law enforcement officers killed, location of the incident, active shooter movement during the event, and if the event concluded prior to the arrival of law enforcement).

---

3   Incident overview (e.g., date, location), incident specifics (weapon(s) used, duration of event), and incident outcome (deaths, injuries, resolution).
4   For one incident, the study relied on publicly available official reports which were based on the complete law enforcement investigative files.
5   The investigative files did not contain uniform amounts of subject-related behavioral information, as the depth and breadth of investigations varied based on several factors, including available resources, the prospect or not of trial, and the complexity of the event.

As compared to the 97 cases that were only in Phase I, the 63 cases in Phase II had the following characteristics:

- Had a higher number of victims killed on average during each shooting;

- Were more likely to end before law enforcement arrived;

- Were more likely to include offenders who identified with Asian and Caucasian ethnicity, with active shooters identified with African American and Hispanic ethnicity generally underrepresented as compared to Phase I;

- Were more likely to occur in an educational facility or a house of worship; and

- Were more likely to end with the active shooter committing suicide.

After cases were identified, a three-stage coding process was utilized. First, two researchers read all case materials and independently coded each of the cases across all protocol variables. The researchers took a conservative approach to coding, declining to definitively answer any question that was not supported by record evidence. Second, another experienced coder (the "reviewer") also read each investigative file. In the final stage, the coders and the reviewer met for each of the 63 cases, compared answers, discussed disagreements, and produced a single reconciled set of data.

SHOOTER DEMOGRAPHICS

The sample comprised individuals who varied widely along a range of demographic factors making it impossible to create a demographic profile of an active shooter. Indeed, the findings and conclusions of this study should be considered in light of the reality that these 63 active shooters did not appear to be uniform in any way such that they could be readily identified prior to attacking *based on demographics alone*.

Age:

The youngest active shooter was 12 years old and the oldest was 88 years old with an average age of 37.8 years. Grouping the active shooters by age revealed the following:

FIGURE 1
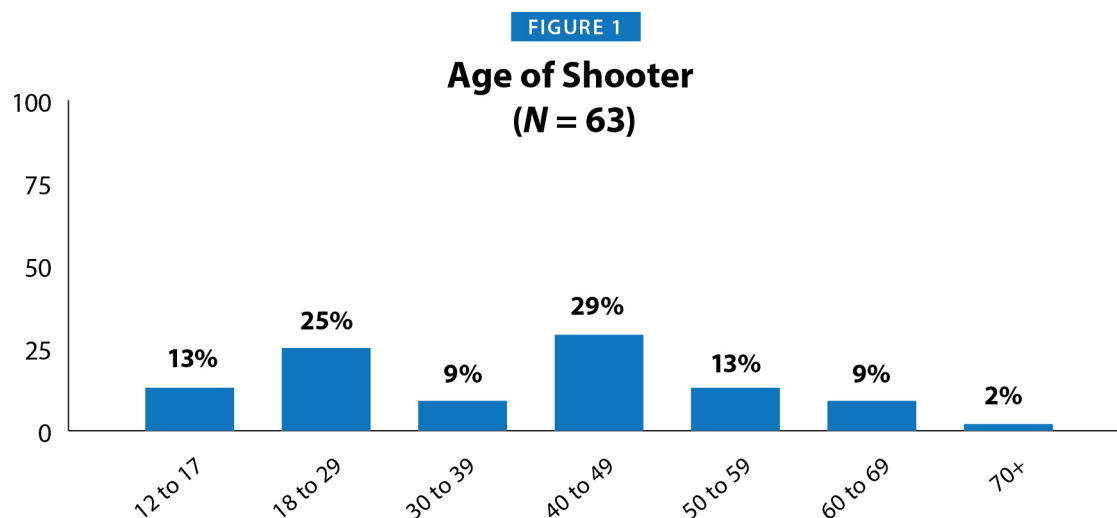
Age of Shooter
($N = 63$)

Gender and Race:

The sample was overwhelmingly male (94%, *n* = 59), with only four females in the data set (6%, *n* = 4), and varied by race as shown in Figure 2:[6]

FIGURE 2

Race (*N* = 63)

- WHITE 63%
- ASIAN 10%
- BLACK 16%
- HISPANIC 6%
- MIDDLE EASTERN 3%
- NATIVE AMERICAN 2%
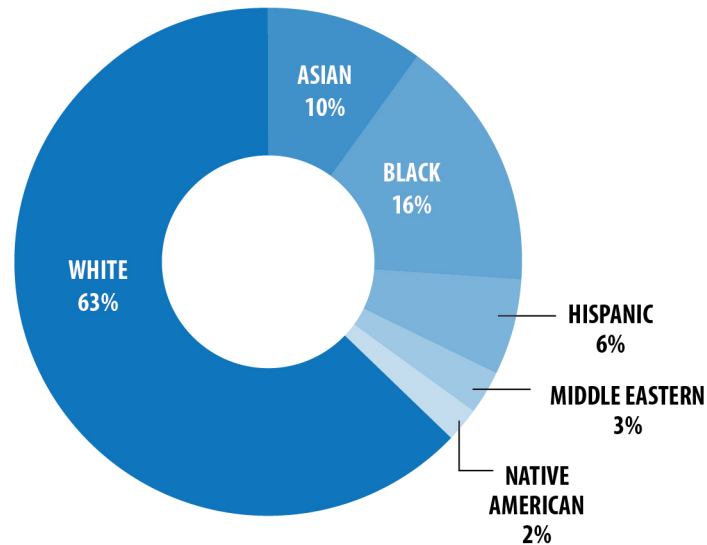
Highest Level of Education[7]:

None of the active shooters under the age of 18 had successfully completed high school, and one (age 12) had not yet entered high school. When known, the highest level of education of adults varied considerably, as shown in Figure 3:

FIGURE 3

Highest Level of Education Completed – 18 Years and Older
(*n* = 55)

- UNKNOWN 36%
- COMPLETED MASTERS/DOCTORATE 5%
- SOME GRADUATE EDUCATION 2%
- COMPLETED FOUR YEAR COLLEGE 7%
- ATTENDED FOUR YEAR COLLEGE 11%
- ATTENDED COMMUNITY COLLEGE/TRADE SCHOOL 11%
- COMPLETED HIGH SCHOOL 20%
- NONE OR SOME HIGH SCHOOL 7%
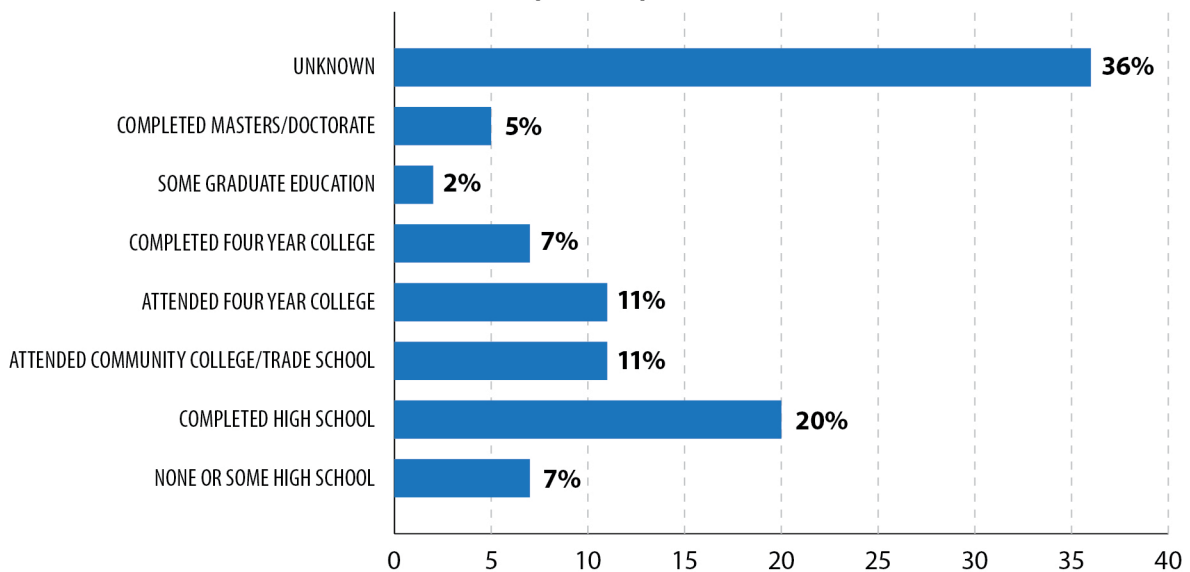
*Does not sum to 100% due to rounding.

---

6   Descriptors of active shooters' races were obtained from law enforcement records.

7   Active shooters under the age of 18 (*n*=8) were excluded in analyses for those variables not typically pertaining to juveniles (e.g., marital status, higher education).

10

Employment:

The active shooters who were under 18 years old were all students. As featured in Figure 4, nearly equal percentages of the adult active shooters 18 years or older were employed as were unemployed, and 7% ($n = 4$) were primarily students. The rest of the adults were categorized as retired, disabled/receiving benefits, or other/unknown.

Employment – 18 Years and Older
($n = 55$)

UNEMPLOYED
38%

STUDENT
7%

OTHER
4%

RETIRED
4%

EMPLOYED
44%

DISABLED
2%

UNKNOWN
2%

*Does not sum to 100% due to rounding.
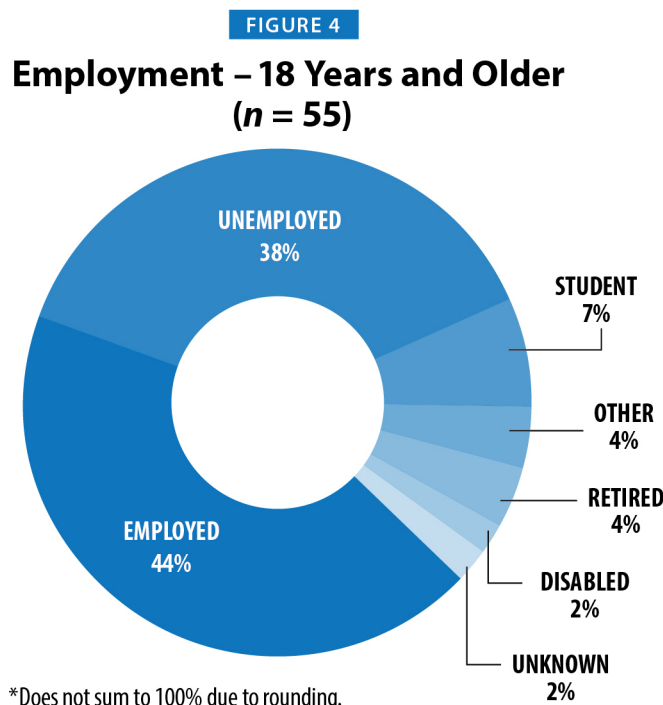
Military:

Of the active shooters 18 and older, 24% ($n = 13$) had at least some military experience, with six having served in the Army, three in the Marines, two in the Navy, and one each in the Air Force and the Coast Guard.

Relationship Status:

The active shooters included in the Phase II study were mostly single at the time of the offense (57%, $n = 36$). Thirteen percent ($n = 8$) were married, while another 13% were divorced. The remaining 11% were either partnered but not married ($n = 7$) or separated (6%, $n = 4$).

Criminal Convictions and Anti-Social Behavior[8]:

Nineteen of the active shooters aged 18 and over (35%) had adult convictions prior to the active shooting event. As visualized in Figure 5, the convictions can be categorized as crimes against society, property, or persons. The category of "crimes against society" included offenses such as driving under the influence, disorderly conduct and the possession of drug paraphernalia. Both the misdemeanor and felony "crimes against property" involved non-violent offenses, such as conspiracy to commit theft, theft, possession of stolen property, and criminal mischief. The misdemeanor "crimes against persons" were not inherently dangerous, but the felony "crimes against persons" involved convictions for criminal sexual assault of a family member, aggravated stalking, and endangering a person (although no active shooter was convicted of more than one crime against a person).

---

8   The study does not include juvenile adjudications; therefore, we did not run the analyses on those aged 17 and younger.

FIGURE 5
Adult Criminal Convictions – 18 Years and Older
(*n* = 55)
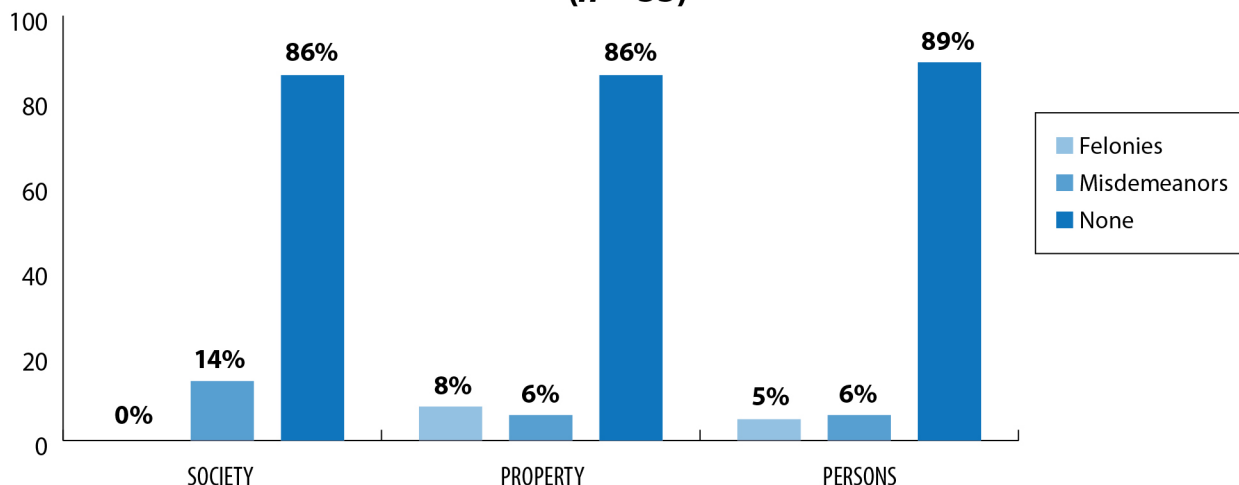
*There was only one case where an active shooter had both a felony and a misdemeanor conviction in a single category (under "Property").

In sum, the active shooters had a limited history of adult convictions for violent crime and a limited history of adult convictions for crime of any kind.

Because formal criminal proceedings may not capture the full range of anti-social behaviors in a person's background, the FBI also looked for evidence of behaviors that were abusive and/or violent, but which did not result in a criminal charge. For some active shooters, no evidence of these behaviors was found, but given that these actions by definition did not involve the formal criminal justice system, it is possible that more violent incidents occurred than are reported here.

We found evidence that 62% (*n* = 39) of the active shooters had a history of acting in an abusive, harassing, or oppressive way (e.g., excessive bullying, workplace intimidation); 16% (*n* = 10) had engaged in intimate partner violence; and 11% (*n* = 7) had engaged in stalking-related conduct.[9]

Considerations

There were very few demographic patterns or trends (aside from gender) that could be identified, reinforcing the concept that there is no one "profile" of an active shooter. Perhaps most noteworthy is the absence of a pronounced violent criminal history in an overwhelming majority of the adult active shooters. Law enforcement and threat management professionals assessing a potentially violent person may therefore wish to avoid any reliance on demographic characteristics or on evidence (or lack thereof) of prior criminal behavior in conducting their assessments.

---

9   This number may be underrepresented given the high percentage of unknown responses as related to stalking behaviors (68%).

PLANNING AND PREPARATION

This study examined two related but separate temporal aspects of the active shooters' pre-attack lives — total time spent *planning* the attack and total time spent *preparing* for the attack.[10,11,12] The purpose in analyzing these chronologies was to establish the broad parameters during which active shooters were moving toward the attack and to identify behaviors that may have been common during these time periods.

In this context, planning means the full range of considerations involved in carrying out a shooting attack. This includes the decision to engage in violence, selecting specific or random targets, conducting surveillance, and addressing all ancillary practical issues such as victim schedules, transportation, and site access. Planning is more specific than a general intent to act violently and involves the thought processes necessary to bring about an intended outcome. Since planning may primarily be an internal thought process, it was often difficult to find objective, observable indications of an active shooter's planning. In nearly half of the cases, the total time spent planning is unknown. However, this is different than declaring that there was no evidence of planning at all, because in every case there was at least some evidence that the active shooter planned the attack; the challenge was ascertaining when the planning began.

In establishing the total duration of planning, the FBI looked for evidence of behaviors that were observable (e.g., conversations, conducting surveillance) as well as in materials that were private to the active shooter (e.g., journals, computer hard drives) and likely unknowable to others until after the attack. As demonstrated in Figure 6, there was a wide range of planning duration in the 34 cases where the time spent planning could reasonably be determined.

Time Spent Planning
(*n* = 34)

*Does not sum to 100% due to rounding.
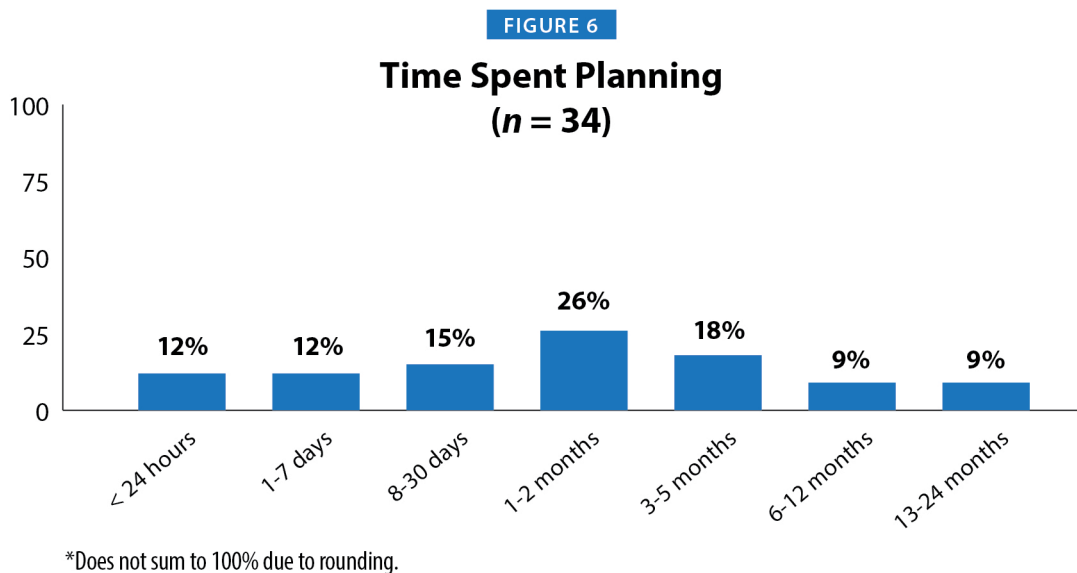
With regard to specific planning activities, care should be taken in the interpretation of the data. For instance, our study indicates that few active shooters overall approached or conducted surveillance on their target (14%, *n* = 9), and fewer still researched or studied the target site where the attack occurred (10%, *n* = 6). While this could indicate that the active shooters were uninterested in knowing about their targets or attack sites in advance or engaged in little tactical planning, this is inconsistent with the operational experience of the FBI. The likely reason for this finding is that the active shooters often attacked people and places with which they were already familiar. There was

10   Calhoun, T., & Weston, S., (2003). Contemporary threat management. San Diego: Specialized Training Services;

11   Fein, R. & Vossekuil, B. (1999). Assassination in the United States: an operational study of recent assassins, attackers, and near-lethal approachers. *Journal of Forensic Sciences.*

12   Vossekuil, B., Fein, R., Reddy, M., Borum, R., & Modzeleski, W. (2004). *The final report and findings of the safe school initiative: Implications for the prevention of school attacks in the United States.* Washington, DC: U.S. Secret Service and the U.S. Department of Education.

a known connection between the active shooters and the attack site in the majority of cases (73%, *n* = 46), often a workplace or former workplace for those 18 and older (35%, *n* = 19), and almost always a school or former school for those younger than 18 (88%, *n* = 7), indicating that in most cases the active shooter was already familiar with both the attack site as well as the persons located at the site. Conversely, those active shooters with no affiliation to the targeted site behaved differently. Active shooters with no known connection to the site of their attack were more likely to conduct surveillance (p < .05) and research the site (p < .01). With routine contact, pre-attack surveillance could presumably be conducted concurrent to normalized activity and eliminate the need for a more formalized or detectable reconnaissance of a chosen target.

The investigative files also demonstrated that only some active shooters researched or studied past attacks by others (21%, *n* = 13). This is not to say that other active shooters were unaware of past attacks — it is difficult to imagine that they did not have at least some basic knowledge of prior infamous shootings that received national media coverage. The FBI again suspects that this behavior may be underrepresented in the study sample, especially as we could not determine if active shooters researched past attacks in 46% of the cases.

Preparing was narrowly defined for this story as actions taken to procure the means for the attack, typically items such as a handgun or rifle, ammunition, special clothing and/or body armor. The focus was on activities that could have been noticed by others (e.g., a visit to a gun store, the delivery of ammunition) and which were essential to the execution of the plan. The FBI was able to find evidence of time spent preparing in more cases than for time spent planning (likely reflecting the overt nature of procuring materials as opposed to the presumably largely internal thought process of planning). As Figure 7 demonstrates, in more than half of the cases where the time spent preparing was known, active shooters spent one week or less preparing for the attack.

Time Spent Preparing
(*n* = 46)
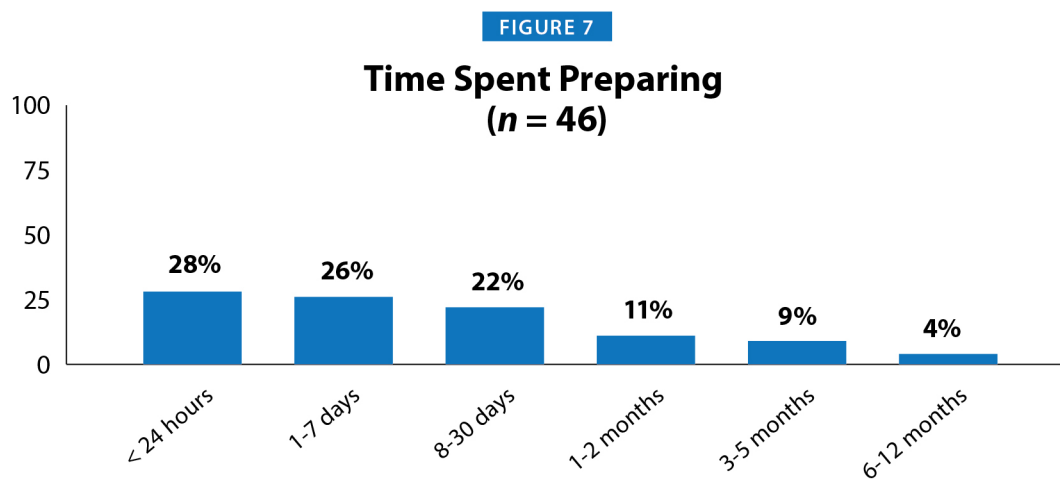
FIREARMS ACQUISITION

As part of the review of the active shooter's preparations, the FBI explored investigative records and attempted to identify how each active shooter obtained the firearm(s) used during the attack. Most commonly (40%, *n* = 25), the active shooter purchased a firearm or firearms legally and specifically for the purpose of perpetrating the attack. A very small percentage purchased firearms illegally (2%, *n* = 1) or stole the firearm (6%, *n* = 4). Some (11%, *n* = 7) borrowed or took the firearm from a person known to them. A significant number of active shooters (35%, *n* = 22) already possessed a firearm and did not appear (based on longevity of possession) to have obtained it for the express purpose of committing the shooting.

FIGURE 8

Firearms Acquisition
(*N* = 63)
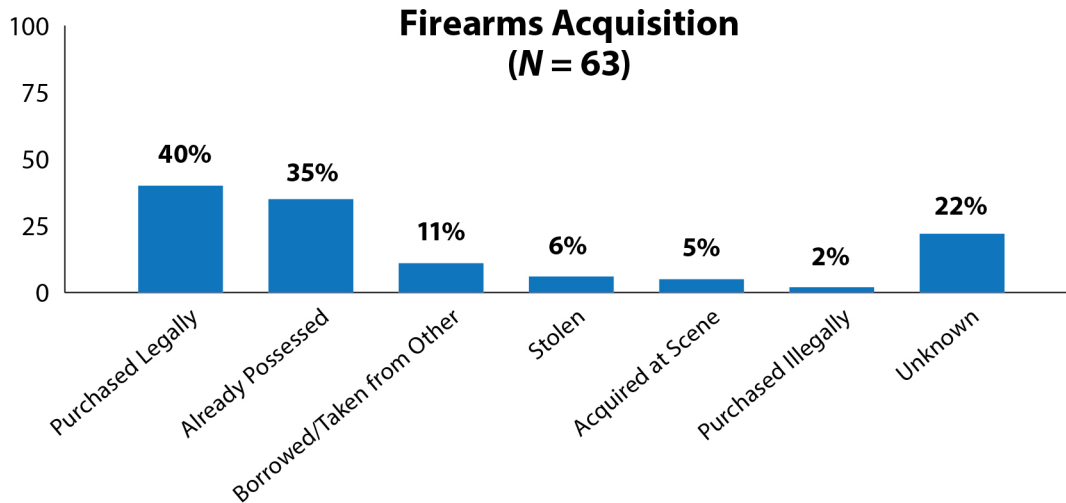
*Data percentages detailed above add to greater than 100% as active shooters could have obtained multiple firearms in different ways.

Considerations

Active shooters generally take some time to plan and carry out the attack. However, retrospectively determining the exact moment when an active shooter decided to engage in violence is a challenging and imprecise process. In reviewing indicators of planning and preparing, the FBI notes that most active shooters (who demonstrated evidence of these processes in an observable manner) spent days, weeks, and sometimes months getting ready to attack. In fact, in those cases where it could be determined, 77% of the active shooters (*n* = 26) spent a week or longer planning their attack, and 46% (*n* = 21) spent a week or longer preparing. Readers are cautioned that simply because some active shooters spent less than 24 hours planning and preparing, this should not suggest that potential warning signs or evidence of an escalating grievance did not exist before the initiation of these behaviors. In the four cases where active shooters took less than 24 hours to plan and prepare for their attacks, all had at least one concerning behavior and three had an identifiable grievance.

Perhaps unsurprisingly, active shooters tended to attack places already familiar to them, likely as a result of a personal grievance which motivated the attack and/or as a result of operational comfort and access. A unique challenge for safety, threat assessment, and security professionals will be to identify "outside" active shooters who are not already operating within the target environment. Pre-attack site surveillance by an outsider may be one observable behavior in physical or online worlds indicative of planning and preparation activities.

STRESSORS

Stressors are physical, psychological, or social forces that place real or perceived demands/pressures on an individual and which may cause psychological and/or physical distress. Stress is considered to be a well-established correlate of criminal behavior.[13] For this study, a wide variety of potential stressors were assessed, including financial pressures, physical health concerns, interpersonal conflicts with family, friends, and colleagues (work and/or school), mental health issues, criminal and civil law issues, and substance abuse.[14]

---

13 Felson, R.B., Osgood, D.W., Horney, J. & Wiernik, C. (2012). Having a bad month: General versus specific effects of stress on crime. *Journal of Quantitative Criminology, 28,* 347-363 for a discussion of various theories describing the relationship between stress and crime.

14 See Appendix A.

The FBI recognizes that most (if not all) people in some way confront similar issues on a regular basis in their daily lives, and that most possess adequate personal resources, psychological resiliency, and coping skills to successfully navigate such challenges without resorting to violence. Therefore, the FBI focused on identifying stressors that appeared to have more than a minimal amount of adverse impact on that individual, and which were sufficiently significant to have been memorialized, shared, or otherwise noted in some way (e.g., in the active shooter's own writings, in conversation with family or friends, work files, court records). Given the fluid nature of some (although not all) of the stressors, the analysis was limited to the year preceding the attack.

The variables were treated as binary, that is, either the stressor was present or not, without regard for the number of separate circumstances giving rise to the stressor. So, an active shooter who had conflict with *one* family member and a shooter who had conflicts with *several* family members were both coded as "yes" for "conflict with other family members."

Overall, the data reflects that active shooters were typically experiencing multiple stressors (an average of 3.6 separate stressors) in the year before they attacked. For example, in the year before his attack, one active shooter was facing disciplinary action at school for abuse of a teacher, was himself abused and neglected at home, and had significant conflict with his peers. Another active shooter was under six separate stressors, including a recent arrest for drunk driving, accumulating significant debt, facing eviction, showing signs of both depression and anxiety, and experiencing both the criminal and civil law repercussions of an incident three months before the attack where he barricaded himself in a hotel room and the police were called.

The only stressor that applied to more than half the sample was mental health (62%, $n = 39$). Other stressors that were present in at least 20% of the sample were related to financial strain, employment, conflicts with friends and peers, marital problems, drug and alcohol abuse, other, conflict at school, and physical injury.

TABLE 1: STRESSORS

Stressors	Number	%
Mental health	39	62
Financial strain	31	49
Job related	22	35
Conflicts with friends/peers	18	29
Marital problems	17	27
Abuse of illicit drugs/alcohol	14	22
Other (e.g. caregiving responsibilities)	14	22
Conflict at school	14	22
Physical injury	13	21
Conflict with parents	11	18
Conflict with other family members	10	16
Sexual stress/frustration	8	13
Criminal problems	7	11
Civil problems	6	10
Death of friend/relative	4	6
None	1	2

MENTAL HEALTH

There are important and complex considerations regarding mental health, both because it is the most prevalent stressor and because of the common but erroneous inclination to assume that anyone who commits an active shooting must de facto be mentally ill. First, the *stressor* "mental health" is not synonymous with a *diagnosis* of mental illness. The stressor "mental health" indicates that the active shooter appeared to be struggling with (most commonly) depression, anxiety, paranoia, etc. in their daily life in the year before the attack. There may be complex interactions with other stressors that give rise to what may ultimately be transient manifestations of behaviors and moods that would not be sufficient to warrant a formal diagnosis of mental illness. In this context, it is exceedingly important to highlight that the FBI could only verify that 25% (*n* = 16) of the active shooters in Phase II were known to have been diagnosed by a mental health professional with a mental illness *of any kind* prior to the offense.[15] The FBI could not determine if a diagnosis had been given in 37% (*n* = 23) of cases.

Of the 16 cases where a diagnosis prior to the incident could be ascertained, 12 active shooters had a mood disorder; four were diagnosed with an anxiety disorder; three were diagnosed with a psychotic disorder; and two were diagnosed with a personality disorder. Finally, one active shooter was diagnosed with Autism spectrum disorder; one with a developmental disorder; and one was described as "other." Having a diagnosed mental illness was unsurprisingly related to a higher incidence of concurrent mental health stressors among active shooters.

Considerations

It is clear that a majority of active shooters experienced multiple stressors in their lives before the attack. While the active shooters' reactions to stressors were not measured by the FBI, what appears to be noteworthy and of importance to threat assessment professionals is the active shooters' ability to navigate conflict and resiliency (or lack thereof) in the face of challenges. Given the high prevalence of financial and job-related stressors as well as conflict with peers and partners, those in contact with a person of concern at his/her place of employment may have unique insights to inform a threat assessment.

In light of the very high lifetime prevalence of the symptoms of mental illness among the U.S. population, formally diagnosed mental illness is not a very specific predictor of violence of any type, let alone targeted violence.[16,17,18] Some studies indicate that nearly half of the U.S. population experiences symptoms of mental illness over their lifetime, with population estimates of the lifetime prevalence of diagnosable mental illness among U.S. adults at 46%, with 9% meeting the criteria for a personality disorder.[19,20] Therefore, absent specific evidence, careful consideration should be given to social and contextual factors that might interact with any mental health issue before concluding that an active shooting was "caused" by mental illness. In short, declarations that all active shooters must simply be mentally ill are misleading and unhelpful.

CONCERNING BEHAVIORS

Concerning behaviors are *observable* behaviors exhibited by the active shooter. For this study, a wide variety of concerning behaviors were considered, including those related to potential symptoms of a mental health disorder, interpersonal interactions, quality of the active shooter's thinking or communication, recklessness, violent media usage, changes in hygiene and weight, impulsivity, firearm behavior, and physical aggression.[21] Although these may be related to stressors in the active shooter's life, the focus here was not on the internal, subjective experience of

---

15   The number of documented, diagnosed mental illness may be the result of a number of factors, including those related to situational factors (access to health care) as well as those related to the study factors (access to mental health records).

16   Elbogen, E.B., & Johnson, S.C. (2009). The intricate link between violence and mental disorder. *Arch Gen Psychiatry,66(2),*152-161.

17   Glied, S.A., and Frank, R.G. (2014). Mental illness and violence: Lessons from the evidence. *American Journal of Public Health, 104,* e5-e6 doi:10.2015/AJPH.2013.301710

18   Monahan, J., Steadman, H. J., Silver, E., Applebaum, P.S., Clark Robbins, P., Mulvey, E. P., & Banks, S. (2001). Rethinking Risk Assessment: The MacArthur Study of Mental Disorder and Violence. Oxford, UK: Oxford University Press

19   Kessler, R.C., Berglund, P., Demler, O., Jin, R., Merikangas, K.R., Walters, E.E. Lifetime prevalence and age-of-onset distributions of DSM-IV disorders in the National Comorbidity Survey Replication. *Arch Gen Psychiatry.* 2005:62(6): 593-602.

20   Lenzweger, M.F., Lane, M.C., Loranger, A.W., Kessler, R.C., DSM-IV personality disorders in the National Comorbidity Survey Replication. *Biol Psychiatry*. 2007;62(6): 553-564.

21   See Appendix B.

the active shooter, but rather on what was *objectively knowable* to others. So, while the assessment of stressors is meant to provide insight into the active shooter's inner turmoil, the examination of concerning behaviors addresses a related but separate issue — the possibility of identifying active shooters before they attack by being alert for observable, concerning behaviors. The FBI looked for documented confirmation that someone noticed a facet of the shooter's behavior causing the person to feel a "more than minimal" degree of unease about the well-being and safety of those around the active shooter.

Before examining what behaviors were observable by others, it is useful to address the widespread perception that active shooters tend to be cut off from those around them. In general, the active shooters in Phase II were not completely isolated and had at least some social connection to another person. While most of the active shooters age 18 and older were single/never married (51%, $n = 28$) or separated/divorced (22%, $n = 12$) at the time of the attack, the majority did live with someone else (68%, $n = 43$). This percentage was slightly less (64%, $n = 35$) for only those active shooters who were 18 years or older. Most had significant in-person social interactions with at least one other person in the year before the attack (86%, $n = 54$), and more than a quarter of them had significant online interactions with another person within a year of the attack (27%, $n = 17$). All active shooters either: a) lived with someone, or b) had significant in-person or online social interactions.

Since the observation of concerning behaviors offers the opportunity for intervention prior to the attack, this study examines not only what was observed, but when the observations were made, who made them, and what if anything the person(s) did with regard to these observations. To better serve threat assessment teams, mental health professionals, community resources, and law enforcement officials, the FBI expanded the inquiry to capture behaviors that may have been observed at any point (in many cases beyond one year) before the attack.

Overall, active shooters showed concerning behaviors in multiple ways, with an average of 4.7 concerning behaviors per active shooter. Behaviors observed in more than half of the sample were related to the shooter's mental health[22], interpersonal interactions, leakage (the communication to a third-party of an intent to harm someone, discussed with threats in a separate section), and the quality of the active shooter's thinking or communication.

Of note was that contextually inappropriate firearms behavior was noted in approximately one fifth of the active shooters, while drug and alcohol abuse figured even less prominently in the sample (for the purposes of the study, contextually inappropriate firearms behavior was defined as interest in or use of firearms that appeared unusual given the active shooter's background and experience with firearms).

TABLE 2: CONCERNING BEHAVIORS

Concerning Behavior	Number	%
Mental health	39	62
Interpersonal interactions	36	57
Leakage	35	56
Quality of thinking or communication	34	54
Work performance*	11	46
School performance**	5	42
Threats/confrontations	22	35
Anger	21	33
Physical aggression	21	33

Continues on next page

22   Thirty-nine active shooters were experiencing a mental health stressor, and 39 active shooters showed concerning behaviors related to mental health, but the same 39 active shooters did not appear in each category; there were five active shooters who had a mental health stressor but who did not show a concerning behavior, and five other active shooters who showed a mental health-related concerning behavior but for whom there was no evidence of mental health stress.

Risk-taking	13	21
Firearm behavior	13	21
Violent media usage	12	19
Weight/eating	8	13
Drug abuse	8	13
Impulsivity	7	11
Alcohol abuse	6	10
Physical health	6	10
Other (e.g. idolizing criminals)	5	8
Sexual behavior	4	6
Quality of sleep	3	5
Hygiene/appearance	2	3

* Based on the 24 active shooters who were employed at the time of the offense
** Based on the 12 active shooters who were students at the time of the offense

When Were the Concerning Behaviors Noticed?

Since the overwhelming majority of active shooters (all but three) displayed at least two concerning behaviors, there are a number of different ways to assess the data. One way is to examine the data by active shooter and to observe the first instance that any concerning behavior was noticed (this could not be determined for three active shooters). Figure 9 shows this data and helps frame the longest time before a shooting during which others were concerned about the active shooter's behavior.

First Instance of Concerning Behavior
(*N* = 63)
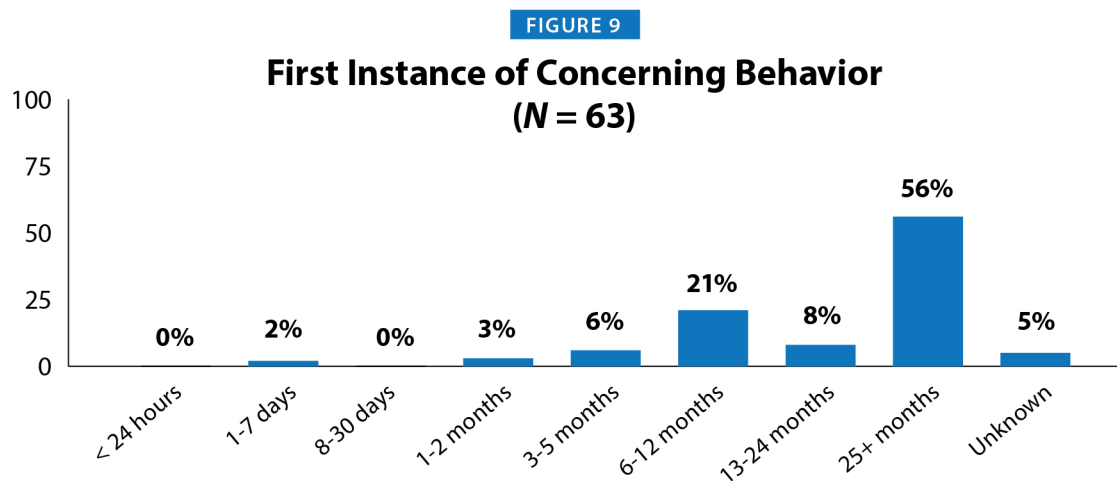
*Does not sum to 100% due to rounding.

Again, this chart shows the first instance of *any* concerning behavior, and it should be kept in mind that this behavior might not have been the type that by *itself* would cause a reasonable person to be alarmed or to report it to others. For example, a co-worker who noticed that an active shooter had more than the normal amount of conflict with a supervisor might be unlikely to take any action. Perhaps only after an attack and with the benefit of hindsight would this singular behavior be considered to be — in and of itself — troubling or concerning. Yet, on average, each active shooter displayed *four to five* concerning behaviors over time. While it may only be the interaction and cumulative effect of these behaviors that would cause alarm, early recognition and detection of growing or interrelated problems may help to mitigate the potential for violence.

In What Way Were the Concerning Behaviors Noticed?

Concerning behaviors came to the attention to others in a variety of ways, with some far more common than others. The most prevalent way in which concerning behaviors were noticed was verbal communication by the active shooter (95%, $n = 60$), followed by observing the physical actions of the active shooter (86%, $n = 54$), written communication (27%, $n = 17$), and finally instances where concerning behavior was displayed online (16%, $n = 10$). A large majority of active shooters (89%, $n = 56$) demonstrated concerning behaviors that were noticed in multiple ways.

Who Noticed the Concerning Behaviors?

At least one person noticed a concerning behavior in *every* active shooter's life, and on average, people from three different groups noticed concerning behaviors for each active shooter. As shown below, classmates (for those who were students), partners (for those in relationships), family members and friends most frequently noticed concerning behavior, followed by co-workers, other, and law enforcement:

TABLE 3: WHO NOTICED CONCERNING BEHAVIORS

Who Noticed	Number	%
Schoolmate*	11	92
Spouse/domestic partner**	13	87
Teacher/school staff*	9	75
Family member	43	68
Friend	32	51
Co-worker	25	40
Other (e.g. neighbors)	23	37
Law enforcement	16	25
Online individual	6	10
Religious mentor	3	5

* Percentage calculated only with those active shooters who were students at the time of the offense
** Percentage calculated only with those active shooters who were in a relationship at the time of the offense

What, If Anything, Did the Concerned Party Do?

If the person recognizes behaviors as problematic but takes no action, the opportunity for intervention is missed. Whether and how a person responds to an active shooter's concerning behavior is likely influenced by a host of personal and situational factors (e.g., whether the behavior is threatening to the observer or others, the relationship of the observer and active shooter, avenues for anonymous reporting, and/or confidence in authorities or others to address the behavior).

In this study, even in cases where an active shooter displayed a variety of concerning behaviors that might indicate an intent to act violently, the observer(s) of that information did not necessarily pass it along to anyone else. As shown above, the people most likely to notice concerning behaviors were those who knew the active shooter best — family, friends and classmates. For the very reason they are the people most likely to take note of concerning behaviors, they are also people who may feel constrained from acting on these concerns because of loyalty, disbelief, and/or fear of the consequences.[23]

---

23   Borum, R. (2013). Informing Lone-Offender Investigations. *Criminology & Public Policy,* 12(1), 103-112.

Again, keeping in mind that active shooters displayed multiple concerning behaviors and those who observed these behaviors might have responded in different ways to each, the most common response was to communicate directly to the active shooter (83%, $n = 52$) or do nothing (54%, $n = 34$). Thus, in many instances, the concern stayed between the person who noticed the behavior and the active shooter.

The next most common responses were: report the active shooter to a non-law enforcement authority (51%, $n = 32$); discuss the concerning behavior with a friend or family member (49%, $n = 31$); and, report the active shooter to law enforcement authority (41%, $n = 26$).

Considerations

The analysis above is not intended to, nor could it, encompass the innumerable ways in which the observer of a concerning behavior might react. Nor does it suggest that every concerning behavior warrants assertive intervention; many of the concerning behaviors that registered with others likely would not have presaged deadly violence to a reasonable person. The FBI is aware that in retrospect certain facts may take on a heightened degree of significance that may not have been clear at the time.

Nevertheless, understanding that there are often opportunities before a shooting to recognize concerning behaviors that may suggest progression toward violence, the FBI is highlighting the most common behaviors displayed in the sample. There is no single warning sign, checklist, or algorithm for assessing behaviors that identifies a prospective active shooter. Rather, there appears to be a complex combination of behaviors and interactions with bystanders that may often occur in the days, weeks, and months leading up to an attack. Early recognition *and* reporting of concerning behaviors to law enforcement or threat assessment professionals may initiate important opportunities for mitigation.

PRIMARY GRIEVANCE

A grievance is defined for this study as the cause of the active shooter's distress or resentment; a perception — not necessarily based in reality — of having been wronged or treated unfairly or inappropriately.[24,25,26] More than a typical feeling of resentment or passing anger, a grievance often results in a grossly distorted preoccupation with a sense of injustice, like an injury that fails to heal. These thoughts can saturate a person's thinking and foster a pervasive sense of imbalance between self-image and the (real or perceived) humiliation. This nagging sense of unfairness can spark an overwhelming desire to "right the wrong" and achieve a measure of satisfaction and/or revenge. In some cases, an active shooter might have what appeared to be multiple grievances but, where possible, the FBI sought to determine the primary grievance. Based on a review of the academic literature and the facts of the cases themselves, the FBI identified eight categories of grievances, with an additional category of "other" for grievances that were entirely idiosyncratic.

As shown in the following table, the FBI could not identify a primary grievance for 13 (21%) of the active shooters, either because they did not have one or because there was insufficient evidence to determine whether one existed. While it may be particularly difficult to understand the motivation(s) for attacks that do not appear to be based on identifiable grievances, these active shooters still displayed concerning behaviors, were under identifiable stressors, and engaged in planning and preparation activities. For example, for the active shooters where no grievance could be identified, all had at least two behaviors (with an average of 5.4 behaviors) that were noted to be concerning by others.

24   Calhoun, T., & Weston, S., (2003).
25   Fein, R., & Vossekuil, B. (1999).
26   Vossekuil, B., Fein, R., Reddy, M., Borum, R., & Modzeleski, W. (2004).

The majority (79%, *n* = 50) of the active shooters did appear to be acting in accord with a grievance of some kind. Of course, the grievance itself may not have been reasonable or even grounded in reality, but it appeared to serve as the rationale for the eventual attack, giving a sense of purpose to the shooter. Most of these grievances seem to have originated in response to some specific action taken regarding the active shooter. Whether interpersonal, employment, governmental, academic, or financial, these actions were (or were perceived to be) directed against the active shooter personally. In contrast, grievances driven by more global or broad considerations — such as ideology or hatred of a group — account for less than 7% of the overall cases. In general then, active shooters harbored grievances that were distinctly personal to them and the circumstances of their daily lives.

TABLE 4: PRIMARY GRIEVANCE

Primary Grievance	Number	%
Adverse interpersonal action against the shooter	21	33
Adverse employment action against the shooter	10	16
Other (e.g. general hatred of others)	6	10
Adverse governmental action against the shooter	3	5
Adverse academic action against the shooter	2	3
Adverse financial action against the shooter	2	3
Domestic	2	3
Hate crime	2	3
Ideology/extremism	2	3
Unknown	13	21

Precipitating Events

Of the 50 active shooters who had an identifiable grievance, nearly half of them experienced a precipitating or triggering event related to the grievance (44%, *n* = 22). Seven active shooters (14%) did not experience a precipitating event, and the FBI could not determine whether the remaining 21 (42%) did. Precipitating events generally occurred close in time to the shooting and included circumstances such as an adverse ruling in a legal matter, romantic rejection, and the loss of a job.

These precipitating events were of more consequence in the timing of the attack, and while they appear to have accelerated the active shooter's movement on the trajectory to violence, they did not by themselves appear to set the course.

Considerations

Of course, many people have grievances and never act violently. What caused the active shooters in this study to act the way they did cannot be explained simply by the presence of a grievance. There was likely the interaction of a variety of operational considerations and psychological stressors that eventually crystallized in the decision to ignore non-violent options and choose to attack. However, the types of grievances most commonly experienced by the active shooters in this study may be important considerations for the many threat assessment teams and law enforcement professionals who work each day to assess a subject's progression along the pathway to violence.

TARGETING

For this study, a target is defined as a person or group of people who were *identifiable before the shooting occurred* and whom the active shooter intended to attack. It was not necessary that the active shooter knew the target by name; intending to attack a person holding a position at or affiliated with a business, educational facility, or in a governmental agency sufficed. The target could be a group, so long as members of that group could have been identified prior to the attack.

In cases where the victims could not reasonably have been identified prior to the shooting, the active shooter was deemed to have selected the victims at random. While there is *some* element of selection in any attack where there is more than one potential victim (unless the active shooter literally does not aim at all), the FBI considered victims to be random where there was: 1) no known connection between the active shooter and the victims, and 2) the victims were not specifically linked to the active shooter's grievance.

In many cases, there was a mix of targeted and random victims in the same shooting. The typical circumstance occurred when an active shooter went to a location with targets in mind and also shot others who were at the same location, either because they presented some obstacle in the attack or for reasons that could not be identified.

The overall numbers for targeted and random victims are listed below:

FIGURE 10

RANDOM VICTIMS
(37%, *n* = 23)

BOTH RANDOM
AND TARGETED
VICTIMS
(37%, *n* = 23)

TARGETED VICTIMS
(27%, *n* = 17)
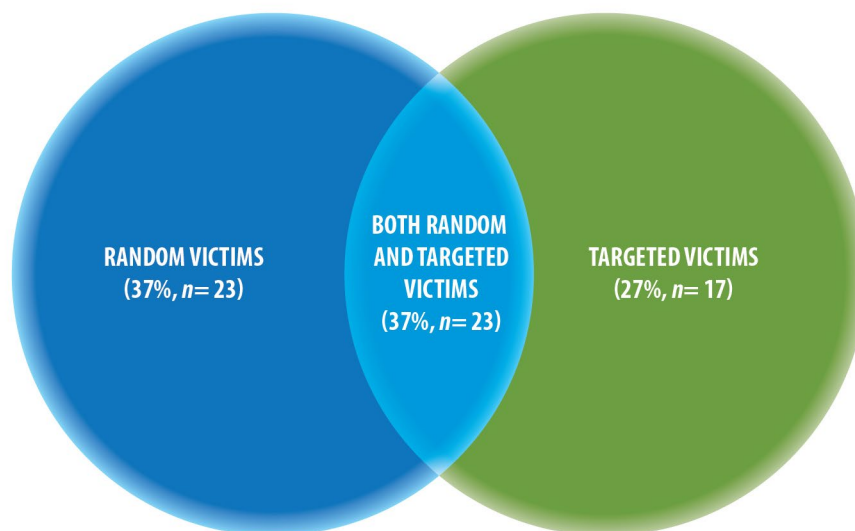
*Does not sum to 100% due to rounding.

Considerations

While approximately one-third of active shooters in this sample victimized only random members of the public, most active shooters arrive at a targeted site with a specific person or persons in mind. Awareness of targeting behaviors can provide valuable insight for threat assessment professionals. Relatedly, the FBI has observed that when an active shooter's grievance generalizes — that is, expands beyond a desire to punish a specific individual to a desire to punish an institution or community — this should be considered to be progression along a trajectory towards violence and ultimately a threat-enhancing characteristic.

SUICIDE: IDEATION AND ATTEMPTS

For this study, "suicidal ideation" was defined as thinking about or planning suicide, while "suicide attempt" was defined as a non-fatal, self-directed behavior with the intent to die, regardless of whether the behavior ultimately results in an injury of any kind. Although these definitions are broad, the FBI concluded that an active shooter had suicidal ideation or engaged in a suicide attempt only when based on specific, non-trivial evidence.

Nearly half of the active shooters had suicidal ideation or engaged in suicide-related behaviors at some time prior to the attack (48%, $n = 30$), while five active shooters (8%) displayed no such behaviors (the status of the remaining 28 active shooters was unknown due to a lack of sufficient evidence to make a reasonable determination).

An overwhelming majority of the 30 suicidal active shooters showed signs of suicidal ideation (90%, $n = 27$), and seven made actual suicide attempts (23%). Nearly three-quarters (70%, $n = 21$) of these behaviors occurred within one year of the shooting.

Considerations

The high levels[27] of pre-attack suicidal ideation — with many appearing within 12 months of the attack — are noteworthy as they represent an opportunity for intervention. If suicidal ideation or attempts in particular are observed by others, reframing bystander awareness within the context of a mass casualty event may help to emphasize the importance of telling an authority figure and getting help for the suicidal person. Without stigmatizing those who struggle with thoughts of self-harm, researchers and practitioners must continue to explore those active shooters who combined suicide with externalized aggression (including homicidal violence) and identify the concurrent behaviors that reflect this shift.

CONCERNING COMMUNICATIONS

One useful way to analyze concerning communications is to divide them into two categories: *threats/confrontations* and *leakage of intent.*

Threats/Confrontations

Threats are *direct communications to a target* of intent to harm and may be delivered in person or by other means (e.g., text, email, telephone). For this study, threats need not be verbalized or written; the FBI considered in-person confrontations that were intended to intimidate or cause safety concerns for the target as falling under the category of threats as well.

More than half of the 40 active shooters who had a target made threats or had a prior confrontation (55%, $n = 22$). When threats or confrontations occurred, they were almost always in person (95%, $n = 21$) and only infrequently in writing or electronically (14%, $n = 3$). Two active shooters made threats both in person and in writing/electronically.

Leakage

Leakage occurs when a person intentionally or unintentionally reveals clues to a *third-party* about feelings, thoughts, fantasies, attitudes or intentions that may signal the intent to commit a violent act.[28] Indirect threats of harm are included as leakage, but so are less obvious, subtle threats, innuendo about a desire to commit a violent attack, or boasts about the ability to harm others. Leakage can be found not only in verbal communications, but

---

27   The National Survey on Drug Use and Health (2015) shows that in 2015: 4% of adults had serious thoughts of suicide, 1.1% made serious plans, and 0.6% attempted suicide (https://www.samhsa.gov/data/sites/default/files/NSDUH-DR-FFR3-2015/NSDUH-DR-FFR3-2015.htm)

28   Meloy, J. R. & O'Toole, M. E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences and the Law, 29,* 513-527

also in writings (e.g., journals, school assignments, artwork, poetry) and in online interactions (e.g., blogs, tweets, texts, video postings). Prior research has shown that leakage of intent to commit violence is common before attacks perpetrated by both adolescents and adults, but is more common among adolescents.[29,30,31]

Here, too, leakage was prevalent, with over half of the active shooters leaking intent to commit violence (56%, n = 35). In the Phase II sample, 88% (n = 7) of those active shooters age 17 and younger leaked intent to commit violence, while 51% (n = 28) of adult active shooters leaked their intent. The leaked intent to commit violence was not always directed at the eventual victims of the shootings; in some cases what was communicated was a more general goal of doing harm to others, apparently without a particular person or group in mind. For example, one active shooter talked to a clerk at a gas station about killing "a family" and another expressed interest in becoming a sniper like a character featured in *The Turner Diaries*. In 16 of the 40 cases (40%) where the active shooter had a target, however, the leaked intent to act violently was directly pertaining to that target. In these cases, the leakage was generally a statement to a third-party of the intent to specifically harm the target.

Legacy Tokens

Finally, the FBI considered whether or not an active shooter had constructed a "legacy token" which has been defined as a communication prepared by the offender to claim credit for the attack and articulate the motives underlying the shooting.[32] Examples of legacy tokens include manifestos, videos, social media postings, or other communications deliberately created by the shooter and delivered or staged for discovery by others, usually near in time to the shooting. In 30% (n = 19) of the cases included in this study, the active shooter created a legacy token prior to the attack.

Considerations

Although more than half of the active shooters with pre-attack targets made threats (n = 22), in the majority (65%) of the overall cases no threats were made to a target, and the FBI cautions that the absence of a direct threat should not be falsely reassuring to those assessing the potential for violence raised by other circumstances and factors. Nor should the presence of a threat be considered conclusive. There is a significant amount of research and experience to demonstrate that direct threats are not correlated to a subsequent act of targeted violence.[33,34,35,36,37,38]

It is important to highlight that in this Phase II study the overwhelming majority of direct threats were verbally delivered by the offender to a future victim. Only a very small percentage of threats were communicated via writing or electronically. In many ways this is not surprising. Written, directly communicated threats against a target (e.g., "I'm going to shoot and kill everyone here on Tuesday") often spark a predictable response that includes a heightened law enforcement presence and the enhancement of security barriers. These responses are highly undesirable to an offender planning an active shooting.[39] Verbal threats issued directly to another person appear to be far more common among the active shooters included in the Phase II study.

29   Hemple, A., Meloy, J.R., & Richards, T. (1999). Offender and offense characteristics of a nonrandom sample of mass murderers. *Journal of the American Academy of Psychiatry and the Law, 27,* 213-225. Meloy, J.R., Hoffman, J., Guldimann, A., & James, D. (2011). The role of warning behaviors in threat assessment: An exploration and suggested typology. Behavioral Sciences and the Law, 30, 256-279.

30   Meloy, J. R. & O'Toole, M. E. (2011).

31   Meloy, J.R., Hoffman, J., Guldimann, A., & James, D. (2011). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences and the Law, 30,* 256-279.

32   Simons, A., & Tunkel, R. (2014). The assessment of anonymous threatening communications. In J.R. Meloy & J. Hoffman (Eds.), *International handbook of threat assessment* (pp. 195-213). New York: Oxford University Press.

33   Borum, R., Fein, R. Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence. *Behavioral Sciences and the Law*, 17, 323-337.

34   Calhoun, F. (1998). Hunters and howlers: *Threats and violence against federal judicial officials in the United States, 1789-1993*. Arlington, VA: US Marshals Service.

35   Calhoun T. & Weston, S. (2003).

36   Dietz, P., Matthews, D., Martell, D., Stewart, T., Hrouda, D., & Warren, J. (1991a). Threatening and otherwise inappropriate letters to members of the United States Congress. *Journal of Forensic Sciences, 36,* 1445-1468.

37   Dietz, P., Matthews, D., Van Duyne, C., Martell, D., Parry, C., Stewart, T., et al. (1991b). Threatening and otherwise inappropriate letters to Hollywood celebrities. *Journal of Forensic Sciences, 36,* 185-209.

38   Meloy, J.R. (2000). *Violence risk and threat assessment*. San Diego: Specialized Training Services.

39   Simons A. & Tunkel, R. (2014)

Whether verbal or written, concerning communications are challenging as those on the receiving end must assess sometimes ominously vague or nebulous verbiage. Such confusion can create doubt in the listener's mind as to the communicator's true intent toward violence.[40] As law enforcement agencies continue to remind bystanders if they "see something, say something" it becomes relevant to use this data (particularly regarding leakage behaviors) to lower the internal threshold for reporting, even in the face of ambiguous language. It is troubling to note that no bystanders reported instances of leakage to law enforcement, perhaps out of a fear of overreacting or perhaps due to a lack of understanding as to what law enforcement's response would be. This suggests that more robust efforts need to be made to educate bystanders (especially students and adolescents) on the nature of leakage and its potential significance.

Limitations

The findings presented in this report reflect a thorough and careful review of the data derived almost exclusively from law enforcement records. Nevertheless, there are limitations to the study which should be kept in mind before drawing any conclusions based on the findings.

First, the Phase I study on which the present analysis is based included only a specific type of event. Shootings must have been (a) in progress in a public place and (b) law enforcement personnel and/or citizens had the potential to affect the outcome of the event based on their responses. The FBI acknowledges there is an inherent element of subjectivity in deciding whether a case meets the study criteria. Moreover, while every effort was made to find all cases between 2000 and 2013 which met the definition, it is possible that cases which should have been included in the study were not identified. Overall, as with the Phase I study, the incidents included in the Phase II study were not intended to and did not comprise all gun-related violence or mass or public shootings occurring between 2000 and 2013.

Second, although the FBI took a cautious approach in answering protocol questions and limited speculation by relying on identifiable data, there was some degree of subjectivity in evaluating which of the original 160 cases had sufficient data to warrant inclusion in the study.

Third, while reliance on official law enforcement investigative files was reasonable based on the study's objectives, the level of detail contained in these files was not uniform throughout and the FBI was not able to definitively answer all protocol questions for all subjects.

This is a purely descriptive study. With the exception of mental health and suicidal behaviors, the FBI did not make any comparisons to the general population or to criminals who were not active shooters. Therefore, we cannot postulate on the probability as to whether some of the behaviors and characteristics seen here would also have been seen in other populations. Furthermore, the FBI cautions readers to not treat the observed behaviors as having predictive value in determining if a person will become violent or not, as the findings and observations presented herein are not a "checklist" but instead are offered to promote awareness among potential bystanders and for consideration in the context of a thorough, holistic threat assessment by trained professionals. Future research may benefit from comparisons between those who completed active shooting attacks and those who planned to attack but were disrupted prior to the offense, and/or in comparison to those individuals who may have displayed concerning behaviors but had no true intent to commit an act of targeted violence.

---

40   The FBI noted that there were four cases where threats were made and someone notified law enforcement (out of 22 cases where a threat was made, or 14%)

Conclusion

The ability to utilize case files (as compared to open-source documents) allowed the FBI to carefully examine both the internal issues experienced and the behaviors demonstrated by active shooters in the weeks and months preceding their attacks. What emerges is a complex and troubling picture of individuals who fail to successfully navigate multiple stressors in their lives while concurrently displaying four to five observable, concerning behaviors, engaging in planning and preparation, and frequently communicating threats or leaking indications of an intent to attack. As an active shooter progresses on a trajectory towards violence, these observable behaviors may represent critical opportunities for detection and disruption.

The information contained in this Phase II report can be utilized by myriad safety stakeholders. The successful prevention of an active shooting frequently depends on the collective and collaborative engagement of varied community members: law enforcement officials, teachers, mental health care professionals, family members, threat assessment professionals, friends, social workers, school resource officers…and many others. A shared awareness of the common observable behaviors demonstrated by the active shooters in this study may help to prompt inquiries and focus assessments at every level of contact and every stage of intervention.

While many dedicated professionals work to thwart active shootings, the FBI suspects that future active shooters themselves are looking for ways to avoid detection and maximize damage as they plan and prepare for their acts of violence. The prevention of these future attacks will depend on our ability to remain agile and recognize evolving pre-attack behaviors. To that end, the FBI continues to study active shooters to better inform all safety stakeholders and to support the development of sound threat mitigation strategies.

As tragically seen from current events, active shootings continue to impact our nation. The FBI hopes that the information contained in this Phase II study will help in efforts to promote safety across all communities.

Appendix A:

STRESSORS

Abuse of illicit drugs or alcohol: difficulties caused by the effects of drugs/alcohol and/or frustrations related to obtaining these substances.

Civil legal problems: being party to a non-trivial lawsuit or administrative action.

Conflict with friends/peers: general tension in the relationship beyond what is typical for the active shooter's age or specific instances of serious and ongoing disagreement.

Conflict with other family members: general tension in the relationship beyond what is typical for the active shooter's age, or specific instances of serious and ongoing disagreement.

Conflict with parents: general tension in the relationship beyond what is typical for the active shooter's age, or specific instances of serious and ongoing disagreement.

Criminal legal problems: arrests, convictions, probation, parole.

Death of friend/relative: death that caused emotional or psychological distress.

Financial strain: related to job loss, debt collection, potential or actual eviction, inability to pay normal and usual daily bills.

Job-related problems: ongoing conflicts with co-workers or management, pervasive poor performance evaluations, or disputes over pay or leave.

Marital problems/conflict with intimate partner(s)/divorce or separation: difficulties in the relationship that were a consistent source of psychological distress and/or which did or were likely to lead to the end of the relationship or the desire to end the relationship.

Mental health problems: symptoms of anxiety, depression, paranoia, or other mental health concerns that have a negative effect on daily functioning and/or relationships.

Other: any other circumstance causing physical, psychological, or emotional difficulties that interfere in a non-trivial way with normal functioning in daily life.

Physical injury: physical condition/injury that significantly interfered with or restricted normal and usual activities.

School-related problems: conflicts with teachers and staff that go beyond single instances of minor discipline; pervasive frustration with academic work; inability to follow school rules.

Sexual stress/frustration: pronounced and ongoing inability to establish a desired sexual relationship.

Appendix B:

CONCERNING BEHAVIORS

Amount or quality of sleep: unusual sleep patterns or noticeable changes in sleep patterns.

Anger: inappropriate displays of aggressive attitude/temper.

Change, escalation, or contextually inappropriate firearms behavior: interest in or use of firearms that appears unusual given the active shooter's background and experience with firearms.

Changes in weight or eating habits: significant weight loss or gain related to eating habits.

Hygiene or personal appearance: noticeable and/or surprising changes in appearance or hygiene practices.

Impulsivity: actions that in context appear to have been taken without usual care or forethought.

Interpersonal interactions: more than the usual amount of discord in ongoing relationships with family, friends, or colleagues.

Leakage: communication to a third-party of the intent to harm another person.

Mental health: indications of depression, anxiety, paranoia or other mental health concerns.

Other: any behavior not otherwise captured in above categories that causes more than a minimal amount of worry in the observer.

Physical aggression: inappropriate use of force; use of force beyond what was usual in the circumstances.

Physical health: significant changes in physical well-being beyond minor injuries and ailments.

Quality of thinking or communication: indications of confused or irrational thought processes.

Risk-taking: actions that show more than a usual disregard for significant negative consequences.

School performance: appreciable decrease in academic performance; unexplained or unusual absences.

Sexual behavior: pronounced increases or decreases in sexual interest or practices.

Threats/Confrontations: direct communications to a target of intent to harm. May be delivered in person or by other means (e.g., text, email, telephone).

Use of illicit drugs or illicit use of prescription drugs: sudden and/ recent use or change in use of drugs; use beyond social norms that interferes with the activities of daily life.

Use or abuse of alcohol: sudden and/or recent use or changes in use of alcohol; use beyond social norms that interferes with the activities of daily life.

Violent media usage: more than a usual age-appropriate interest in visual or aural depictions of violence.

Work performance: appreciable decrease in job performance; unexplained or unusual absences.

U.S. Department of Justice
Federal Bureau of Investigation

PREVENTATIVE MEASURES

BUILDING THREAT ASSESSMENT TEAMS IN SCHOOLS:

NATIONWIDE BEST PRACTICES

UNITED STATES SECRET SERVICE

ENHANCING SCHOOL SAFETY USING A THREAT ASSESSMENT MODEL

An Operational Guide for Preventing Targeted School Violence

National Threat Assessment Center
July 2018

U.S. SECRET SERVICE SCHOOL SAFETY RESEARCH

Over the last 20 years, the U.S. Secret Service National Threat Assessment Center (NTAC) has conducted research, training, and consultation on threat assessment and the prevention of various forms of targeted violence. Following the tragedy at Columbine High School in April 1999, the Secret Service partnered with the Department of Education on two studies related to school safety. Published in 2002, the *Safe School Initiative (SSI)* examined 37 incidents of targeted violence that occurred at elementary and secondary schools to analyze the thinking and behavior of students who commit these attacks. The report, and accompanying guide, served as the impetus for establishing threat assessment programs in schools. In 2008, the agencies released the Bystander Study, a report that explored a key SSI finding that prior to most attacks, other students knew of the attackers' plans, yet most did not report it to an adult. The report highlighted the importance of creating safe school climates in which students are empowered to share their concerns. Since then, NTAC has continued to provide and update training to schools, law enforcement, and others on threat assessment and prevention practices.

U.S. SECRET SERVICE'S LATEST INITIATIVE REGARDING SCHOOL SAFETY

The tragic events of the February 14, 2018 shooting at Marjory Stoneman Douglas High School in Parkland, Florida, and the May 18, 2018 shooting at Santa Fe High School in Santa Fe, Texas, demonstrated the ongoing need to provide leadership in preventing future school attacks. As such, the U.S. Secret Service, along with many of our partners, have redoubled our efforts and are poised to continue enhancing school safety. As part of these efforts, NTAC created an operational guide that provides actionable steps that schools can take to develop comprehensive targeted violence prevention plans for conducting threat assessments in schools. The guide, titled *Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence,* is available on the U.S. Secret Service website. A condensed overview is outlined on the following page.

KEY CONSIDERATIONS

- In conjunction with physical security and emergency management, a threat assessment process is an effective component to ensuring the safety and security of our nation's schools.
- Threat assessment procedures recognize that students engage in a continuum of concerning behaviors, the vast majority of which will be non-threatening and non-violent, but may still require intervention.
- The threshold for intervention should be relatively low so that schools can identify students in distress before their behavior escalates to the level of eliciting concerns about safety.
- Everyone has a role to play in preventing school violence and creating safe school climates. Students should feel empowered to come forward without fear of reprisal. Faculty and staff should take all incoming reports seriously, and assess any information regarding concerning behavior or statements.

Additional Resources: The full guide provides information and links to additional resources that can help schools create threat assessment teams, establish reporting mechanisms, train stakeholders, and promote safe school climates.

CREATING A TARGETED VIOLENCE PREVENTION PLAN

The goal of a threat assessment is to identify students of concern, assess their risk for engaging in violence or other harmful activities, and identify intervention strategies to manage that risk. This process begins with establishing a comprehensive targeted violence prevention plan that requires schools to:

Step 1: **Establish a multidisciplinary threat assessment team** of school personnel including faculty, staff, administrators, coaches, and available school resource officers who will direct, manage, and document the threat assessment process.

Step 2: **Define behaviors,** including those that are prohibited and should trigger immediate intervention (e.g., threats, violent acts, and weapons on campus) and other concerning behaviors that require a threat assessment.

Step 3: **Establish and provide training on a central reporting system** such as an online form on the school website, email address, phone number, smartphone application, or other mechanisms. Ensure that it provides anonymity to those reporting concerns and is monitored by personnel who will follow-up on all reports.

Step 4: **Determine the threshold for law enforcement intervention,** especially if there is a safety risk.

Step 5: **Establish threat assessment procedures** that include practices for maintaining documentation, identifying sources of information, reviewing records, and conducting interviews. Procedures should include the following investigative themes to guide the assessment process:
- Motive: What motivated the student to engage in the behavior of concern? What is the student trying to solve?
- Communications: Have there been concerning, unusual, threatening, or violent communications? Are there communications about thoughts of suicide, hopelessness, or information relevant to the other investigative themes?
- Inappropriate Interests: Does the student have inappropriate interests in weapons, school attacks or attackers, mass attacks, other violence? Is there a fixation on an issue or a person?
- Weapons Access: Is there access to weapons? Is there evidence of manufactured explosives or incendiary devices?
- Stressors: Have there been any recent setbacks, losses, or challenges? How is the student coping with stressors?
- Emotional and Developmental Issues: Is the student dealing with mental health issues or developmental disabilities? Is the student's behavior a product of those issues? What resources does the student need?
- Desperation or Despair: Has the student felt hopeless, desperate, or like they are out of options?
- Violence as an Option: Does the student think that violence is a way to solve a problem? Have they in the past?
- Concerned Others: Has the student's behavior elicited concern? Was the concern related to safety?
- Capacity: Is the student organized enough to plan and execute an attack? Does the student have the resources?
- Planning: Has the student initiated an attack plan, researched tactics, selected targets, or practiced with a weapon?
- Consistency: Are the student's statements consistent with his or her actions or what others observe? If not, why?
- Protective Factors: Are there positive and prosocial influences in the student's life? Does the student have a positive and trusting relationship with an adult at school? Does the student feel emotionally connected to other students?

Step 6: **Develop risk management options** to enact once an assessment is complete. Create individualized management plans to mitigate identified risks. Notify law enforcement immediately if the student is thinking about an attack, ensure the safety of potential targets, create a situation less prone to violence, redirect the student's motive, and reduce the effect of stressors.

Step 7: **Create and promote a safe school climate** built on a culture of safety, respect, trust, and emotional support. Encourage communication, intervene in conflicts and bullying, and empower students to share their concerns.

Step 8: **Provide training for all stakeholders,** including school personnel, students, parents, and law enforcement.

ENHANCING SCHOOL SAFETY
USING A THREAT ASSESSMENT MODEL

An Operational Guide for
Preventing Targeted School Violence

U.S. Department of
Homeland Security

**United States
Secret Service**

National Threat Assessment Center
July 2018

This guide was prepared by the staff of the
U.S. Secret Service National Threat Assessment Center (NTAC)

Lina Alathari, Ph.D.
Chief

Ashley Blair, M.A.
Social Science Research Specialist

Catherine Camilletti, Ph.D.
Social Science Research Specialist

Steven Driscoll, M.Ed.
Social Science Research Specialist

Diana Drysdale, M.A.
Lead Social Science Research Specialist

Jeffrey McGarry, M.A.
Social Science Research Specialist

Amanda Snook, Ph.D.
Social Science Research Specialist

CONTENTS

MESSAGE FROM THE DIRECTOR

Since the creation of the U.S. Secret Service in 1865, the agency has evolved to meet changing mission demands and growing threats in our nation. To ensure we remain on the forefront, the U.S. Secret Service's National Threat Assessment Center (NTAC) was created in 1998 to provide guidance and training on threat assessment both within the U.S. Secret Service and to others with criminal justice and public safety responsibilities. Today, the highly skilled men and women of the U. S. Secret Service lead the field of threat assessment by conducting research on acts of targeted violence and providing training using the agency's established threat assessment model for prevention.

Our agency is dedicated to expanding research and understanding of targeted violence, including those that impact our nation's schools. Since the creation of the U.S. Secret Service's NTAC, we have provided 450 in-depth trainings on the prevention of targeted school violence to over 93,000 attendees including school administrators, teachers, counselors, mental health professionals, school resource officers, and other public safety partners. Our agency, through our local U.S. Secret Service field offices, continues to coordinate and provide this training to our community partners.

The tragic events of the February 14, 2018 shooting at Marjory Stoneman Douglas High School in Parkland, Florida, and the May 18, 2018 shooting at Santa Fe High School in Santa Fe, Texas, demonstrated the ongoing need to provide leadership in preventing future school attacks. As such, the U.S. Secret Service, along with many of our partners,

have redoubled our efforts and are poised to continue enhancing school safety. Keeping our school children safe requires the shared commitment from states, school boards, and communities with the ability to dedicate resources to this critical issue. In the wake of these tragedies, the U.S. Secret Service has launched an initiative to provide updated research and guidance to school personnel, law enforcement, and other public safety partners on the prevention of school-based violence. I am pleased to release this operational guide, *Enhancing School Safety Using a Threat Assessment Model*, as the first phase of this initiative.

As we have seen in recent months, the pain of each act of targeted violence in our nation's schools has had a powerful impact on all. With the creation and distribution of this operational guide, the U.S. Secret Service sets a path forward for sustainable practices to keep our children safe, extending our expertise in the field of threat assessments to provide school officials, law enforcement personnel, and other public safety professionals with guidance on "how to" create a Targeted Violence Prevention Plan. This guide will serve as an important contribution to our partners on the Federal Commission on School Safety - the Department of Homeland Security, the Department of Education, the Department of Health and Human Services and the Office of the Attorney General. I am proud of the continued efforts of the U.S. Secret Service, and we remain committed to the prevention of targeted violence within our nation's schools and communities.

Randolph D. Alles
Director

INTRODUCTION

When incidents of school violence occur, they leave a profound and lasting impact on the school, the community, and our nation as a whole. Ensuring safe environments for elementary and secondary school students, educators, administrators, and others is essential. This operational guide was developed to provide fundamental direction on how to prevent incidents of *targeted school violence,* that is, when a student specifically selects a school or a member of the school community for harm. The content in this guide is based on information developed by the U.S. Secret Service, Protective Intelligence and Assessment Division, National Threat Assessment Center (NTAC).

Over the last 20 years, NTAC has conducted research, training, and consultation on threat assessment and the prevention of various forms of targeted violence. Following the tragedy at Columbine High School in April 1999, the Secret Service partnered with the Department of Education on a study that examined 37 incidents of targeted violence that occurred at elementary and secondary schools (i.e., K-12). The goal of that study, the *Safe School Initiative (SSI),* was to gather and analyze accurate and useful information about the thinking and behavior of students who commit these types of acts. The findings of the *SSI,* and an accompanying guide, served as the impetus for establishing threat assessment programs in schools. In 2008, the agencies collaborated again and released a report that further explored one of the key *SSI* findings, namely, that prior to most attacks, though other students had information about the attackers' plans, most did not report their concerns to an adult. The findings of this report, known as the *Bystander Study,* highlighted the importance of creating safe school climates to increase the likelihood that students will speak up in order to prevent an attack.[1]

The information gleaned from these studies underscores the importance of establishing a threat assessment process in schools to enhance proactive targeted violence prevention efforts. The goal of a threat assessment is to identify students of concern, assess their risk for engaging in violence or other harmful activities, and identify intervention strategies to manage that risk. This guide provides actionable steps that schools can take to develop a comprehensive targeted violence prevention plan and create processes and procedures for conducting threat assessments on their campus. These steps serve as minimum guidelines and may need to be adapted for a particular school or district's unique resources and challenges. For institutions that already have prevention plans or threat assessment capabilities in place, these guidelines may provide additional information to update existing protocols, or to formalize the structures of reporting, gathering information, and managing risk.

When establishing threat assessment capabilities within K-12 schools, keep in mind that **there is no profile of a student attacker.** There have been male and female attackers, high-achieving students with good grades as well as poor performers. These acts of violence were committed by students who were loners and socially isolated, and those who were well-liked and popular. Rather than focusing solely on a student's personality traits or school performance, we can learn much more about a student's risk for violence by working through the threat assessment process, which is designed to gather the most relevant information about the student's communications and behaviors, the negative or stressful events the student has experienced, and the resources the student possesses to overcome those setbacks and challenges.

---

[1] All publications related to studies conducted by the U.S. Secret Service, National Threat Assessment Center (NTAC) are available from https://www.secretservice.gov/protection/ntac/.

CREATING A COMPREHENSIVE TARGETED VIOLENCE PREVENTION PLAN

Ensuring the safety of our schools involves multiple components, including physical security, emergency management, and violence prevention efforts in the form of a threat assessment process. This process begins with establishing a comprehensive targeted violence prevention plan. The plan includes forming a multidisciplinary threat assessment team, establishing central reporting mechanisms, identifying behaviors of concern, defining the threshold for law enforcement intervention, identifying risk management strategies, promoting safe school climates, and providing training to stakeholders. It can also help schools mitigate threats from a variety of individuals, including students, employees, or parents.

This guide provides basic instructions for schools on creating a targeted violence prevention plan, the focus of which is to decrease the risk of *students* engaging in harm to themselves or the school community. These recommendations serve as the starting point on a path to implementation that will need to be customized to the specific needs of your school, your student body, and your community. When creating these plans, schools should consult with legal representatives to ensure that they comply with any applicable state and federal laws or regulations.

Step 1.
Establish a multidisciplinary threat assessment team

The first step in developing a comprehensive targeted violence prevention plan is to establish a multidisciplinary threat assessment team (hereafter referred to as the "Team") of individuals who will direct, manage, and document the threat assessment process. The Team will receive reports about concerning students and situations, gather additional information, assess the risk posed to the school community, and develop intervention and management strategies to mitigate any risk of harm. Some considerations for establishing a Team include:

- Some schools may pool their resources and have a single Team that serves an entire district or county, while other districts may choose to have a separate Team for each school.

- Teams should include personnel from a **variety of disciplines** within the school community, including teachers, guidance counselors, coaches, school resource officers, mental health professionals, and school administrators. The multidisciplinary nature of the Team ensures that varying points of view will be represented and that access to information and resources will be broad.

- The Team needs to have a **specifically designated leader.** This position is usually occupied by a senior administrator within the school.

- Teams should establish **protocols and procedures** that are followed for each assessment, including who will interview the student of concern; who will talk to classmates, teachers, or parents; and who will be responsible for documenting the Team's efforts. Established protocols allow for a smoother assessment process as Team members will be aware of their own roles and responsibilities, as well as those of their colleagues.

- Team members should meet whenever a concerning student or situation has been brought to their attention, but they should also **meet on a regular basis** to engage in discussions, role-playing scenarios, and other team-building and learning activities. This will provide members of the Team with opportunities to work together and learn their individual responsibilities so that when a crisis does arise, the Team will be able to operate more easily as a cohesive unit.
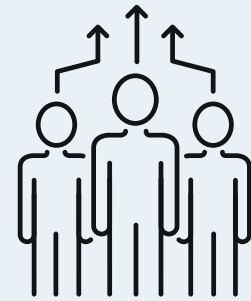
While the information in this guide refers to this group as a Threat Assessment Team, schools can choose an alternative name. For example, some schools have opted to use the label "Assessment and Care Team" to encourage involvement from those who might be concerned about a student, and to focus on getting a student access to needed resources and supports. Other schools have chosen to refer to this group as a "Behavioral Intervention Team" to focus on a spectrum of concerning behaviors that a student may be exhibiting. Finally, some schools have continued to refer to their groups as "Threat Assessment Teams" to highlight the heightened sense of concern about a student who is identified.

Step 2.
Define prohibited and concerning behaviors

Schools need to establish policies defining prohibited behaviors that are unacceptable and therefore warrant immediate intervention. These include threatening or engaging in violence, bringing a weapon to school, bullying or harassing others, and other concerning or criminal behaviors. Keep in mind that **concerning behaviors occur along a continuum.** School policies should also identify behaviors that may not necessarily be indicative of violence, but also warrant some type of intervention. These include a marked decline in performance; increased absenteeism; withdrawal or isolation; sudden or dramatic changes in behavior or appearance; drug or alcohol use; and erratic, depressive, and other emotional or mental health symptoms.

- If these behaviors are observed or reported to the Team, schools can offer resources and supports in the form of mentoring and counseling, mental health care, tutoring, or social and family services.

- The **threshold for intervention** should be relatively low so that Teams can identify students in distress before their behavior escalates to the point that classmates, teachers, or parents are concerned about their safety or the safety of others. It is much easier to intervene when the concern is related to a student's struggle to overcome personal setbacks, such as a romantic breakup, than when there are concerns about threats posed to others.

- During the assessment process, Teams may identify other **concerning statements and actions** made by the student that may not already be addressed in their policies. Gathering information about these behaviors will help the Team assess whether the student is at risk for attacking the school or its students and identify strategies to mitigate that risk.
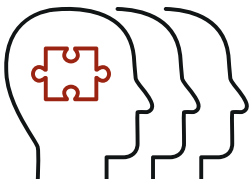
Step 3.
Create a central reporting mechanism

" ...reports will be acted upon..."

Students may elicit concern from those around them in a variety of ways. They may make threatening or concerning statements in person, online, or in text messages; they may engage in observable risky behavior; or they may turn in assignments with statements or content that is unusual or bizarre. When this occurs, those around the student need a method of reporting their concerns to the Team.

• Schools can **establish one or more reporting mechanisms,** such as an online form posted on the school website, a dedicated email address or phone number, smart phone application platforms, or another mechanism that is accessible for a particular school community.

• Students, teachers, staff, school resource officers, and parents should be **provided training and guidance on recognizing behaviors of concern, their roles and responsibilities in reporting the behavior, and how to report the information.**

• Teams need to be sure that a team member proactively monitors all incoming reports and can **respond immediately** when someone's safety is concerned.

• Regardless of what method schools choose to receive these reports, there should be an **option for passing information anonymously,** as students are more likely to report concerning or threatening information when they can do so without fear of retribution for coming forward.

• The school community should feel confident that team members will be responsive to their concerns, and that **reports will be acted upon, kept confidential, and handled appropriately.**
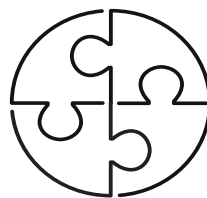
Many reporting mechanisms employed by K-12 schools resemble nationwide criminal reporting apps. The online and phone reporting capabilities of these types of apps allow individuals across the country, including students, parents, and teachers, to report crimes and other concerning behaviors in their communities and schools. Some reporting mechanisms are developed specifically for use by students in K-12 school settings. These programs allow students, parents, and teachers to anonymously report threats, bullying, and other situations that make them feel unsafe or fear for the safety of a peer to trained experts who respond appropriately.

Step 4.
Determine the threshold for law enforcement intervention

The vast majority of incidents or concerns that are likely to be reported can be handled by school personnel using school or community resources. For example, the most common types of reports submitted to Safe2Tell Colorado during the 2016-2017 school year were related to suicide, bullying, drugs, cutting (self-harm), and depression.[2] Some of these common reports may not require the involvement of law enforcement. Those that do warrant law enforcement intervention include threats of violence and planned school attacks, which constituted Safe2Tell's sixth and seventh most common types of reports, respectively.

- Reports regarding student behaviors **involving weapons, threats of violence, physical violence, or concerns about an individual's safety** should immediately be reported to local law enforcement. This is one reason why **including a school resource officer or local law enforcement officer** on the Team is beneficial.

- If a school resource officer is not available to serve on the Team, schools should set a clear threshold for times and situations when **law enforcement will be asked to support or take over an assessment.** For example, it might be necessary to have law enforcement speak with a student's parent or guardian, search a student's person or possessions, or collect additional information about the student or situation outside the school community during the assessment.

---

[2] Data 2 Report 2016-2017. (n.d.). Safe2Tell Colorado. Retrieved on June 20, 2018, from https://safe2tell.org/sites/default/files/u18/End%20of%20Year%202016-2017%20Data2Report.pdf

Step 5.
Establish assessment procedures

Teams need to establish clearly defined processes and procedures to guide their assessments. Note that any safety concerns should be immediately addressed before the procedures described below take place. When followed, the procedures should allow the Team to form an accurate picture of the student's thinking, behavior, and circumstances to inform the Team's assessment and identify appropriate interventions.

- **Maintain documentation** to keep track of when reports come in; the information that is gathered; when, where, and how it was obtained; who was interviewed; the behaviors and circumstances of the student of concern; and the intervention strategies taken. Documentation requirements, such as forms and templates, should be included in the plan to ensure standardization across cases.

- **Use a community systems approach.** An effective approach for gathering information to assess a student of concern is to **identify the sources that may have information on the student's actions and circumstances.** This involves identifying the persons with whom the student has a relationship or frequently interacts and the *organizations or platforms* that may be familiar with the student's behaviors. Students exist in more than one system and they come in contact with people beyond their classmates and teachers at school. Gathering information from multiple sources ensures that Teams are identifying concerning behaviors, accurately assessing the student's risks and needs, and providing the appropriate interventions, supports, and resources.

- **Examine online social media pages, conduct interviews, review class assignments, and consider searching the student's locker or desk.** Team members should also review **academic, disciplinary, law enforcement, and other formal records** that may be related to the student. When reviewing school records, be sure to determine whether the student has been the subject of previous reports to school officials, especially if the student has a history of engaging in other concerning or threatening behaviors. Also determine if the student received any intervention or supports and whether those were beneficial or successful. The Team may be able to draw on information from previous incidents and interventions to address the current situation for the student. This factor further emphasizes the importance of the Team's documentation to ensure the accuracy and availability of information regarding prior contacts the student of concern may have had with the Team.

Step 5 continued.
Establish assessment procedures
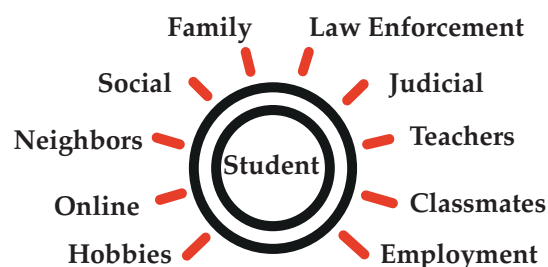
Key Themes to Guide Threat Assessment Investigations

- **Build rapport that can facilitate information-gathering efforts.** By demonstrating that their goal is to support individuals who may be struggling, while ensuring that the student and the school are safe, Teams may be better able to build a positive relationship with a student of concern and the student's parents or guardians. When Teams have established this rapport, parents or guardians may be more likely to share their own concerns, and the student may be more forthcoming about frustrations, needs, goals, or plans.

- **Evaluate the student's concerning behaviors and communications in the context of his/her age and social and emotional development.** Some students' behaviors might seem unusual or maladaptive, but may be normal for adolescent behavior or in the context of a mental or developmental disorder. To ensure that these students are being accurately assessed, collect information from diverse sources, including the reporting party, the student of concern, classmates, teammates, teachers, and friends. Consider whether those outside of their immediate circle, such as neighbors or community groups, may be in a position to share information regarding observed behaviors.

U.S. Secret Service research identified the following themes to explore when conducting a threat assessment investigation:

- The student's motives and goals

- Concerning, unusual, or threatening communications

- Inappropriate interest in weapons, school shooters, mass attacks, or other types of violence

- Access to weapons

- Stressful events, such as setbacks, challenges, or losses

- Impact of emotional and developmental issues

- Evidence of desperation, hopelessness, or suicidal thoughts and gestures

- Whether the student views violence as an option to solve problems

- Whether others are concerned about the student's statements or behaviors

- Capacity to carry out an attack

- Evidence of planning for an attack

- Consistency between the student's statements and actions

- Protective factors such as positive or prosocial influences and events

Investigative themes

Teams should organize their information gathering around **several themes or areas pertaining to the student's actions, circumstances, and any other relevant threat assessment factors.** Addressing each theme is necessary for a complete assessment and may uncover other avenues of inquiry to help determine whether the student is at risk for engaging in violence. Using the themes to identify where the student might be struggling will help the Team identify the most appropriate resources. Keep in mind, there is no need to wait until the Team has completed all interviews or addressed every theme before taking action. As soon as an area for intervention is identified, suitable management strategies should be enacted.

Motives

Students may have a variety of motives that place them at risk for engaging in harmful behavior, whether to themselves or others. If you can discover the student's motivation for engaging in the concerning behavior that brought him/her to the attention of the Team, then you can understand more about the student's goals. The Team should also assess how far the student may be willing to go to achieve these goals, and what or who may be a potential target. Understanding motive further allows the Team to develop management strategies that can direct the student away from violent choices.

On February 12, 2016, a 15-year-old female student fatally shot her girlfriend while they were sitting under a covered patio at their high school and then fatally shot herself. In several notes found after the incident, the student explained that she carried out her attack because her girlfriend had recently confessed that she was contemplating ending their relationship. She also wrote in her notes that she hated who she was and that learning her girlfriend wanted to end their relationship "destabilized" her.

Step 5 continued.
Establish assessment procedures, *Investigative themes*

Communications

Look for concerning, unusual, bizarre, threatening, or violent communications the student made. The student's communications may reveal grievances held about certain issues or a possible intended target. They may allude to violent intentions or warn others to stay away from school at a certain time. They may reveal information relevant to the other investigative themes by making reference to feelings of hopelessness or suicide, a fascination with violence, interest in weapons, or other inappropriate interests. These statements might be made in person to classmates, teammates, or friends; in writing on assignments or tests; and/or via social media, text messages, or photo or video-sharing sites.

Earlier NTAC research that examined attacks on schools found that not every student directly threatened their target prior to attack, but in a majority of incidents (81%), another person was aware of what the student was thinking or planning.[3] It is important for Teams to remember that a student who has **not made threatening statements may still be at risk** for engaging in violence. Whether or not the student made a direct threat should not be the lone indicator of concern.

On October 24, 2014, a 15-year-old male student opened fire on five of his closest friends as they were having lunch in the school cafeteria, killing four of them, and then fatally shot himself. In the months prior to his attack, the student sent a number of text messages to his ex-girlfriend indicating he was considering suicide and posted videos on Snapchat that mentioned suicide. Two people confronted the student about his concerning statements, but he told them he was just joking or having a bad moment. The student also posted a number of Twitter messages indicating he was having trouble overcoming a setback, posting in one Tweet, "It breaks me… It actually does… I know it seems like I'm sweating it off… But I'm not.. And I never will be able to…"

---
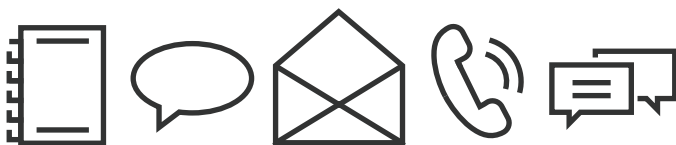
[3] U.S Secret Service and U.S Department of Education. (May 2002). Threat assessment in schools: A guide to managing threatening situations and to creating safe school climates. Retrieved April 5, 2018, from https://www.secretservice.gov/data/protection/ntac/ssi_guide.pdf.

Inappropriate interests

Gather information about whether the student has shown an **inappropriate or heightened interest in concerning topics such as school attacks or attackers, mass attacks, or other types of violence.** These interests might appear in the student's communications, the books the student reads, the movies the student watches, or the activities the student enjoys. The *context* of the student's interests is an important factor to consider. For example, a student's interest in weapons may not be concerning if the student is a hunter or is on the school's rifle team, with no evidence of an inappropriate or unhealthy fixation on weapons. In other situations, the context surrounding a student's interest in weapons could be of concern. For example, if a student is fixated on past school shooters or discusses what firearm would be best to use in a mass attack.

On October 21, 2013, a 12-year-old male student took a handgun to his middle school and opened fire, injuring two classmates and killing a teacher. He then fatally shot himself. In the months leading up to his attack, the student conducted numerous internet searches for violent material and content, including "Top 10 evil children," "Super Columbine Massacre Role Playing Game," "shoot," "guns," "bullets," "revenge," "murder," "school shootings," and "violent game." He also searched for music videos of and songs about school shootings. On his cell phone, the student had saved photos of violent war scenes and images of the Columbine High School shooters. He also enjoyed playing video games, doing so for several hours each night. Of his 69 video games, 47 were first-person shooter or similar games.

Weapons access

In addition to determining whether the student has any inappropriate interests or fascination with weapons, the Team should assess whether the student has **access to weapons.** Because many school attackers used firearms acquired from their homes, consider whether the family keeps weapons at home or if there is a relative or friend who has weapons. Sometimes parents who keep weapons at home incorrectly assume that their children are unaware of where they are stored or how to access them. If there are weapons at home, the Team should determine if they are stored appropriately and if the student knows how to use them or has done so in the past. The Team should also remember that firearms are not the only weapons to be concerned about. Even though many school attackers have used firearms in carrying out their attacks, explosives, incendiary devices, bladed weapons, or combinations of these weapons have been used in past attacks.

On April 29, 2014, a 17-year-old male student was arrested after a concerned citizen called police when she observed the student acting suspiciously around a storage unit and thought he might be attempting to break into one. Responding officers discovered bomb-making material and other weapons inside the unit the student had asked a friend's mother to rent for him. The student later confessed to an extensive plot that involved murdering his parents and sister, setting a diversionary fire, planting explosive devices at his high school, targeting students and the school resource officer for harm, and engaging in gunfire with responding police officers before committing suicide. The student admitted that at some point he became fascinated with chemicals, explosives, and weapons and began researching how to build his own explosive devices. He created his own channel on YouTube to post videos that showed him detonating his devices and included a written commentary about each video.

Step 5 continued.
Establish assessment procedures, *Investigative themes*

Stressors

All students face stressors such as **setbacks, losses, and other challenges** as part of their lives. While many students are resilient and can overcome these situations, for some, these stressors may become overwhelming and ultimately influence their decision to carry out an attack at school. Gather information on stressors the student is experiencing, how the student is coping with them, and whether there are supportive friends or family who can help the student overcome them. Assess whether the student experienced stressors in the past that are still having an effect, such as a move to a new school, and whether there might be additional setbacks or losses in the near future, like a relationship that might be ending.

Stressors can occur in all areas of a student's life, including at school with coursework, friendships, romantic relationships, or teammates; or outside of school with parents, siblings, or at jobs. Many students can experience bullying, a stressor which can take place in person at school or online at home. Teams should intervene and prevent bullying and cyberbullying of a student who has been brought to their attention. More broadly, administrators should work to address any concerns regarding bullying school-wide and ensure their school has a safe climate for all students.

On November 12, 2008, a 15-year-old female student fatally shot a classmate while students were changing classes. The attacker fled to a restaurant across the street from her high school and phoned 9-1-1 to turn herself in to police. Prior to her attack, she faced a number of stressors in her life, mostly outside of school. As an infant, her college-aged parents abandoned her and she was raised largely by her grandparents. At the age of six years, she was sexually molested by a family member; and at age 12, she was raped by an uncle. She did have some contact with her birth parents, but her mother was reportedly abusive and suffered from severe mental illness; and her father began serving a 25-year prison sentence for murder around the time she was 14 years old. At her high school, she was lonely, appeared to struggle to connect with others, and had behavior problems.

Emotional and developmental issues

Anxiety, depression, thoughts of suicide, and other mental health issues are important factors to consider when conducting an assessment. Keep in mind that students with emotional issues or developmental disorders might behave in a way that is maladaptive, but might not be concerning or threatening because the behavior is a product of their diagnosis. **Behaviors exhibited by a student with a diagnosed disorder need to be evaluated in the context of that diagnosis and the student's known baseline of behavior.** If the student is experiencing feelings related to a diagnosable mental illness, such as depression, then the Team needs to consider the effect of these feelings on their behaviors when assessing the student's risk of engaging in harm to self or others.

On January 18, 1993, a 17-year-old male student fatally shot his English teacher and a school custodian at his high school and held classmates hostage before surrendering to police. The student had recently turned in a poem to his English teacher for an assignment that discussed his thoughts of committing homicide or suicide. The student had failed in at least three prior suicide attempts, including one the night before his attack. Although the student entered a plea of guilty but mentally ill at trial, ultimately he was convicted and sentenced to life in prison.

Desperation or despair

Assess whether the student feels **hopeless, desperate, or out of options.** Determine if the student has had thoughts about or engaged in behaviors that would indicate the student's desperation. The Team should determine whether the student has felt this way before, how the student managed those feelings then, and whether those same resources for coping are available to the student now. Consider whether the student has tried addressing the problems in a positive way, but was unable to resolve them, thereby leading to a sense of hopelessness about their situation.

On February 1, 1997, a 16-year-old male student used a shotgun to fire on fellow students in the common area of his high school prior to the start of the school day. He killed one student and the principal and injured two additional students. Prior to his attack, the student had been bullied and teased by several classmates, including the student killed. At some point prior to his attack, the student asked the principal and dean of students for help with the bullying he was experiencing. They intervened, and though the situation improved temporarily, the teasing and bullying soon resumed. The student asked the principal for help a second time, but this time the principal advised him to just ignore the bullies. The student tried, but felt like the victimization worsened and he began to feel hopeless that it would ever end. After his attack, the student explained that he felt as though he had asked the "proper people" for assistance, but he was denied help, so he decided that bringing a gun to school would scare his tormentors and get them to leave him alone. When some friends learned of the plan, they told him that he had to use the weapon to shoot people or the bullying would continue. The student decided he would have to fire the weapon at people in order to end his torment.

Step 5 continued.
Establish assessment procedures, *Investigative themes*

Violence as an option

Some students, who are feeling hopeless and out of options, **may think violence is the only way to solve a problem or settle a grievance.** The Team should look to see whether the student thinks violence is acceptable or necessary, if the student has used violence in the past to address problems, and whether the student has thought of alternative ways to address the grievances. The Team should also assess whether peers, or others, support and encourage the student to use violence as a means to an end. If possible, connect the student with more positive, prosocial role models who discourage violence and identify more acceptable ways to solve problems.

On March 25, 2011, a 15-year-old male student fired two shots at a classmate, wounding him in the abdomen. After firing the weapon, the student fled the scene and dropped the gun in a field. He was arrested about an hour after the incident. The student had a history of being involved in numerous physical altercations with other students throughout his 6th, 7th, and 8th grade school years. Additionally, he tried to start a fight with the targeted victim, and once threatened him with a chain. About three weeks prior to the attack, the student threatened to blow up the school. Days prior to the incident, the student, who was angry at the targeted victim, told a friend that he planned to kill him.

Concerned others

In previous incidents, many students made statements or engaged in behaviors prior to their attacks that elicited concern from others in their lives. Assess whether parents, friends, classmates, teachers, or others who know the student are worried about the student and whether they have taken any actions in response to their concerns. Gather information on the specific behaviors that caused worry or fear. These could include **behaviors that may have elicited concerns about the safety of the student or others,** such as unusual, bizarre or threatening statements; intimidating or aggressive acts; indications of planning for an attack; suicidal ideations or gestures; or a fixation on a specific target. **Other behaviors that elicit concern may not necessarily be indicative of violence,** but do require that the Team assess the behavior and provide appropriate supports. Examples of these behaviors include alcohol or drug use; behavior changes related to academic performance, social habits, mood, or physical appearance; conflicts with others; and withdrawal or isolation.

On December 7, 2017, a 21-year-old male shot and killed two students at his former high school before fatally shooting himself. Prior to his attack, a number of individuals had expressed concern regarding his behaviors and statements. Sometime in 2012, other users of an online forum were concerned after the student made threats about attacking his school. In March 2016, federal investigators met with the student after he made comments in an online chat room about wanting to find an inexpensive assault rifle he could use for a mass shooting. At the time, a family member told the investigators that the student was troubled and liked to make outlandish statements. At some point prior to his attack, the student posted content supportive of the attacks at Columbine High School in an online forum, upsetting many of the forum's users.
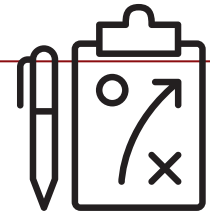
Capacity to carry out an attack

Determine whether the student's thinking and behavior is organized enough to plan and execute an attack and whether the student has the resources to carry it out. **Planning does not need to be elaborate** and could be as simple as taking a weapon from home and inflicting harm on classmates at school. Other student attackers may develop more complex and lengthier plans. At the very least, carrying out an attack requires that the student has access to a weapon and the ability to get that weapon to school undetected.

On January 14, 2014, a 12-year-old male student used a shotgun with a sawed-off stock to fire three rounds of birdshot at fellow students gathered in their middle school gymnasium prior to the start of the school day. He injured two students and a security guard before surrendering to a teacher. The student began talking about his attack plans as early as November 2013, saying that he wanted to fire a weapon in the air to make people take him seriously. According to reports, his father owned a pistol and a shotgun. In January 2014, the student wrote in his diary that he wanted to use his father's pistol for his attack, but was unable to locate it so he used the shotgun instead. The morning of the attack, the student was driven to school by a family member so he hid his shotgun in a duffel bag, claiming it contained items for his gym class.

Planning

Targeted attacks at school are **rarely sudden or impulsive** acts of violence. The Team should assess whether the student has made specific plans to harm the school. The student might create lists of individuals or groups targeted for violence, or research tactics and materials needed to carry out the attack. The student may conduct surveillance, draw maps of the planned location, and test security responses at school. He/she may write out detailed steps and rehearse some aspects of a plan, such as getting to the school, the timing of the attack, or whether to attempt escape, be captured, or commit suicide. The student may also acquire, manufacture, or practice with a weapon.

On December 13, 2013, an 18-year-old male student entered his high school with a shotgun, a large knife, bandoliers with ammunition, and a number of homemade Molotov cocktails. He opened fire on two female students, fatally shooting one. He then entered the school library and opened fire on a faculty member there, who was able to escape through a back door. The student then set fire to a shelf of books in the library with one of his Molotov cocktails before fatally shooting himself. The student spent three months planning his attack, starting a diary on his computer in September 2013 to detail his plans. There he wrote that he wanted to choose a day during final exams so that the largest number of students would be present. Over the next few months, he planned how and where he would enter the school, including where he would initiate the attack, and purchased the firearm and ammunition he would use. On the morning of the incident, the student purchased a four-pack of glass soda bottles and used these to create the Molotov cocktails he deployed during the attack.

Step 5 continued.
Establish assessment procedures, *Investigative themes*

Consistency

The Team should **corroborate the student's statements** to determine that they are consistent with the student's actions and behaviors and with what other people say about the student. When inconsistencies are identified, the Team should then try to determine why that is the case. For example, the student might say that he/she is handling a romantic break-up well, but posts on social media indicate the student is struggling to move on, and friends report that the student is more upset or angry about the break-up than reported. Determine whether the inconsistency is because the student is deliberately hiding something or if the inconsistency stems from another underlying issue. For example, a depressed student may claim that they are isolated, even if they regularly go out with a large group of students. If the inconsistency is deliberate, it is important to determine why the student feels the need to conceal his/her actions. The concealment may be as simple as a fear of facing punishment for some other inappropriate behavior, or it may be related to hidden plans for a violent act.

On June 10, 2014, a 15-year-old male student brought a rifle, handgun, nine magazines with ammunition, and a knife into the boy's locker room at his high school. He had taken the weapons from his brother's locked gun case in his home. Once at school, he changed into all black clothing, and donned a helmet, face mask, and a non-ballistic vest. He then fatally shot one student and wounded a teacher. After being confronted by staff and law enforcement, the student fatally shot himself in a bathroom. Prior to his attack, the student was an ordained deacon at his church and was appointed president of the deacon's quorum. He participated in youth night at the church, Boy Scouts, youth basketball, and track. Friends described him as friendly and outgoing. He was also a member of the Junior Reserve Officers' Training Corps (JROTC) and was fascinated with guns and the military. Despite his outward appearance, some time prior to his attack, he wrote in a journal about his plans to kill his classmates and spoke harshly about "sinners," which included people who smoked cigarettes and took the Lord's name in vain.

Protective factors

A thorough threat assessment requires understanding the full picture of a student's behaviors and environment, which also includes accounting for the positive and prosocial influences on the student's life. The Team should identify factors that may restore hope to a student who feels defeated, desperate, or in a situation that is impossible to overcome. This includes determining whether the student has a **positive, trusting relationship with an adult at school.** This could be a teacher, coach, guidance counselor, administrator, nurse, resource officer, or janitor. A trusted adult at school in whom the student can confide and who will listen without judgment can help direct a student toward resources, supports, and options to overcome setbacks. Learn who the student's friends are at school and if the student feels **emotionally connected to other students.** A student may need help developing friendships that they can rely on for support.

Positive situational or personal factors might help to deter a student from engaging in negative or harmful behaviors. Changes in a student's life, such as having a new romantic relationship or becoming a member of a team or club, might discourage any plan to engage in violence. The Team could also use activities or groups the student wants to take part in as motivation for the student to engage in positive and constructive behaviors, such as attending class, completing assignments, and adhering to a conduct or behavior code.

Step 6.
Develop risk management options

Once the Team has completed a thorough assessment of the student, it can **evaluate whether the student is at risk for self-harm or harming someone else** at school. Concern may be heightened if the student is struggling emotionally, having trouble overcoming setbacks or losses, feeling hopeless, preoccupied with others who engaged in violence to solve problems, or has access to weapons. Remember, the Team is not attempting to predict with certainty if violence will happen. Instead, evaluate the presence of factors that indicate violence might be a possibility. Teams can then **develop risk management strategies that reduce the student's risk for engaging in violence** and make positive outcomes for the student more likely.

- Each student who comes to the Team's attention will require an **individualized management plan.** The resources and supports the student needs will differ depending on the information gathered during the assessment.

- Often, the Team will determine that the student is not currently at risk for engaging in violence, but **requires monitoring or is in need of guidance** to cope with losses, develop resiliency to overcome setbacks, or learn more appropriate strategies to manage emotions.

- **Resources to assist the student** could take the form of peer support programs or therapeutic counseling to enhance social learning or emotional competency, life skills classes, tutoring in specific academic subjects, or mental health care. Most programs and supports will be available within the school, but the Team may need to also access community resources to assist with managing the student.

- Sometimes management involves suspension or expulsion from school. When this is necessary, Teams and school administrators should consider how it might affect their ability to monitor the student. **Removing a student from school does not eliminate the risk to the school community.** Several school attacks have been carried out by former students who had been removed from the school or aged out of their former school. A suspended or expelled student might become isolated from positive peer interactions or supportive adult relationships at school. Teams should develop strategies to stay connected to the suspended or expelled student to determine whether the student's situation is deteriorating or the behaviors of concern are escalating so that they can respond appropriately.

Management plans should remain in place until the Team is no longer concerned about the student or the risk for violence. This is accomplished by addressing the following basic elements that can reduce the likelihood a student will engage in violence and provide support and resources for those in need.

- **Notify law enforcement immediately if a student is thinking about or planning to engage in violence,** so that they may assist in managing the situation.

- **Make efforts to address the safety of any potential targets** by altering or improving security procedures for schools or individuals and providing guidance on how to avoid the student of concern.

Step 6 continued.
Develop risk management options

- **Create a situation that is less prone to violence** by asking the family or law enforcement to block the student's access to weapons, while also connecting the student to positive, prosocial models of behavior. Another option may involve removing the student from campus for a period of time, while maintaining a relationship with the student and the student's family.

- **Remove or redirect the student's motive.** Every student's motive will be different, and motives can be redirected in a variety of ways. These strategies may include bullying prevention efforts or offering counseling for a student experiencing a personal setback.

- **Reduce the effect of stressors** by providing resources and supports that help the student manage and overcome negative events, setbacks, and challenges.

In one recent case, a school principal described a situation when a student was suspended from his high school for drug possession. Soon after, a fellow student discovered a concerning video he posted online and notified school personnel. A school administrator met with the student and his father. While the administrator had no immediate safety concerns about the student, he was aware that the student was experiencing a number of stressors. The student's parents were divorced and he was living with his father, who was diagnosed with a terminal illness and was receiving frequent medical treatments. His mother was dealing with a mental illness, was a source of embarrassment to him, and was unlikely to be able to serve as his guardian after his father's passing. He was also recently removed from the wrestling team, and due to his suspension, banned from attending the matches. While suspended, the student was required to attend tutoring sessions in lieu of school, but was unable to make his sessions because he was transporting his father to medical appointments. The administrator reported that he would have alerted their school resource officer and local sheriff's office if he had safety concerns about the student, but instead the school worked with community services to provide access to resources and supports, including transportation services for his father to his medical appointments so the student could attend tutoring sessions, and counseling and support services that would assist the student after his father's passing. The school also worked with the student and his father to develop a plan for the student to return to campus and remain on track to graduate.

Step 7.
Create and promote safe school climates

A crucial component of preventing targeted violence at schools relies on developing positive school climates **built on a culture of safety, respect, trust, and social and emotional support.** Teachers and staff in safe school environments support diversity, encourage communication between faculty and students, intervene in conflicts, and work to prevent teasing and bullying. Students in safe school climates feel empowered to **share concerns with adults,** without feeling ashamed or facing the stigma of being labeled a "snitch." Administrators can take action to develop and sustain safe school climates.

- Help students feel connected to the school, their classmates, and teachers. This is an important first step to creating school climates that are supportive, respectful, and safe. **Encourage teachers and staff to build positive, trusting relationships with students** by actively listening to students and taking an interest in what they say.

- **Break down "codes of silence"** and help students feel empowered to come forward and share concerns and problems with a trusted adult. At one school, administrators used a faculty meeting to identify students who lacked a solid connection with an adult at school. They provided faculty with a roster of enrolled students and asked them to place a mark next to students with whom they had a warm relationship. For students without a mark next to their name, popular, well-liked teachers and staff were asked to reach out and develop positive connections with them.

- Help students feel more **connected to their classmates and the school.** One teacher asked her elementary students to write down names of classmates they wanted to sit next to. If a student's name did not appear on anyone's list, the teacher placed that student's desk next to a friendly or outgoing classmate in an effort to help the student develop friendships. This effort could be easily adapted with middle or high school-aged students by asking students to identify one or two classmates they would like to be partnered with for a project and assigning any student not named on a list to be partnered with a friendly or outgoing classmate.

- Adults can also help students **identify clubs or teams at school** they can join or encourage them to start their own special interest group.

Step 7 continued.
Create and promote safe school climates

Schools can also support positive school climates by implementing school-wide Positive Behavioral Interventions and Supports (PBIS) programs. These programs actively teach students what appropriate behavior looks like in a variety of settings, including in the classroom, with their friends, or among adults. Teachers frequently praise prosocial behavior they observe and encourage students' good behavior. PBIS can improve academic outcomes for schools and has been shown to reduce the rates of school bullying.[4]

While teachers and staff can foster relationships and connectedness among the student body, **students themselves have a role to play** in sustaining safe school climates. They should be actively engaged in their schools, encouraged to reach out to classmates who might be lonely or isolated, and empowered to intervene safely when they witness gossiping, teasing, and bullying.

Following an averted attack at a high school, the school principal sent a note home to students and parents about the incident. He used the note to explain what had been reported, the steps the school had taken to avert the attack, and praise for the students who had alerted school officials about concerning and threatening statements they saw online. In the note, he also asked parents to encourage their students to speak up if they ever felt concerned about a classmate's behavior, explaining that students' "cooperation [with school officials] is important for everybody's safety."

---

[4] Lee, A.M.I. (n.d.). PBIS: How schools can support positive behavior. Understood.org. Retrieved on April 5, 2018, from https://www.understood.org/en/learning-attention-issues/treatments-approaches/educational-strategies/pbis-how-schools-support-positive-behavior.

Step 8.
Conduct training for all stakeholders

> " School safety is everyone's responsibility."

The final component of a comprehensive targeted violence prevention plan is to identify training needs for all stakeholders, including faculty, staff, and administrators; students; parents; and school resource officers or local law enforcement. **School safety is everyone's responsibility.** Anyone who could come forward with concerning information or who might be involved in the assessment process should be provided with training. Effective training addresses the goals and steps of an assessment, the type of information that should be brought forward, and how individuals can report their concerns. It might be beneficial for staff and students to hear presentations, see videos, and role-play scenarios so they have a thorough understanding of their responsibilities and the steps they can take to keep their school safe. Each audience will require a slightly different message, but some stakeholders may also benefit from attending training together, such as parents and students, or school faculty/staff and law enforcement personnel. When developing a training program, consider how frequently each stakeholder will receive training, and whether to vary the delivery method of trainings. Also, each audience may have unique needs.

Faculty, staff, and administrators. Every adult at school needs training related to threat assessment and violence prevention, **including administrative, maintenance, custodial, and food service staff.** Training can include who should be notified when concerning or threatening information is discovered, what information should be brought forward, how school staff might learn about information, and the steps school staff can take to safely intervene with concerning or threatening situations. Providing training on other topics, such as suicide awareness and prevention, conflict resolution, mental health, and developmental disabilities, might also allow school faculty, staff, and administrators to foster positive school climates.

Students. Students need training on the threat assessment process, where to report concerns, and what information they should bring forward. Students also need assurances that they can make a report to the Team or another trusted adult **anonymously,** that their information will be **followed-up on,** and will be kept **confidential.** Training can also educate students about other actionable steps they can take to cultivate a safe school climate, including ways they can safely intervene with bullying, gossip, or name-calling.

Messaging should demonstrate to students that there is a big **difference between "snitching," "ratting," or "tattling," and seeking help.** While snitching is informing on someone for personal gain, here, students are encouraged to come forward when they are worried about a friend who is struggling, or when they are trying to keep someone from getting hurt. Remind students that if they are concerned about a classmate or friend, they need to keep speaking out until that person gets the help they need. Finally, maintaining a safe school climate includes providing students with training or lessons to acquire skills and abilities to manage emotions, resolve conflicts, cope with stress, seek help, and engage in positive social interactions.

Who needs training?

- [ ] Teachers, staff, administrators
- [ ] Parents
- [ ] Students
- [ ] Law enforcement
- [x] All of the above

Step 8 continued.
Conduct training for all stakeholders

Parents. Parents should also be trained on the threat assessment process at their child's school and their role in that process. **They should be clear on who to call, when, and what information they should be ready to provide.** Parents can also benefit from training that helps them recognize when children and teenagers may be in emotional trouble or feeling socially isolated. Training can also reduce the stigma around mental, emotional, or developmental issues and provide information on available resources and when they should seek professional assistance.

Law enforcement and school resource officers. Not every school will have a school resource officer, but schools can still **develop relationships with local law enforcement** agencies and personnel. Schools can encourage local officers to co-teach classes at the school, serve as coaches or assistant coaches of sports teams, and work with parents and teachers at after-school events. In some communities without school resource officers, local law enforcement

agencies have encouraged officers to "adopt a school," stopping by the school to greet and become familiar with students and teachers, eating lunch on campus, or doing paperwork in an office at the school.

Like parents and teachers, local law enforcement and school resource officers need to be aware of the school's threat assessment process and their own responsibilities once a threat is identified. Training for law enforcement and school resource officers should also provide familiarity with emergency response procedures the school has in place and the layout of the campus. Officers and school staff might benefit from attending training together so that all parties are aware of the point at which local law enforcement should be involved in an investigation. This would also allow officers to get to know administrators, teachers, counselors, facilities and maintenance personnel, and other school staff. It is much easier to work through an emergency situation when schools and law enforcement are already familiar with each other and their procedures.

CONCLUSION

Despite having a comprehensive targeted violence prevention plan in place, and despite a school and Team's best efforts at prevention, incidents of targeted school violence may still occur. It is critical to **develop and implement emergency response plans and procedures** and provide training on them to all stakeholders. The U.S. Department of Homeland Security recommends that emergency response plans be developed with input from local law enforcement and first responders.[5] For example, procedures should be developed for reporting emergencies, evacuation procedures and routes, use of emergency notification systems, and information regarding local hospitals or trauma centers. Law enforcement and first responders should be apprised of these plans and procedures and know how to implement them.

Everyone has a role in preventing school violence and creating safe school climates. The **threat assessment procedures detailed in this guide are an important component of school safety and security efforts** and have been determined to be the best-practice in the prevention of targeted school violence. The model highlights that students can engage in a continuum of concerning behaviors and communications, the vast majority of which may not be threatening or violent. Nevertheless, it encourages schools to set a low threshold when identifying students who might be engaging in unusual behavior, or experiencing distress, so that early interventions can be applied to reduce the risk of violence or other negative outcomes.

Threat Assessment
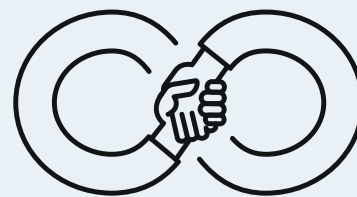
Active Incident Response

---

[5] U.S. Department Homeland Security. (October 2008). Active Shooter: How to Respond. Homeland Security Active Shooter Preparedness. Retrieved on May 29, 2018, from https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf. Interagency Security Committee. (November 2015). Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide. Homeland Security Active Shooter Preparedness. Retrieved on May 29, 2018, from https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf.

ADDITIONAL RESOURCES FOR SCHOOLS

This section provides information and links to resources that can help schools create threat assessment teams, establish central reporting mechanisms, train stakeholders on assessment procedures, and promote safe school climates. It also provides links to resources related to emergency planning, responses to violence, and mental health. The U.S. Secret Service provides the listed non-government resources as a public service only. The U.S. government neither endorses nor guarantees in any way the external organizations, services, advice, or products included in this list. Furthermore, the U.S. government neither controls nor guarantees the accuracy, relevance, timeliness or completeness of the information contained in non-government websites.[6]

Threat assessment

THE NATIONAL THREAT ASSESSMENT CENTER (NTAC). Provides links to best-practices in threat assessment and the prevention of targeted violence, including resources on conducting threat assessments in K-12 schools, building positive school climates, and requesting training from NTAC personnel.
https://www.secretservice.gov/protection/ntac/

NATIONAL ASSOCIATION OF SCHOOL PSYCHOLOGISTS (NASP). Provides information and links to research on conducting threat assessments in K-12 schools.
https://www.nasponline.org/resources-and-publications/resources/school-safety-and-crisis/threat-assessment-at-school/threat-assessment-for-school-administrators-and-crisis-teams

THE NATIONAL BEHAVIORAL INTERVENTION TEAM ASSOCIATION (NABITA). Provides education, resources, and supports to campus behavioral intervention team personnel and those who work to provide caring interventions of at-risk individuals.
https://nabita.org/

THE VIRGINIA STUDENT THREAT ASSESSMENT MODEL. Provides guidelines and resources for schools to conduct threat assessments of students, including links to research on threat assessment.
https://curry.virginia.edu/faculty-research/centers-labs-projects/research-labs/youth-violence-project/virginia-student-threat

---

[6] The provided links were active at the time of the publication of this guide. Organizations may have updated or changed their links since this guide was published.

School safety and violence prevention

NATIONAL EDUCATION ASSOCIATION (NEA). Provides resources, reports, and information about school safety and violence prevention.
http://www.nea.org/home/16364.htm

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE, YOUTH FOCUSED POLICING (YFP). Provides information, resources, and training to enable law enforcement to work and intervene with children, teens, and young adults. Resources focus on reducing crimes and victimization among youth populations.
http://www.iacpyouth.org/

NATIONAL ASSOCIATION OF SCHOOL RESOURCE OFFICERS (NASRO). Provides training, information, and resources to school-based law enforcement officers.
https://nasro.org/

NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER, SCHOOL SAFETY RESOURCES. Provides links to resources and information, including training material, computer software, and videos for law enforcement officers who work in K-12 schools.
https://www.justnet.org/school_safety.html

CENTER FOR THE STUDY AND PREVENTION OF VIOLENCE (CSPV). Conducts research and provides support to professionals implementing evidence-based programs that promote positive youth development, reduce problem behaviors, and prevent violence and other antisocial behaviors.
https://www.colorado.edu/cspv/

THE TEXAS SCHOOL SAFETY CENTER (TXSSC). Provides information and resources related to bullying, school violence, drugs and tobacco, technology safety, and emergency management.
https://txssc.txstate.edu/

SCHOOL SAFETY ADVOCACY COUNCIL (SSAC). Provides school safety training and services to school districts, law enforcement organizations, and communities. Provides links to grant opportunities, training courses, and conferences.
http://www.schoolsafety911.org/index.html

Emergency management and response to school violence

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS (REMS) TECHNICAL ASSISTANCE CENTER. National clearing-house for school safety information. Provides resources, training, and information related to violence prevention, response, and recovery from incidents of school violence.
https://rems.ed.gov/

GUIDE FOR PREVENTING AND RESPONDING TO SCHOOL VIOLENCE. Provides strategies to consider when creating safe learning environments and considers the full range of possible violence that can occur in schools.
http://www.theiacp.org/portals/0/pdfs/schoolviolence2.pdf

Creating safe and positive school climates

RESOURCE GUIDE FOR IMPROVING SCHOOL CLIMATE AND DISCIPLINE. Resource guide developed by the U.S. Department of Education for schools to create nurturing, positive, and safe environments to help boost student achievement and success.
https://www2.ed.gov/policy/gen/guid/school-discipline/guiding-principles.pdf

SCHOOLS SECURITY TASK FORCE, WHAT MAKES SCHOOLS SAFE? Publication by the New Jersey School Boards Association to provide guidance and direction on school safety issues. The final report provides recommendations and resources to ensure the physical and emotional well-being of students.
https://www.njsba.org/news-information/research/school-security-task-force/

POSITIVE BEHAVIORAL INTERVENTIONS AND SUPPORTS (PBIS). Clearinghouse and technical assistance center that supports schools, school districts, and state agencies to create and implement a multi-tiered approach to social, emotional, and behavioral support. Provides links to resources, information, and training on PBIS tools and strategies.
https://www.pbis.org/

Prevention and intervention of bullying

STOPBULLYING.GOV. Provides information from government agencies on bullying, cyberbullying, risk factors, responses to bullying, and prevention efforts.
https://www.stopbullying.gov/

NATIONAL PTA. Provides resources regarding bullying prevention and creating positive school climates.
https://www.pta.org/home/programs/Connect-for-RespectBullying

YOUTH VIOLENCE PROJECT, BULLYING RESOURCES. Provides an aggregate of online and in-print resources for parents, teachers, and students to intervene, prevent, and respond to bullying.
https://curry.virginia.edu/faculty-research/centers-labs-projects/research-labs/youth-violence-project/bullying/bullying-0

Mental health

NATIONAL ALLIANCE ON MENTAL ILLNESS (NAMI). NAMI is dedicated to assisting those affected by mental illness and their families. They provide information specific to conditions and symptoms experienced by teens and young adults, as well as resources for education and advocacy for all those who suffer from mental health symptoms.
https://www.nami.org/
https://www.nami.org/Find-Support/Teens-and-Young-Adults

NATIONAL INSTITUTE OF MENTAL HEALTH (NIMH). Provides links to resources for assistance with mental health and mental illness, information related to mental health symptoms and disorders, and outreach to various stakeholders.
https://www.nimh.nih.gov/index.shtml
https://www.nimh.nih.gov/health/find-help/index.shtml

MENTAL HEALTH FIRST AID. Provides resources for free and low-cost training on mental health, symptoms of mental illness, and intervening with those with mental health symptoms.
https://www.mentalhealthfirstaid.org/

PREVENTATIVE MEASURES

BUILDING THREAT ASSESSMENT TEAMS IN SCHOOLS:

THREAT ASSESSMENT MODEL, POLICIES, PROCEDURES & GUIDELEINES

VIRGINIA'S EXAMPLE

Threat Assessment in Virginia Public Schools:
Model Policies, Procedures, and Guidelines

Second Edition (2016)
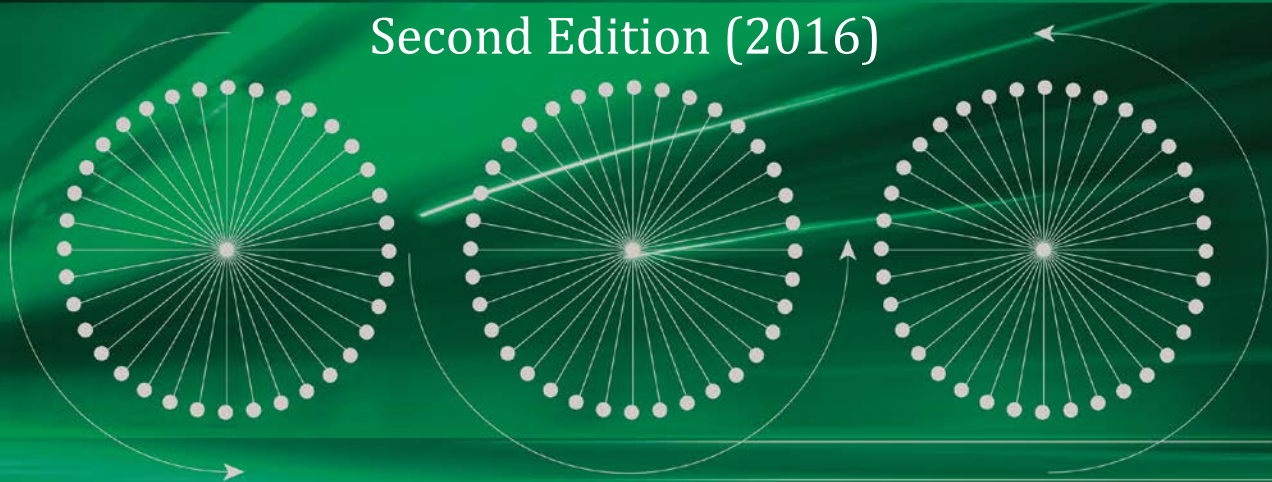
A Resource Provided by the

Virginia Department of Criminal Justice Services

Revised: August 2016

This edition revised by:

Gene Deisinger, Ph.D.
Threat Management Consultant
Virginia Department of Criminal Justice Services
Virginia Center for School and Campus Safety

CONTENTS

INTRODUCTION

The model threat assessment policies, procedures, and guidelines contained herein were initially developed in response to legislation enacted by the Virginia General Assembly in 2013. In accordance with *Code of Virginia*, § 9.1-184.A.10, the Virginia Center for School and Campus Safety (VCSCS), under the Virginia Department of Criminal Justice Services (DCJS) developed and provided model policies and procedures to help local school boards establish and operate threat assessment teams to support their schools. The primary focus was on providing schools with "a model policy for the establishment of threat assessment teams, including procedures for the assessment of and intervention with *students* whose behavior poses a threat to the safety of school staff or students."

On July 1, 2016, the Virginia General Assembly enacted several updates and additions to the *Code of Virginia* related to threat assessment teams in Virginia K-12 schools. These changes increase the consistency between the Virginia laws regarding threat assessment teams in public schools, and those regarding threat assessment teams in public institutions of higher education. The changes serve to broaden the legislated purview of school threat assessment teams, and provide those teams with more of the tools and protections that had previously been available only to campus threat assessment teams.

This document has been updated to reflect those statutory changes, and is provided as the current model policies, procedures and guidance for school threat assessment teams. There are no legislative mandates to use the model policies and procedures developed and provided in this document. However, in accordance with § 9.1-184, school division policies must be consistent with the model policies developed by the DCJS Virginia Center for School and Campus Safety. The DCJS/VCSCS model adheres to legislated requirements and is a synthesis of best practices or standards of practices in threat assessment and management in school settings. The DCJS/VCSCS model is available for use, free of charge for both public and private schools in Virginia.

Threat assessment in Virginia public educational settings, falls under the umbrella of the **Virginia C.A.R.E.S. for Schools and Campuses** program which was developed in 2016 to illustrate initiatives by the DCJS Virginia Center for School and Campus Safety to support schools and campuses in enhancing the safety and well-being of educational settings across the Commonwealth. The Virginia C.A.R.E.S program recognizes that threat assessment and management is but one part of a larger and on-going approach to support and enhance school & campus safety. School and campus safety (and well-being) are sustained and enhanced through:

    C: Caring and connection to build a positive school/campus climate;

    A: Awareness of resources and reporting options;

    R: Recognition of (and response to) aberrant and concerning behaviors;

    E: Engagement with the community and will persons (within the school or campus) for whom there is concern; and

    S: Support for each other.

This document, and other resources to support school and campus safety, are available at the DCJS website at: www.dcjs.virginia.gov/virginia-center-school-and-campus-safety/k-12/resources

UPDATES TO THE CODE OF VIRGINIA (2016)

The following is a summary of the 2016 updates to the *Code of Virginia* related to school threat assessment teams and guidance for schools in implementing statutory changes.

SCOPE OF K12 THREAT ASSESSMENT TEAMS

For the past three years, Virginia public schools were required to establish threat assessment teams whose functions included the assessment and intervention with *students* whose behavior may pose a threat to the safety of the school. Effective July 1, 2016, Virginia public schools are required to establish threat assessment teams whose functions included the assessment and intervention with *individuals* whose behavior may pose a threat to the safety of the school. This change makes the school threat assessment team statute more consistent with the similar statute for threat assessment teams in institutions of higher education. The change reflects the understanding that it is not only students who may pose a threat of harm to a school, but a range of others including (but not limited to):

- Students: current and former (and potentially prospective)

- Employees: current and former (and potentially prospective)

- Parents/guardians of students

- Persons who are (or have been) in relationships with faculty, staff or students

- Contractors, vendors or other visitors

- Unaffiliated persons

School threat assessment teams should adopt policies and practices to enhance awareness of potential or developing threatening behaviors exhibited not only by students, but from a broad range of persons who might convey or indicated the intent to pose a danger to the school.

Following is the relevant section of the *Code of Virginia:*

> **§ 22.1-79.4. Threat assessment teams and oversight committees.**
>
> A. Each local school board shall adopt policies for the establishment of threat assessment teams, including the assessment of and intervention with individuals whose behavior may pose a threat to the safety of school staff or students consistent with the model policies developed by the Virginia Center for School and Campus Safety in accordance with § 9.1-184. Such policies shall include procedures for referrals to community services boards or health care providers for evaluation or treatment, when appropriate.

SCHOOL THREAT ASSESSMENT TEAMS: ACCESS TO INFORMATION

Again, as a part of enhancing consistency between public school threat assessment teams and those operating in public institutions of higher education, Virginia added language to the school threat assessment code that broadens the authority of school threat assessment team members to request information from otherwise protected or restricted sources.

The updated statute allows members of a school threat assessment team, upon a preliminary determination that an individual:

1) poses a threat of violence to self or others; or

2) exhibits significantly disruptive behavior; or

3) need for assistance;

to obtain criminal history record information regarding adult or juvenile subjects, and to obtain information from health records regarding the subject whose behavior is of concern.

In order to make a lawful request for those records under this statute, the requesting party must be a member of a public school threat assessment team established by a school board.

In addition, the school threat assessment team must have made a preliminary determination that one or more of the three requirements (Items 1–3 in this section) have been met.

The school threat assessment team members may then request and obtain the relevant records for the purpose of the threat assessment team, i.e., to assess and manage the potential threat to the school.

Note that no threat assessment team member may re-disclose any information obtained under this section, nor may they use it for any purpose other than the purposes and role of the threat assessment team. Criminal history record information or health information may *not* be shared with any other persons (other than members of the threat assessment), nor used for any other purposes (e.g., discipline, student conduct, etc.).

In regard to criminal history information obtained via the Virginia State Police Central Criminal Records Exchange (CCRE) and the Juvenile Virginia Criminal Information System (JVCIN), note that any information/records printed from a terminal (having access to the system) *must* be destroyed after the information is obtained. The threat assessment team may *not* maintain the record printed from the system access terminal, *nor may they make copies of it.* It is a violation of the *Code of Virginia* (see § 18.2-152 computer invasion of privacy and § 18.2-152.7 personal trespass by computer) to disseminate such records/information. Criminal history information may *not* be placed in a student's educational file.

Following are the relevant sections of the *Code of Virginia* regarding school threat assessment team access to otherwise protected or restricted information:

§ 22.1-79.4. Threat assessment teams and oversight committees.

F. Upon a preliminary determination by the threat assessment team that an individual poses a threat of violence to self or others or exhibits significantly disruptive behavior or need for assistance, a threat assessment team may obtain criminal history record information, as provided in §§ 19.2-389 and 19.2-389.1, and health records, as provided in § 32.1-127.1:03. No member of a threat assessment team shall redisclose any criminal history record information or health information obtained pursuant to this section or otherwise use any record of an individual beyond the purpose for which such disclosure was made to the threat assessment team.

§ 19.2-389. Dissemination of criminal history record information.

A. Criminal history record information shall be disseminated, whether directly or through an intermediary, only to:

25. Members of a threat assessment team established by a local school board pursuant to § 22.1-79.4, by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805), or by a private nonprofit institution of higher education, for the purpose of assessing or intervening with an individual whose behavior may present a threat to safety; however, no member of a threat assessment team shall redisclose any criminal history record information obtained pursuant to this section or otherwise use any record of an individual beyond the purpose that such disclosure was made to the threat assessment team;

§ 19.2-389.1. Dissemination of juvenile record information.

Record information maintained in the Central Criminal Records Exchange pursuant to the provisions of § 16.1-299 shall be disseminated only:

(x) to members of a threat assessment team established by a school board pursuant to § 22.1-79.4, by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805), or by a private nonprofit institution of higher education, to aid in the assessment or intervention with individuals whose behavior may present a threat to safety; however, no member of a threat assessment team shall redisclose any juvenile record information obtained pursuant to this section or otherwise use any record of an individual beyond the purpose that such disclosure was made to the threat assessment team;

§ 32.1-127.1:03. Health records privacy.

D. Health care entities may, and, when required by other provisions of state law, shall, disclose health records:

35. To a threat assessment team established by a local school board pursuant to § 22.1-79.4, by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805), or by a private nonprofit institution of higher education;

EXCLUSION OF CERTAIN RECORDS FROM THE VIRGINIA FREEDOM OF INFORMATION ACT

Recognizing the sensitivity of information provided through school safety audits and/or obtained through the efforts of threat assessment teams, Virginia enacted statutes that exclude certain related records from required disclosure under the Virginia Freedom of Information Act (FOIA). Records that meet the criteria for the statute, such as:

- school security plans,

- assessment components of school safety audits, and

- records received by the Virginia Department of Criminal Justice Services for the purposes of evaluating threat assessment teams

are excluded from required disclosure under the Virginia Freedom of Information Act. The custodian of the relevant record retains discretion and may release such records if they so decide.

The *Code of Virginia* also specifies limitations to the exclusion (from disclosure) in certain situations such as a request for records regarding:

1) the effectiveness of security plans after someone on school property has experienced or been threatened with personal injury, or

2) records of a threat assessment team where an individual (who has been under assessment) commits an act that causes the death or serious bodily injury (including felony sexual assault) to another.

In circumstances such as those, schools and their threat assessment teams may be compelled to provide records relevant to the circumstances.

Note that even in cases where there may be required disclosure of certain records, the statutes also limit disclosure of subset of those records, such as criminal history or health information. Those sensitive and otherwise protected records (and information from them) may not be re-disclosed without a court order.

Finally, in regard to records of a threat assessment team, where disclosure of records may be required (or released at the discretion of the custodian of the record), the persons releasing the record must remove information identifying any person who provided information to the threat assessment team under a promise of confidentiality.

Following are the relevant sections of the *Code of Virginia* regarding protection of records created by a school threat assessment team:

§ 2.2-3705.2. Exclusions to application of chapter; records relating to public safety.

The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law:

7. Security plans and specific assessment components of school safety audits, as provided in § 22.1-279.8.

Nothing in this subdivision shall be construed to prohibit the disclosure of records relating to the effectiveness of security plans after (i) any school building or property has been subjected to fire, explosion, natural disaster or other catastrophic event, or (ii) any person on school property has suffered or been threatened with any personal injury.

17. Records received by the Department of Criminal Justice Services pursuant to §§ 9.1-184, 22.1-79.4, and 22.1-279.8 or for purposes of evaluating threat assessment teams established by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805) or by a private nonprofit institution of higher education, to the extent such records reveal security plans, walk-through checklists, or vulnerability and threat assessment components.

§ 2.2-3705.4. Exclusions to application of chapter; educational records and certain records of educational institutions.

The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law:

8. Records of a threat assessment team established by a local school board pursuant to § 22.1-79.4 or by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805) relating to the assessment or intervention with a specific individual. However, in the event an individual who has been under assessment commits an act, or is prosecuted for the commission of an act that has caused the death of, or caused serious bodily injury, including any felony sexual assault, to another person, the records of such threat assessment team concerning the individual under assessment shall be made available as provided by this chapter, with the exception of any criminal history records obtained pursuant to § 19.2-389 or 19.2-389.1, health records obtained pursuant to § 32.1-127.1:03, or scholastic records as defined in § 22.1-289. The public body providing such records shall remove information identifying any person who provided information to the threat assessment team under a promise of confidentiality.

The model policy, procedures, and guidelines provided in this document are based not only on relevant Virginia statutes, but also upon a synthesis of established research and recognized standards of practice regarding threat assessment and management in school and workplace settings. For example, they are consistent with the process for identifying, assessing, and managing persons who may pose a threat as set forth in "Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates," a 2002 publication of the U.S. Secret Service and the U.S. Department of Education (Fein et al, 2002). The process described in the *Guide* was informed by research on incidents of targeted violence in schools (e.g., "The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States" (2002) that would have indicated an inclination toward or the potential for targeted violence had they been identified. Findings about the pre-attack behaviors validated use of a fact-based threat assessment process relying primarily on an appraisal of behaviors, rather than traits, as the basis for determining the nature and degree of any safety concerns, and for developing a strategic approach to reducing risk and improving the safety and well-being of the school community.

Although communicated/expressed threats of violence require assessment, the DCJS model emphasizes the identification and assessment of a broader range of concerning behaviors, including but not limited to communicated/expressed threats. The model also emphasizes that effective threat assessment can best occur in school climates of safety, respect, and emotional support – environments in which students, teachers, administrators (and, where appropriate, parents/guardians) pay attention to the social and emotional, as well as academic, needs of students and staff; and have access to assistance for addressing and resolving underlying problems.

As noted above, the *Code of Virginia* (in § 22.1-79.4) now requires each local school board to "adopt policies for the establishment of threat assessment teams, including the assessment of and intervention with *individuals* (rather than solely students) whose behavior may pose a threat to the safety of school staff or students." This is consistent with long-standing research and practice literature on workplace violence prevention and intervention that recommends that a comprehensive approach to school safety would also identify and assess threats from all sources, and not solely students.

Some non-student threats are already addressed by most local school board policies and procedures. Model policies promulgated by the Virginia School Boards Association as well as the Virginia Department of Criminal Justice Services' publication "Model Crisis, Emergency Management and Medical Response Plan" address unauthorized visitors, hostile parents, and trespassers who may include former employees and students.

Two examples of non-student threats that were previously not regularly addressed in local school board policies involved threatening behavior exhibited by 1) school division employees, and 2) persons who are (or have been) involved in abusive relationships with school division employees (or students) and exhibit violence that spills over into the school/workplace. Under the current law and when the school could reasonably know of the concerns, these examples would be included under the purview of school threat assessment teams.

While a comprehensive approach to school safety focuses on any individual who may pose a threat to the safety of school staff or students, it is expected that the majority of cases identified will involve students engaging in (or perceived to be engaging in) threatening behaviors. To that end, the following procedures and guidelines also reflect a review and synthesis of procedures currently in use in many Virginia school divisions. School divisions may (when dealing with students who may be engaging in threatening behavior) use tools designed to assess threats posed by students.

For example, a model that has been used by many schools in Virginia is based on the University of Virginia "Student Threat Assessment Guidelines" developed by the Youth Violence Project of the Curry School of Education at the University of Virginia. This model has been empirically studied and evaluated (e.g., Cornell, Allen, & Fan, 2012; Cornell, Gregory, & Fan, 2011; Cornell, Sheras, Gregory, & Fan, 2009) and, in 2013, the model was added to the National Registry of Evidence-based Programs and Practices (NREPP). The model was derived from threat assessment principles and adapted for use in assessing students who engaged in threatening communications and behaviors in schools. The "Student Threat Assessment Guidelines" specify a series of decision steps and related criteria and offer an alternative to zero tolerance practices in addressing student threats. References and links to the University of Virginia Youth Violence Project and the "Student Threat Assessment Guidelines" are provided in the resource section of this document.

MODEL POLICY, PROCEDURES, AND GUIDELINES

The threat assessment policies and procedures contained herein are models that are based on a synthesis of best practices or established standards of practice, and are consistent with Virginia law. They are not intended to be prescriptive. Although required to adopt policies for the establishment of threat assessment teams, local school boards have authority to establish any policies or procedures that are consistent with these model policies and procedures.

The Model School Board Policy on Threat Assessment presented here is based on the requirements of § 22.1-79.4, *Code of Virginia* requiring local school boards to adopt policies for the establishment of threat assessment teams and prescribing the composition and responsibilities of teams as well as related referral and reporting requirements. The model policy also reflects best practices or accepted standards of practice.

MODEL SCHOOL BOARD POLICY ON SCHOOL THREAT ASSESSMENT

- The superintendent shall establish, for each school, a threat assessment team, for the assessment of and intervention with individuals whose behavior may pose a threat to the safety of school staff or students.

- A particular threat assessment team may serve one or more schools as determined by the superintendent.

- Each team shall include persons with expertise in counseling, instruction, school administration, human resources, and law enforcement.

- Each team shall:

    - Provide guidance to students, faculty, and staff regarding recognition of threatening or aberrant behavior that may represent a threat to the community, school, or self;

    - Identify members of the school community to whom threatening behavior should be reported; and

    - Implement school board policies for the assessment of and intervention with individuals whose behavior poses a threat to the safety of school staff or students.

- The superintendent may establish a committee (operating within the division) charged with oversight of the threat assessment team(s). An existing committee may be designated to assume the oversight responsibility; however, any such committee established for oversight of the threat assessment team(s) shall include individuals with expertise in human resources, education, school administration, mental health, and law enforcement.

- All school division employees, volunteers, and contractors are required to report any expressed threat(s) or behavior(s) that may represent a threat to the community, school, or self.

- In cases where determined to be appropriate, teams shall follow established procedures for referrals to community services boards or health care providers for evaluation or treatment.

- Regardless of threat assessment activities, disciplinary action and referral to law enforcement are to occur as required by school board policy and the *Code of Virginia*.

- Upon a preliminary determination that a ***student*** poses a threat of violence or physical harm to self or others, the threat assessment team shall immediately report its determination to the superintendent or designee. The superintendent or designee shall immediately attempt to notify the student's parent or legal guardian.

    - Nothing in this policy shall preclude school division personnel from acting immediately to address an imminent threat.

    - Nothing in this policy shall preclude the threat assessment team from notifying the superintendent (or designee) of any individual (other than a student) who poses a threat of violence or physical harm to self or others.

- Upon a preliminary determination (by the threat assessment team) that an individual poses: 1) a threat of violence to self or others or, 2) exhibits significantly disruptive behavior or, 3) need for assistance, members of the threat assessment team may request & obtain criminal history record information and health records.

  - No member of a threat assessment team shall re-disclose any criminal history record information or health information obtained pursuant to this section or otherwise use any record of an individual beyond the purpose for which such disclosure was made to the threat assessment team.

  - The threat assessment team may ***not*** maintain the criminal history record printed from the system access terminal, nor may they make copies of it.

  - Criminal history information may ***not*** be placed in a student's educational file.

- Each threat assessment team established pursuant to *Code of Virginia*, § 22.1-79.4 shall report quantitative data on its activities according to guidance developed by the Virginia Department of Criminal Justice Services.

Reference statutory authority for policy: *Code of Virginia*, § 22.1-79.4

Refer to: [*School division lists here the specific local school regulation(s) setting forth student threat assessment procedures and any closely related regulations.*]

The following model procedures are consistent with the requirements of the *Code of Virginia* and reflect best practices or accepted standards of practice identified in school divisions and workplaces in Virginia and across the nation. Such standards of practice include "Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates;" the "Guide for Developing High-Quality School Emergency Operations Plans," and "Workplace Violence Prevention and Intervention: American National Standard." Elements of the procedure that are aligned with *Code of Virginia* requirements include a cross-reference to the applicable section of the *Code*.

MODEL PROCEDURES FOR SCHOOL THREAT ASSESSMENT PROGRAMS

PURPOSE

The purpose of this document is to establish procedures for the assessment and intervention with individuals whose behavior poses a threat to the safety of school staff or students.

DEFINITIONS

- A **threat** is a concerning communication or behavior that indicates that an individual poses a danger to the safety of school staff or students through acts of violence or other behavior that would cause harm to self or others. The threat may be expressed/communicated behaviorally, orally, visually, in writing, electronically, or through any other means; and is considered a threat regardless of whether it is observed by or communicated directly to the target of the threat or observed by or communicated to a third party; and regardless of whether the target of the threat is aware of the threat.

- A **threat assessment** is a fact-based process emphasizing an appraisal of observed (or reasonably observable) behaviors to identify potentially dangerous or violent situations, to assess them, and to manage/address them.

- **Aberrant behavior** is that which is atypical for the person or situation and causes concern for the safety or well-being of those involved. Aberrant behavior for an individual involves actions, statements, communications or responses that are unusual for the person or situation; or actions which could lead to violence toward self or others; or are reasonably perceived as threatening or causing concern for the well-being of the person. These can include (but are not limited to):

  - Unusual social distancing or isolation of subjects from peers and family members;

  - Sullen or depressed behavior from an otherwise friendly and positive person;

  - Out of context outbursts of verbal or physical aggression;

  - Increased levels of agitation, frustration and anger;

  - Confrontational, accusatory or blaming behavior;

  - An unusual interest in or fascination with weapons; and/or

  - Fixation on violence as means of addressing a grievance.

- A **low risk threat** is one in which the individual/situation does not appear to pose a threat of violence or serious harm to self/others, and any exhibited issues/concerns can be resolved easily.

- A **moderate risk threat** is one in which the person/situation does not appear to pose a threat of violence, or serious harm to self/others, at this time; but exhibits behaviors that indicate a continuing intent and potential for future violence or serious harm to self/others; and/or exhibits other concerning behavior that requires intervention.

- A **high risk threat** is one in which the person/situation appears to pose a threat of violence, exhibiting behaviors that indicate both a continuing intent to harm and efforts to acquire the capacity to carry out the plan; and may also exhibit other concerning behavior that requires intervention.

- An **imminent threat** exists when the person/situation appears to pose a clear and immediate threat of serious violence toward others that requires containment and action to protect identified or identifiable target(s); and may also exhibit other concerning behavior that require intervention.

- A **direct threat** is one in which the person poses a significant risk to the health or safety of others that cannot be eliminated by a modification of policies, practices, or procedures, or by the provision of auxiliary aids or services. The direct threat standard applies when the threat assessment team or school administration determines that a subject poses a direct threat, and the administration also determines that applicable disciplinary procedures are not available or sufficient to mitigate the threat. If the administration makes such a determination, the school division is not required to permit the student to participate in or benefit from the services, programs, or activities of the division. A determination that a person with a disability poses a direct threat may not be based on generalizations or stereotypes about the effects of a particular disability and must be based on an individualized assessment, based on reasonable judgment relying on current medical evidence or on the best available objective evidence, to determine: the nature, duration, and severity of the risk; the probability that the potential injury will actually occur; and whether reasonable modifications of policies, practices, or procedures will mitigate the risk.

THREAT ASSESSMENT TEAM

- The threat assessment team must include persons with expertise in counseling (e.g., a guidance counselor, a school psychologist and/or school social worker), instruction (e.g., a teacher or administrator with instructional experience), school administration (e.g., a principal or other senior administrator from the school(s) covered by the team and human resource professionals); and law enforcement (typically a school resource officer). Other school staff (or community resources) may serve as regular members on the team, or be consulted during the threat assessment process, as appropriate, and as determined by the team. [Note: § 22.1-79.4.D., *Code of Virginia,* requires school threat assessment teams to include persons with expertise in counseling, instruction, school administration; and law enforcement. Note that Human Resources is not one of the areas of expertise required (by statute) to be part of the threat assessment team. However, given that Virginia law requires schools to have processes for the assessment of and intervention with individuals whose behavior may pose a threat to the safety of school staff or students (i.e., including faculty and staff), schools will generally want to include involvement by human resource professionals when possible].

- School threat assessment teams should have a designated team leader, typically a principal or other senior administrator for the school(s)

- Team members shall work collaboratively with each other, with other school staff, and (as appropriate) with community resources to support the purposes of the team and the safety of the school and its students and staff.

- The threat assessment team leader may designate a subset of team members to triage cases reported to the team. This triage process serves to screen cases and determine their appropriateness for review and/or action by the full team. If the team elects to implement a triage process, at least two members of the team will review initial reports of concern to determine if existing resources and mechanisms are sufficient to address those concerns, or whether the full team should further assess and manage the situation. All members of the team should have opportunity to review triaged cases to ensure they have been adequately addressed.

- Unless it is not feasible to do so, all team members should be involved with the assessment and intervention of individuals whose behavior poses a threat to the safety of school staff or students.

- Team members shall actively, lawfully, and ethically communicate with each other; with school administrators; and with other school staff who have a need to know particular information to support the safety and well-being of the school, its students and its staff.

- In fulfilling statutory responsibilities, school threat assessment teams shall:

  – Provide guidance to students, faculty, and staff regarding recognition of threatening behavior that may represent a threat by conducting presentations, broadly disseminating relevant information, and ensuring access to consultation from threat assessment teams;

  – Clearly identify members of the school community to whom threatening behavior should be reported;

  – Implement school board policies in an effective manner for the assessment of and intervention with individuals whose behavior poses (or may pose) a threat to the safety of school staff or students, including (where appropriate) referrals to community services boards or health care providers for evaluation or treatment. (§ 22.1-79.4. A&C., *Code of Virginia*).

- *If established by the superintendent*, the school division-level oversight team shall oversee and provide support for school threat assessment teams. [Note: § 22.1-79.4.B., *Code of Virginia,* authorizes *(but does not require)* the superintendent of each school division to establish a committee charged with oversight of the threat assessment teams operating within the division, which may be an existing committee established by the division. If such a committee is established (or designated) with the purpose of oversight of the threat assessment team(s), it is required that the oversight committee include individuals with expertise in human resources, education, school administration, mental health, and law enforcement.]

  – The team shall include a senior division administrator (e.g., Assistant Superintendent for Administration) and senior division administrators in school safety, in student services, and in human resources in consultation with designated representatives of the *(specify)* community services board and *(locality)* police department (or sheriff's office).

  – The school division level threat assessment team shall provide oversight to school level threat assessment teams; ensure that procedures are maintained for effective information sharing between the school division and community mental health and law enforcement agencies; assess the effectiveness of the threat assessment process throughout the school division; and recommend changes to policies and procedures, as needed, to ensure an effective threat assessment process reflecting known best practices.

PROCEDURES

- Identifying and Reporting Threats

  – When an individual makes a threat or engages in concerning communications or behaviors that suggest the likelihood of a threatening situation, the *[School Division]* **Threat Assessment Guidelines** shall be followed. The goal of the threat assessment process is to take appropriate preventive or corrective measures to maintain a safe and secure school environment, to protect and support potential victims, and to provide assistance, as needed, to the individual being assessed.

  – Regardless of threat assessment activities, disciplinary action and referral to law enforcement are to occur when required by school board policy or the *Code of Virginia*.

  – Threats of self-harm by students, also require compliance with § 22.1-272.1, *Code of Virginia* and with applicable school board policies and regulations *[cite Division Regulation #]*. For any individual, when threats of self-harm are accompanied by threats to harm others, or investigation suggests the existence of a threat to others, the threat assessment team shall be notified and take appropriate action to prevent acts of violence. The threat assessment team shall work collaboratively with other entities involved in the case.

  – All school division employees, volunteers, and contractors are required to report immediately to the designated school administrator any expression of intent to harm another person, concerning communications, or concerning behaviors that suggest an individual may intend to commit an act of violence.

  – Anyone who believes that a person or situation poses a clear and immediate threat of serious violence that requires containment shall notify school security and/or law enforcement in accordance with school board policies on Critical Incident Response *[cite Division Regulation #]*.

- In accordance with § 22.1-279.3:1, *Code of Virginia* certain types of threats require immediate notification to law enforcement. The principal shall immediately report to the local law enforcement agency:

  - Assault and battery that results in bodily injury, sexual assault, death, shooting, stabbing, cutting, or wounding of any person, or stalking of any person, on a school bus, on school property, or at a school-sponsored activity;
  - Threats against school personnel while on a school bus, on school property or at a school-sponsored activity;
  - Illegal carrying of a firearm (see § 22.1-277.07) onto school property;
  - Illegal conduct involving firebombs, explosive materials or devices, or hoax explosive devices, or explosive or incendiary devices, or chemical bombs, on a school bus, on school property, or at a school-sponsored activity;
  - Threats or false threats to bomb (see § 18.2-83) made against school personnel or involving school property or school buses;

- The school administrator shall also immediately report any act noted above that may constitute a criminal offense to the parents and/or guardians of any minor student who is alleged to have committed the act and shall report that the incident has been reported to local law enforcement, as required by law. The school administrator shall inform the parents and/or guardians that they may contact local law enforcement for further information, if they so desire. In addition, the school administrator may report other threats to the local law enforcement agency as necessary and appropriate.

- Assessing Threats

  - When a threat is reported, the school administrator and/or threat assessment team leader shall initiate an initial inquiry/triage and, in consultation with the threat assessment team, make a determination of the seriousness of the threat as expeditiously as possible in accordance with *[school division]* **Student Threat Assessment Guidelines**.

Upon notification of threatening behavior or communications, the school administrator or threat assessment team leader shall determine if an imminent threat is believed to exist. If the individual appears to pose a clear and immediate threat of serious violence, the administrator shall notify law enforcement in accordance with School Board policies on Critical Incident Response *[cite Division Regulation #]*. [Note: In accordance with "Model Crisis, Emergency Management and Medical Response Plan", school responses may include actions such as evacuation, lockdown, and shelter-in-place.]

  - If there is no reasonably apparent imminent threat present, or once such an imminent threat is contained, the threat assessment team leader shall ensure that the situation is screened/triaged to determine if the full threat assessment team needs to be involved. This triage may include (as necessary and appropriate):

    - Review of the threatening behavior or communication.
    - Review of school and other records for any prior history or interventions with the individual(s) involved.
    - Conducting timely and thorough interviews (as necessary) of the person(s) who reported the threat, the recipient(s) or target(s) of the threat, other witnesses who have knowledge of the threat, and where reasonable, the individual(s) who allegedly engaged in the threatening behavior or communication. The purpose of the interviews is to evaluate the individual's threat in context, so that the meaning of the threat and intent of the individual can be determined.

  - If it is determined that the threat is no identifiable or a low threat of violence or harm to self or others, and the threat assessment team determines that no further assessment, intervention, or monitoring is required at this time to prevent violence:

    - The threat assessment team leader shall ensure that the incident and review is adequately documented via *[cite School Division documentation source here]*. The threat assessment team shall maintain the documentation in accordance with School Board policy. [NOTE: A sample **Threat Assessment and Response Form** is provided as part of this guidance document. The form is available at the DCJS website and may be adapted to meet the needs of the school].
    - If the individual (about whom the report was made) does not pose a threat but could benefit from or is in need of some other need of assistance, the threat assessment team leader shall ensure that the individual is referred to the appropriate school or community-based resources.

- – If it cannot be determined with a reasonable degree of confidence that the alleged threat is no/low threat, then a more in-depth assessment is to be undertaken by the threat assessment team to determine the nature and degree of any safety concerns and to develop strategies to prevent violence and reduce risk, as necessary. The assessment may include but not be limited to reviews of records; interview and consultation with staff, students or community who know the individual; and interviews of the individual and the target/recipient of the threat(s).

- – Based on information collected, the school threat assessment team shall determine strategies to mitigate the threat and provide intervention and assistance to those involved, as needed.

- – Upon a determination that a student poses a threat of violence or physical harm to self or others, a threat assessment team shall immediately report its determination to the superintendent or designee. The superintendent or designee shall immediately attempt to notify the student's parent or legal guardian. (§ 22.1-79.4.D., *Code of Virginia* and § 22.1-272.1., *Code of Virginia*).

- – In instances where the threat is deemed moderate risk or high risk, or requires further intervention to prevent violence or serious harm, the school administrator ***shall*** notify the parent and/or guardian of any student who is the target/recipient of a threat as well as the parent and/or guardian of any student who made the threat.

- – In cases involving no/low risk threats, the school administrator ***may*** notify the parent and/or guardian of any student who is the target/recipient of a threat and/or may notify the parent and/or guardian of any student who made the threat.

- Intervening, Monitoring, and Resolving Threats

  - – If it is determined that an individual poses a threat of violence, the threat assessment team shall develop, implement, and monitor an individualized plan to intervene with, address and reduce the threat. The threat assessment team shall maintain documentation in accordance with School Board policy.

  - – The threat assessment team shall assist individual(s) within the school who engaged in threatening behavior or communication, and any impacted staff or students, in accessing appropriate school and community-based resources for support and/or further intervention.

  - – For each case, a member of the threat assessment team shall be designated as a case manager to monitor the status of the individual(s) of concern (in that case) and to notify the threat assessment team of any change in status, response to intervention/referrals, or additional information that would be cause for a re-assessment and changes in intervention strategies. Updates regarding the case are to be documented in accordance with School Board policy. These updates are to be submitted regularly (e.g., at least every 30 days) until the case is resolved and is no longer assessed to pose a threat to the school or its staff or students. [NOTE: A sample **Threat Assessment and Response Form** is provided as part of this guidance document. The form is available at the DCJS website and may be adapted to meet the needs of the school].

  - – Resolution and closure of the case is to be documented in accordance with School Board policy. [NOTE: A sample **Threat Assessment and Response Form** is provided as part of this guidance document. The form is available at the DCJS website and may be adapted to meet the needs of the school].

See also:
- Student Conduct Policies (specify those dealing with threat/intimidation)
- Suicide Prevention Policies and Procedures
- Critical Incident Response Policies and Procedures
- § 22.1-79.4., *Code of Virginia*

SCHOOL THREAT ASSESSMENT GUIDELINES

VIRGINIA C.A.R.E.S. FOR SCHOOL AND CAMPUS SAFETY

Threat assessment in Virginia public educational settings, falls under the umbrella of the **Virginia C.A.R.E.S. for Schools and Campuses** program which was developed in 2016 to illustrate initiatives by the DCJS Virginia Center for School and Campus Safety to support schools and campuses in enhancing the safety and well-being of educational settings across the Commonwealth. The Virginia C.A.R.E.S program recognizes that threat assessment and management is but one part of a larger and on-going approach to support and enhance school & campus safety. School and campus safety (and well-being) are sustained and enhanced through:

> **C**: Caring and connection to build a positive school/campus climate;
>
> **A**: Awareness of resources and reporting options;
>
> **R**: Recognition of (and response to) aberrant and concerning behaviors;
>
> **E**: Engagement with the community and will persons (within the school or campus) for whom there is concern; and
>
> **S**: Support for each other.

Threat assessment is to be viewed as one component of an overall strategy to reduce school violence and implemented within the larger context of strategies to ensure schools are safe and secure environments. The principle objective of school violence-reduction strategies should be to create cultures and climates of safety, respect, and emotional support within the school.

Among other school safety strategies employed by *[school division]* are:

[School division to insert list of strategies employed]; examples include:

- Effective communication among and between school staff, students and parents/guardians of students

- School climate assessments

- Emphasis on school connectedness

- Strong, but caring, stance against the code of silence

- Bullying prevention and intervention

- School-law enforcement partnerships including school resource officers

- Collaborative relationships with mental health, social services, and other community-based resources

- Planning and preparation to deal with, respond to, and recover from potential crises

- Physical security

PRINCIPLES OF THREAT ASSESSMENT

Threat assessment is a systematic process that is designed to:

1) Identify individual(s)/situation(s) whose behavior causes concern for violence

2) Gather additional relevant information in a lawful and ethical manner

3) Assess the individual(s)/situation(s) in context based on the totality of the information available

4) Manage the individual situation to prevent violence and mitigate impact of harm

Assumptions

Assumptions reflected in the guidelines are informed by findings of the *Safe School Initiative,* as well as other research about targeted violence occurring in, or related to educational settings. Among key findings:

- Incidents of targeted violence at school/workplaces are rarely sudden, impulsive acts.

- In addition to students, others also engage in targeted violence in schools, including administrators, teachers, other staff, parent/guardians of students, contractors, people in relationships with staff or students, and even people with no connection with the school.

- Prior to most incidents of targeted violence, other people knew about the individual's idea and/or plan to attack.

- Most individuals who perpetrated violence engaged in some behavior, prior to the incident, that caused others to have serious concerns about their behavior and/or well-being.

- Many individuals who perpetrated violence had significant difficulties with losses or failures. Many were suicidal.

- Many felt bullied, persecuted, or injured by others prior to engaging in violence.

- In many cases, others (e.g., staff, students, peers, family members, etc.) were involved in some way, such as helping with plans or preparation for violence, encouraging violence, or failing to report (or take other steps) to prevent violence.

- Most individuals who perpetrated violence did not threaten their targets directly prior to engaging in violence.

- Violence is a dynamic process. No one is either always dangerous or never dangerous. Rather, the risk for violence is an interaction between the individual, the situation, circumstances, provocations and inhibitory factors that are present.

The fact that most individuals engaged in pre-incident planning and preparation, and frequently shared their intentions, plans and preparations with others, suggests that the information (about targeted violence) is likely to be uncovered through a sound threat assessment process.

Targeted violence is the end result of a process of thinking and behavior that begins with an idea (i.e., to use violence to address a real or perceived grievance), progresses to development of a plan, moves on to preparation (e.g. acquiring the means (e.g., weapons, training, capacity, access) to carry out the plan, and culminates in an attack. A graphic representation of the "Pathway to Violence" process is shown in Figure 1.

Figure 1: The Pathway to Violence
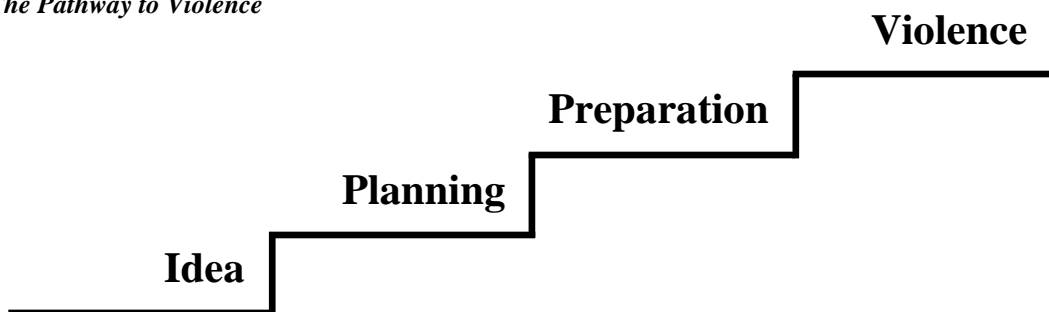
The steps along this path indicate opportunities to observe, identify and intervene with threatening and/or aberrant behaviors that cause concern for violence by, or the well-being of, the individual. Frequently, information about an individual's ideas, plans and preparations for violence can be observed before violence can occur. However, information is likely to be scattered and fragmented. For example, a teacher may see a certain set of behaviors of an individual in her class, a coach observes other behaviors or expressed thoughts by the individual, a school resource officer has other concerns, and a school administrator is aware of certain conduct violations. The challenge, and the key, is to act quickly upon initial reports of concern, gather other pieces of the puzzle, and assemble them to determine what picture emerges.

Principles

The appraisal of risk in a threat assessment focuses on actions/behaviors, communications, and specific circumstances that might suggest that an individual intends to engage in violence and is planning or preparing for that event. The threat assessment process is centered upon an analysis of the known (or reasonably knowable) behavior(s) in a given situation.

According to threat assessment experts, several core principles that form the foundation of the threat assessment process include:

1. **The central question in a threat assessment inquiry is whether an individual poses a threat (i.e., is building the capability to cause harm), not just whether the person has made a threat (directly expressed intent to harm).**
   Research on targeted violence in schools and workplaces has found that fewer than 20 percent of violent perpetrators communicated a direct or conditional threat to their target before the violence. In the majority of incidents of targeted violence, perpetrators did not directly threaten their targets, but they did communicate their intent and/or plans to others before the violence. This indirect expression or third party communication of intent to cause harm is often referred to as "leakage". Individuals who are found to *pose* threats (i.e., engaged in violence) frequently *do not make* threats to their targets. The absence of a direct threat should not, by itself, cause a team to conclude that a subject does not pose a threat or danger to others.

2. **Targeted violence is the end result of an understandable, and often discernible, process of thinking and behavior, often referred to as the Pathway to Violence as noted above and referenced in Figure 1.**
   Individuals who have committed targeted violence did not "just snap," but engaged in a process of thought and escalation of action over days, weeks, months, and even years.

3. **Targeted violence stems from an interaction among the Subject(s), Target(s), Environment and Precipitating Incidents.**
   Identifying, preventing and intervening with acts of violence requires a focus on these four components and their interaction. A focus on the *Subject/individual* of concern should provide insight into how the individual perceives and deals with conditions, often stressful, in his or her life and the intensity of effort they direct toward planning and preparation for violence. A focus on the *Target* examines choices and coping strategies they are using or responding with that may increase or decrease their risk for harm. A focus on the *Environment* examines school/workplace climate and systemic issues that contribute to the risk of violence, or do not discourage it. Finally, a focus on *Precipitating* events should examine critical stressors or events such as bullying, personal losses, enforcement actions, or even threat assessment team interventions, that may increase or decrease the risk for violence.

4. **An investigative, skeptical, inquisitive mindset is critical to successful threat assessment.**
   Those who carry out threat assessment must strive to be both accurate and fair, continuing throughout the assessment process both to gather pieces of information and to fit the pieces into a larger picture and to gain understanding of the context and situation.

5. **Effective assessment is based upon facts and observations of behavior, rather than on characteristics, traits or profiles. Perpetrator "profiles" do not provide a reliable basis for making judgments of the threat posed by a particular individual.**

6. **An "integrated systems approach", coordinating between local agencies and service systems within the school and the community (e.g., mental health services, law enforcement) should guide threat assessment and management processes.**

Relationships with agencies and service systems within the school (e.g., school psychologist, school social worker, school-based mental health clinicians, administrators, disciplinary officers, human resources, etc.,) and community (e.g., mental health, juvenile justice, child welfare, law enforcement) are critical to identifying, assessing, and managing individuals who are on a path to carrying out an act of targeted violence.

IDENTIFYING AND REPORTING THREATS

All school division employees, volunteers, and contractors are required to report immediately to the school administrator or designee any expression of intent to harm another person, concerning communications, or concerning behaviors that suggest a student may intend to commit an act of targeted violence.

The school threat assessment team shall strive to make the reporting process both understandable and highly accessible and to discourage a "code of silence" that may be a barrier to reporting. Faculty and staff, students, volunteers, and other members of the school community need to know:

- their role and responsibility to report concerns;

- what to report;

- where and how to report it;

- that reports are wanted and will be acted upon appropriately.

Members of the school community should be encouraged on an ongoing basis to report any threatening communication or troubling behavior and be reminded that reporting is an act of caring and not "snitching" or "tattling."

Section 8.01-47, *Code of Virginia,* enacted in 2013, grants immunity from all civil liability to any person who, in good faith with reasonable cause and without malice, reports, investigates, or causes an investigation to be made into information that any person poses a credible danger of serious bodily injury or death to any other person on school property.

All threats of self-harm also require compliance with § 22.1-272.1, *Code of Virginia* and with applicable school board policies and regulations [cite Division Regulation #]. However, when threats of self-harm are accompanied by threats to harm others, or investigation suggests the existence of a threat to others, the threat assessment team shall be notified and take appropriate action to prevent acts of targeted violence.

Anyone who believes that a person or situation poses a clear and immediate threat of serious violence that requires containment should notify school security and law enforcement in accordance with school board policies on Critical Incident Response *[cite Division Regulation #].*

ASSESSING AND CLASSIFYING THREATS

When a threat is reported, the school administrator and/or threat assessment team leader shall initiate an initial inquiry/triage and, in consultation with the threat assessment team, make a determination of the seriousness of the threat as expeditiously as possible in accordance with *[school division]* **Student Threat Assessment Guidelines**.

Upon notification of threatening behavior or communications, the school administrator or threat assessment team leader shall determine if an imminent threat is believed to exist. If the individual appears to pose a clear and immediate threat of serious violence, the administrator shall notify law enforcement in accordance with School Board policies on Critical Incident Response *[cite Division Regulation #]*. [Note: In accordance with "Model Crisis, Emergency Management and Medical Response Plan", school responses may include actions such as evacuation, lockdown, and shelter-in-place.]

If there is no reasonably apparent imminent threat present, or once such an imminent threat is contained, the threat assessment team leader shall ensure that the situation is screened/triaged to determine if the full threat assessment team needs to be involved. This triage may include (as necessary and appropriate):

- Review of the threatening behavior or communication.

- Review of school and other records for any prior history or interventions with the individual(s) involved.

- Conducting timely and thorough interviews (as necessary) of the person(s) who reported the threat, the recipient(s) or target(s) of the threat, other witnesses who have knowledge of the threat, and where reasonable, the individual(s) who allegedly engaged in the threatening behavior or communication. The purpose of the interviews is to evaluate the individual's threat in context, so that the meaning of the threat and intent of the student can be determined.

If it is determined that the threat is not identifiable or a low threat of violence or harm to self or others, and the threat assessment team determines that no further assessment, intervention, or monitoring is required at this time to prevent violence:

- The threat assessment team leader shall ensure that the incident and review is adequately documented via *[cite School Division documentation source here]*. The threat assessment team shall maintain the documentation in accordance with School Board policy. [NOTE: A sample **Threat Assessment and Response Form** is provided as part of this guidance document. The form is available at the DCJS website and may be adapted to meet the needs of the school].

- If the individual (about whom the report was made) does not pose a threat but could benefit from or is in need of some other need of assistance, the threat assessment team leader shall ensure that the individual is referred to the appropriate school or community-based resources.

If it cannot be determined with a reasonable degree of confidence that the alleged threat is no/low threat, then a more in-depth assessment is to be undertaken by the threat assessment team to determine the nature and degree of any safety concerns and to develop strategies to prevent violence and reduce risk, as necessary. The assessment may include but not be limited to reviews of records; interview and consultation with staff, students or community who know the individual; and interviews of the individual and the target/recipient of the threat(s).

Based on information collected, the school threat assessment team shall determine strategies to mitigate the threat and provide intervention and assistance to those involved, as needed.

Upon a determination that a student poses a threat of violence or physical harm to self or others, a threat assessment team shall immediately report its determination to the superintendent or designee. The superintendent or designee shall immediately attempt to notify the student's parent or legal guardian. (§ 22.1-79.4.D., *Code of Virginia* and § 22.1-272.1., *Code of Virginia*).

In instances where the threat is deemed moderate risk or high risk, or requires further intervention to prevent violence or serious harm, the school administrator *shall* notify the parent and/or guardian of any student who is the target/recipient of a threat as well as the parent and/or guardian of any student who made the threat.

In cases involving no/low risk threats, the school administrator *may* notify the parent and/or guardian of any student who is the target/recipient of a threat and/or may notify the parent and/or guardian of any student who made the threat.

Key Questions

The following are examples of key areas of questioning to help assess the situation. Note that this is not intended as an exhaustive or complete list of areas of inquiry. Additional questions may be asked for clarification and/or to probe more deeply to fully understand the circumstances.

Before conducting an interview with an individual of concern, threat assessment team members are best served by being well acquainted with the facts that brought the individual to the attention of school administrators and others. In addition, team members should review available information concerning the individual's background, interests, and behaviors.

Interview with threat recipient(s)/target(s) and witness(es): Individuals who have been identified as potential targets of the subject of concern should also be interviewed where possible, along with any persons who witnessed the concerning behavior. The threat assessment team should inform the subject of the interview that the primary purpose of that interview is to gather information about a possible situation of concern and, where possible, prevent harm to staff or students.

A potential target should be asked about their relationship to the subject of concern and queried about recent interactions with that subject. The interviewer should gather information about grievances and grudges that the subject of concern may hold against a target or against others. Interviews with potential targets should be conducted with special sensitivity. Care must be taken to gather information without unduly alarming a potential target. If the threat assessment team believes that there may be a risk of violence to an identified target, that target should be offered assistance and support for their safety.

The assessment process facilitates increased and revised understanding of issues over time. That is, when new information is made available to the team during or after the initial assessment, the team should review the new information and re-evaluate the threat accordingly. The team will want to maintain contact with the target/recipient to obtain information about any further behaviors of concern, improvements in the situation or other relevant developments.

Review of records/consultation with staff members who know the individual best: Background information can inform the threat assessment team's approach to and questioning of the individual. This information may help the threat assessment team determine whether the student poses a threat to particular targets. In addition, knowledge of background information concerning the student prior to the interview may help the threat assessment team judge whether the individual is forthcoming and straightforward. Some areas for background information from records and consultation with adults in school who know the subject best include:

- Recent (and perhaps historical) work or school performance history

- Disciplinary or personnel actions

- Prior threat assessment team contacts

- Law enforcement or security contacts at school and in the community

- Prior critical involvement with mental health or social services

- Presence of known problems in the life of the individual

- Current or historical grievances that may be related to the behavior of concern

- Online searches: internet, social media, email, etc.

Interview with Individual of Concern: Generally, an individual who is part of the school (staff or student) should be asked directly about his or her actions and intentions. Many subjects will respond forthrightly to direct questions approached in a non-judgmental manner. An interview conducted during a threat assessment inquiry can elicit important information that permits the threat assessment team to better understand the situation of the individual and possible targets. This understanding, in turn, will help the threat assessment team to assess the risk of violence that the individual may pose in a given situation. Interviews with the individual of concern also can generate leads for further inquiry.

An interview can also send the message to the individual that his or her behavior has been noticed and has caused concern. Interviews give individuals of concern the opportunity to tell their perspectives, background and intent; to be heard and experience support/empathy where appropriate; and to reassess and redirect their behavior away from activities that are of concern. The interview may suggest to a subject who has mixed feelings about attacking, that there are people who are interested in his or her welfare, and that there are better, more effective ways to deal with problems or with specific people.

Although an interview with a subject of concern can provide valuable information, relying too heavily (or solely) on that interview as a basis for making judgments about whether that student poses a threat is likely to present problems. The information offered by the subject may be incomplete, misleading, or inaccurate. It therefore is important to collect information to corroborate and verify information learned from the interview.

Assessing Potential Threatening Behavior

Information gathered in a threat assessment inquiry should be examined for evidence of behavior and conditions that suggest that the individual of concern is planning and preparing for an act of violence or to cause harm to self or others. Based on a review of the totality of the information available, the threat assessment team should seek to answer the following questions:

1. **What are the subject's motive(s) and goals? / What first brought him/her to someone's attention?**

    – Does the subject have a major grievance or grudge? Against whom?

    – Does the situation or circumstance that led to these statements or actions still exist?

    – What efforts have been made to resolve the problem and what has been the result?

    – Does the subject feel that any part of the problem is resolved or see any alternatives?

    – Has the subject previously come to someone's attention or raised concern in a way that suggested he or she needs intervention or supportive services?

2. **Have there been any communications suggesting ideas, intent, planning or preparation for violence?**

    – What, if anything, has the subject communicated to someone else (targets, friends, co-workers, others) or written in a diary, journal, email, or Web site concerning his or her grievances, ideas and/or intentions?

    – Do the communications provide insight about ideation, planning, preparation, timing, grievances, etc?

    – Has anyone been alerted or "warned away"?

3. **Has the subject shown any inappropriate interest in, fascination, and/or identification with other incidents of mass or targeted violence (e.g., terrorism, rampage violence, school/workplace shootings, mass murderers):**

    – Previous perpetrators of targeted violence;

    – Grievances of perpetrators

    – Weapons / tactics of perpetrators;

    – Effect or notoriety of perpetrators

4. **Does the subject have (or are they developing) the capacity to carry out an act of targeted violence?**

    – How organized is the subject's thinking and behavior?

    – Does the subject have the means (e.g., access to a weapon) to carry out an attack?

    – Are they trying to get the means to carry out an attack?

    – Have they developed the will and ability to cause harm?

    – Are they practicing or rehearsing for the violence?

    – What is the "intensity of effort" expended in attempting to develop the capability?

5. **Is the subject experiencing hopelessness, desperation, and/or despair?**

    – Is there information to suggest that the subject is feeling desperation and/or despair?

    – Has the subject experienced a recent failure, loss and/or loss of status?

    – Is the subject having significant difficulty coping with a stressful event?

    – Has the subject engaged in behavior that suggests that he or she has considered ending their life?

6. **Does the subject have a positive, trusting, sustained relationship with at least one responsible person?**

    – Does the subject have at least one friend, colleague, family member, or other person that he or she trusts and can rely upon for support, guidance or assistance?

    – Is that trusted person someone that would work collaboratively with the team for the well-being of the subject of concern?

    – Is the subject emotionally connected to other people or becoming more socially isolated?

7. **Does the subject see violence as an acceptable, desirable – or the only – way to solve a problem?**

    – Does the subject still perceive alternatives to violence to address their grievances?

    – Does the setting around the subject (friends, colleagues, family members, others) explicitly or implicitly support or endorse violence as a way of resolving problems or disputes?

    – Has the subject been "dared" by others to engage in an act of violence?

    – Has the subject expressed sentiments of finality or desperation to address grievances?

8. **Are the subject's conversation and "story" consistent with his or her actions?**
    – Does information from collateral interviews and from the subject's own behavior confirm or dispute what the subject says is going on and how they are dealing with it?

    – Is there corroboration across sources or are the subject's statements at odds with their actions?

9. **Are other people concerned about the subject's potential for violence?**

    – Are those who know the subject concerned that he or she might take action based on violent ideas or plans?

    – Are those who know the subject concerned about a specific target?

    – Are persons around the subject engaging in protective actions (e.g. distancing, avoiding, minimizing conflict, etc.)

10. **What circumstances might affect the likelihood of an escalation to violent behavior?**

    – What events or situations in the subject's life (currently or in the near future) may increase or decrease the likelihood that the subject will engage in violent behavior?

    – Are threat assessment team interventions escalating, de-escalating, or having no effect on movement toward violence?

    – What is the response of others who know about the subject's ideas or plans?

        ▪ Actively discourage subject from acting violently,

        ▪ Encourage the subject to attack,

        ▪ Deny the possibility of violence,

        ▪ Passively collude with an attack, etc.?

Thoughtful consideration of the answers to the above key questions will produce a sound foundation for the threat assessment team's response to the overarching question in a threat assessment inquiry: ***Does the individual of concern pose a threat of targeted violence toward the school or its staff or students?***

Classifying Threats to Determine Response Strategies

The threat assessment is designed to identify and assess risks in a deliberate and thorough manner. In determining response strategies to mitigate the risk and to provide assistance, as needed, it is helpful to classify threats by level. Based on the information collected, the threat assessment team may classify threats using the following basic criteria:

Threat Levels	Criteria
Low risk threat	individual/situation does not appear to pose a threat of violence or serious harm to self/others, and any exhibited issues/concerns can be resolved easily.
Moderate risk threat	person/situation does not appear to pose a threat of violence, or serious harm to self/others, at this time; but exhibits behaviors that indicate a continuing intent and potential for future violence or serious harm to self/others; and/or exhibits other concerning behavior that requires intervention.
High risk threat	A high risk threat is one in which the person/situation appears to pose a threat of violence, exhibiting behaviors that indicate both a continuing intent to harm and efforts to acquire the capacity to carry out the plan; and may also exhibit other concerning behavior that require intervention.
Imminent threat	person/situation appears to pose a clear and immediate threat of serious violence toward others that requires containment and action to protect identified or identifiable target(s); and may also exhibit other concerning behavior that require intervention.

Documentation

Effective threat assessment and management efforts are accompanied by thorough documentation that demonstrates the team's good faith efforts to identify, investigate, assess, and manage threatening situations. The team can remember this with the acronym **FORT**: Engage in actions and accompanying documentation that demonstrates that the team was:

F: **FAIR** – sought to understand situations and give individuals an opportunity to be heard and understood

O: **OBJECTIVE** – sought information based on facts and observations of the case and not speculation or bias

R: **REASONABLE** – engaged in responses that were effective and proportionate to the situation, and

T: **TIMELY** – quickly and responsively addresses reports of threatening behavior

Source: © G. Deisinger (1996)

RESPONDING TO AND MANAGING THREATENING SITUATIONS

Effective case management integrates interventions, where appropriate and feasible, across the (relevant) domains:

S   De-escalate, contain, or control the **subject** who may take violent action;

T   Decrease vulnerabilities of the **target**;

E   Modify physical and cultural **environment** and systems to discourage escalation; and,

P   Prepare for and mitigate against **precipitating events** that may trigger adverse reactions. If it is determined that the student poses a threat of violence, the threat assessment team shall develop, implement, and monitor an individualized plan to intervene and reduce the threat.

Source: © G. Deisinger & M. Randazzo (2008)

Develop an individualized case management plan based on information gathered through the assessment. The plan must be fact-based and person/situation-specific. Keep in mind that engagement with (i.e., direct communication, empathy, support, and confrontation) can be very helpful with individual of concern from within school communities, even when dealing with someone who is very angry. The more isolated they become the more difficult to assess, intervene with and monitor their response to interventions. Of course, personalities and worldviews matter so sometimes teams have to carefully consider who will be point of contact with the individual of concern, not only in terms of their personality, but also their skills and willingness to support the goals of the threat management process. Generally speaking it is best to use the least intrusive interventions strategies that are likely to be effective with the situation at hand.

Subject-based strategies or interventions

Schools regularly use many of the following examples of interventions or strategies to address inappropriate behavior including, but not limited to, threatening behavior. The focus is on interventions that de-escalate, contain, control, redirect the subject away from plans and preparation for violence; and toward engaging with others, problem solving, adapting, and improving their coping skills and well-being. Examples of subject-based strategies or interventions include (but are not limited to:

- Maintain channel of communication and engagement (with subject) to.

    - Gather information,

    - Build rapport and relationship

    - Decrease isolation

    - De-escalate volatile reactions

    - Provide feedback & mentoring

    - Monitor reactions to grievances, interventions and precipitating events.

- Problem solving about legitimate grievances

- Referral for assistance or support services;

    - Academic assistance or accommodations

    - Social skills training

    - Behavioral contracting

    - Modifications of student classroom assignment or schedule

    - Modification of work schedule or assignments

    - Alternative schooling/home schooling

- – Involvement in extra-curricular activities

- – Performance improvement plans

- – Peer coaching/mentoring

- Counseling/mental health services

- – Check-in/check-out with school counseling staff

- – Outpatient counseling/mental health care.

- – Emergency psychiatric evaluation

- Disciplinary measures

- – Subject confrontation or warning;

- – Administrative orders for no contact of communication

- – Parental involvement

- – In school detention /after-school detention

- – Suspension

- – Termination/expulsion

- – Law enforcement involvement

- – Court issued protective orders

- – Diversion programs

Intervention strategies selected should be the ones with the greatest potential for addressing short-term crises as well as longer-term preventive power. While holding students and staff accountable for their actions, school administrators must be fair and reasonable in disciplinary responses. A broad range of corrective disciplinary actions may be employed including admonition and counseling, behavioral contracts, after-school or in-school detention, and suspension of student privileges for a specified period. These disciplinary responses may be combined with other actions such as parent conferences, modifications of student classroom assignment or schedule, and referrals to in-school and community-based programs such as mediation and community service.

It is important for threat assessment teams to recognize that even fair and reasonable discipline can be perceived as another grievance to which the subject may react. In such cases, the disciplinary response could lead to escalation in threatening behavior. The most punitive responses may or may not prevent acts of violence. Suspension, expulsion or termination *can* create the risk of triggering either an immediate or a delayed violent response unless such actions are coupled with containment and support. A student who is expelled may conclude: "I have lost everything. I have only a short time to act. I will give them what they deserve." In addition, a student who is suspended or expelled is often under less supervision than if he or she were to remain in a school setting.

That is not reason to withhold appropriate and fair consequences for inappropriate behavior, but rather when the situation arises, for threat assessment teams to have considered and planned for those responses. Administrative leave, suspension, expulsion, or termination options that focus solely on accountability and controlling the person do not address the ongoing challenges of:

- Moving person away from thoughts & plans of, and capacity for, violence and/or disruption;

- Connecting person to resources (where needed);

- Mitigating organizational/systemic factors;

- Monitoring person when they are no longer connected to organization.

Use separation strategies with intentionality, awareness of limitations, and anticipation of consequences.

Although detaining a subject may be necessary in a particular situation, without careful attention to the need for confinement, weapons removal, or interpersonal intervention, that action may be insufficient to prevent violence at school or otherwise protect a target. Similarly, referring a subject to the mental health system, without seeing that referral in the context of an overall monitoring/management plan, may not be sufficient to prevent violence. Singular interventions tend to not be sufficient to address complex and on-going situations.

Target-Based Case Management Strategies

In addition to interventions focused on addressing the behavior of the individual(s) of concern, effective threat management teams also attempt to minimize risk and negative impact on identified or identifiable targets and seek to maintain contact (where appropriate) to help monitor the actions and impact of the subject of concern. Examples of target-based case management strategies include (but are not limited to):

- Coaching regarding personal safety approaches in dealing with individual of concern:
    - Clear statements to subject:
        - Relationship/contact is unwanted
        - Stop all contact and/or communication
    - Avoid subsequent contact / response
    - Document all further contacts
    - Do not engage emotionally, monitor "buttons" getting pushed
- Minimize publicly available information
    - Scrub internet information
    - Check privacy settings on social media applications
- Maintain awareness of surroundings
- Vary routine
- Develop contingency plans for escape, shelter, support
- Encourage use of support systems
    - Counseling/mental services
    - Victim assistance programs

Environmental / Systemic Case Management Strategies

In addition to addressing, where necessary interventions with the subject of concern and target, effective teams also take a holistic view of the situation, monitoring for underlying systemic causes that may be contributing not just to a given case, but perhaps to a range of cases over time. This level of intervention is about group and sub-group behavior, not just that of the subject of concern or target. Strategies may include:

- Address systemic, policy or procedural problems that may serve as precipitating events across cases
- Bullying prevention / intervention programs
- Enhance school/workplace climate – build and support a caring community

- Intervene with associates that support or encourage violent behavior

- Enhance conflict management skills of sub-groups

- Identify and address gaps in awareness of reporting and intervention options

- Identify and address gaps in threat assessment & management process

Monitoring for the Impact of Precipitating Events on Case Management

The threat assessment team members recognize that cases do not occur in a vacuum and that life continues while they are assessing and intervening with a given case. The team maintains an ongoing, longitudinal approach to anticipating, monitoring for, and (to the extent possible) manage the impact of potential precipitating events such as:

- Loss impacting the subject

    - Job or income;

    - Status;

    - Significant other/relationship;

    - Health;

    - Rejection / Ostracization;

- Injustice;

- Implementation of administrative notices / court orders;

- Violation of administrative notices / court order

- Anniversary events, e.g.:

    - Date of beginning of relationship

    - Date of end of relationship

    - Date served with court orders/separation documents

    - Birthdays

    - Holidays

- Contagion effect of other high profile or locally significant acts of violence

BUILDING CONSISTENCY BETWEEN THREAT ASSESSMENT AND MANAGEMENT

Based on an individualized assessment of the risk or priority of the case, teams will engage case management strategies that are sufficient, fair and reasonable to address the concerns identified. For each general threat level there is a minimal level of response or case management that is appropriate. Keep in mind that these are general guidelines to prompt consideration of a starting point in developing a case management strategy. A given case may have a fact pattern that necessitates deviation from the general guidelines. Where that is the case, teams should deliberate, reach consensus upon action steps, and document the facts or circumstances that factored into their case management planning. Following are examples of options and considerations for case management for the various levels of threat.

Examples of Low Risk Threat Responses

A low risk threat is one in which the person/situation does not appear to pose a threat of violence and any underlying issues can be resolved easily. The response to such a threat depends on the context of the threat, whether the threat requires some form of

disciplinary action, and what is necessary to resolve the situation. Some low threat cases are generated from a misunderstanding of what was communicated, something taken out of context, or a statement made in the heat of the moment but with not actions to indicate intent to cause harm. Many low risk threats are resolved with a clarification, explanation, retraction and or an apology – all of which (in conjunction with the absence of any other behaviors of concern) indicates that the threat is non-existent or minimal, and is over. School administrators should generally consider the following:

- Since low risk threats by definition do not appear to pose a threat and can be easily resolved, action to protect the person(s) to whom the threat was directed should not be necessary. When the person to whom the threat was directed is a student, his/her parents or guardian may be notified, at the discretion of the threat assessment team or school administration. If parents of a threatened student are notified, they should be contacted promptly and reassured that the threat has been resolved. Parents of the student engaging in the low risk threatening behavior may also be notified so they are aware of the situation and that it has been resolved.

- Some low risk threats may be subject to disciplinary action based on school board policy. The parent or guardian of the subject student is to be notified of the incident and of the disciplinary action taken. All relevant disciplinary due processes should be followed.

- When the threat assessment team determines a threat to be low risk, the case may be resolved entirely with no further action or resolved with referral to appropriate school or community-based resources. When subjects are referred for resources or services, a member of the threat assessment team may be designated to monitor the subject's reactions for a short period of time, and that the referral was made effectively.

- If new information comes to the attention of the team, re-assess and update the case management plan.

Examples of Moderate Risk Threat Responses

A moderate risk threat will typically result in notifying the intended target(s) of the threat and taking precautions to protect them, taking steps to monitor and supervise the subject, and taking disciplinary action in accordance with existing discipline policy. The threat assessment team will also work to address the conflict or problem that led to the threat. Examples of strategies that may be employed include but are not limited to:

- Take precautions to protect potential victims. Precautions typically include:
  - Provide direct supervision so the subject cannot carry out the threat while at school, at school functions, or on the bus.
  - Caution the subject who made the threat about the consequences of carrying out the threat.
  - Where the subject is a student, contact the student subject's parents to assume responsibility for supervision of the student and to enlist their support in preventing the student from carrying out the threat.
  - Notify the intended target(s) and (if they are students) their parents. The intended target(s) (and, where appropriate) their parents, must be notified of the seriousness of the threat, the identity of the subject who made the threat, and what actions are being taken to support the safety of the target and the school as a whole.

- Consult with the school resource officer to assist in monitoring and supervising the subject as well as determining the need, if any, for law enforcement action.

- Follow applicable disciplinary procedure in accordance with conduct policy.

- Where appropriate, refer the subject for counseling, conflict mediation, or other interventions to reduce the threat of violence and to address the underlying conflict or issues that led to the threat. The school administrator should involve school-based professionals (such as the school psychologist, counselor, or social worker) or community based professionals (e.g., Employee Assistance Program, community mental health services, etc.) who can provide assistance and appropriate intervention.

- Where mental health or disability issues are reasonably believed to be causing or contributing to violence risk, a mental health risk assessment *may* be conducted, following parameters for the mental health risk assessment as outlined in the section below regarding high risk threats.

Examples of High Risk Threat Responses

Threatening behaviors indicating the intent, planning, or preparation to cause serious bodily injury or death (e.g., to rape, physically assault and inflict serious injury, kill, or use weapons against others requires the immediate involvement of the threat assessment team. When the threat is determined to be high risk, the threat assessment team must:

- Notify law enforcement per regulation to contain the threat and consult with School Safety and Security.

- Take immediate precautions to protect potential victims:

    – Provide direct supervision so the subject cannot carry out the threat while at school, at school programs, or on the bus.

    – Caution the subject who made the threat about the consequences of carrying out the threat.

    – Where the subject is a student, contact the subject student's parents and enlist their support in preventing the student from carrying out the threat; either law enforcement or the student's parents should assume responsibility for supervising the student.

    – Notify the intended target(s) and (if they are students) their parents. The intended target(s) (and, where appropriate) their parents, must be notified of the seriousness of the threat, the identity of the subject who made the threat, and what actions are being taken to support the safety of the target and the school as a whole.

- Follow applicable disciplinary procedure in accordance with conduct policy.

- Where mental health or disability issues are reasonably believed to be causing or contributing to violence risk, a mental health risk assessment should be conducted by a qualified independent medical/psychological professional. The professional conducting the evaluation should not have a treatment relationship with the subject. The assessment should be based on a review of all available information including but not limited to interview of the subject by the professional. The written report must identify the problem or conflict that prompted the threat and recommend strategies to address the problem and to reduce the risk of violence.

    – The school administrator or disciplinary hearing officer will determine the conditions of readmission to school that may include the requirement to cooperate in a mental health evaluation. If the subject is a student, the parents are to be notified of all requirements and any failure to comply. A re-admission meeting must be held prior to the subjects return to school/work.

    – Every effort will be made by threat assessment team members to obtain any required signed permission for release and exchange of information with mental health provider(s), if any, and where appropriate, local law enforcement agencies.

    – After receiving the mental health evaluation report, the threat assessment team shall convene to complete and implement a written safety plan to address the immediate steps taken to prevent the threat from being carried out and a plan for further action before the subject is permitted to return to school or an alternative educational environment. The safety plan should include:

        ▪ conditions under which the subject may return to school/work;

        ▪ interventions, such as counseling or medication, that are needed to reduce risk;

        ▪ scheduled follow-up contact with the subject (and parent if subject is a student) to assess changes in risk and update the safety plan over time, until the perceived threat is resolved; and

        ▪ person(s) who are responsible for monitoring and verifying that the safety plan recommendations are being followed.

- A student/employee should only be removed if the threatening behaviors engaged in by the subject are a violation of the relevant Code of Conduct /school board policy, and when all applicable disciplinary procedures are followed. However, in the event that the applicable disciplinary procedures are not available to school-based staff and the school administration or threat assessment team believes that the subject poses a significant risk to the health or safety of others that cannot be eliminated by a modification of policies, practices, or procedures, or by the provision of auxiliary aids or services as provided in 28 C.F.R. § 35.129, the direct threat standard may be utilized. Before applying the direct threat standard, the school administrator should contact the school division's Director of Special Education, and, where available, legal counsel.

- In utilizing the direct threat standard where a subject has a disability, it is important to note that a determination that a person with a disability poses a direct threat may not be based on generalizations or stereotypes about the effects of a particular disability and must be based on an individualized assessment, based on reasonable judgment relying on current medical evidence or on the best available objective evidence, to determine: the nature, duration, and severity of the risk; the probability that the potential injury will actually occur; and whether reasonable modifications of policies, practices, or procedures will mitigate the risk.

Imminent Threat Responses

An imminent threat exists when the person/situation appears to pose a clear and immediate threat of serious violence toward others. Such threats require immediate containment and action to protect identified target(s) and referral to law enforcement and consultation with school security. Following immediate containment and action to protect identified target(s), these threats require the involvement of the threat assessment team for the purpose of conducting/coordinating appropriate mental health assessment and developing a safety plan.

Procedures for notification of the superintendent or designee, senior division administrator, and parents of a student subject and/or intended target student(s) that are set forth for high risk threats are to be followed.

- Where mental health or disability issues are reasonably believed to be causing or contributing to violence risk, a mental health risk assessment should be conducted by a qualified independent medical/psychological professional. The professional conducting the evaluation should not have a treatment relationship with the subject. The assessment should be based on a review of all available information including but not limited to interview of the subject by the professional. The written report must identify the problem or conflict that prompted the threat and recommend strategies to address the problem and to reduce the risk of violence.

  - The school administrator or disciplinary hearing officer will determine the conditions of readmission to school/work that may include the requirement to cooperate in a mental health evaluation. If the subject is a student, the parents are to be notified of all requirements and any failure to comply. A re-admission meeting must be held prior to the subject's return to school/work.

  - Threat assessment team members will obtain any required signed permission for release and exchange of information with mental health provider(s), if any, and where appropriate, local law enforcement agencies.

  - After receiving the mental health evaluation report, the threat assessment team shall convene to complete and implement a written safety plan to address the immediate steps taken to prevent the threat from being carried out and a plan for further action before the subject is permitted to return to school or an alternative educational environment. The safety plan should include:

    - conditions under which the subject may return to school/work;
    - interventions, such as counseling or medication, that are needed to reduce risk;
    - scheduled follow-up contact with the subject (and parent if subject is a student) to assess changes in risk and update the safety plan over time, until the perceived threat is resolved; and
    - person(s) who are responsible for monitoring and verifying that the safety plan recommendations are being followed.

- A student/employee should only be removed if the threatening behaviors engaged in by the subject are a violation of the relevant Code of Conduct /school board policy, and when all applicable disciplinary procedures are followed. However, in the event that the applicable disciplinary procedures are not available to school-based staff and the school administration or threat assessment team believes that the subject poses a significant risk to the health or safety of others that cannot be eliminated by a modification of policies, practices, or procedures, or by the provision of auxiliary aids or services as provided in 28 C.F.R. § 35.129, the direct threat standard may be utilized. Before applying the direct threat standard, the school administrator should contact the school division's Director of Special Education, and, where available, legal counsel.

- In utilizing the direct threat standard where a subject has a disability, it is important to note that a determination that a person with a disability poses a direct threat may not be based on generalizations or stereotypes about the effects of a particular disability and must be based on an individualized assessment, based on reasonable judgment relying on current medical evidence or on the best available objective evidence, to determine: the nature, duration, and severity of the risk; the probability that the potential injury will actually occur; and whether reasonable modifications of policies, practices, or procedures will mitigate the risk.

THREAT ASSESSMENT TRIAGE AND ASSESSMENT FORM

PART I. THREAT REPORTED

Date Reported:		Day of Week:	❑Monday ❑Tuesday ❑Wednesday ❑Thursday ❑Friday ❑Saturday ❑Sunday	Time: _____	❑ AM ❑ PM
Taken by:		**School:**		**Position:**	

REPORTING PARTY:

Name:		❑Unknown	ID #:	
Affiliation:	❑Administrator ❑Teacher ❑Staff ❑Student ❑Parent/Guardian ❑Contractor ❑Other:_____ ❑ None/Unknown		**Status:**	❑Current ❑Former ❑Prospective Grade:_____(if student)
School:			**Building/Program:**	
Home Address:			**Phone:**	

INCIDENT:

Date Occurred:		Day of Week:	❑Monday ❑Tuesday ❑Wednesday ❑Thursday ❑Friday ❑Saturday ❑Sunday	Time: _____	❑ AM ❑ PM
Location:	❑School Property [◯In School Building ◯ School Grounds] ❑School Bus ❑School Sponsored Activity ❑Other:				
Address:		**City:**		**State:**	
Threat Type:	❑Assault [◯Physical ◯Sexual) ❑Threat ❑Suspicious ❑Stalking ❑Suicidal/Self-Harm ❑Bomb threat ❑Unusual Communication ❑Vandalism ❑Disruptive ❑Harassment ❑Involuntary MH hold ❑Other:				
Mode:	❑In Person ❑Phone ❑Text ❑Email ❑Letter ❑Social Media ❑Internet ❑Other :			**❑ Multiple Modes**	
Target(s) injured: ❑Yes ❑No ❑Unknown		**Target(s) require medical attention?** ❑Yes ❑No ❑Unknown			
Weapon involved: ❑Yes ❑No ❑Unknown		**Type of Weapon:** ❑Firearm[◯Rifle/Shotgun ◯Pistol] ❑Edged ❑Bomb ❑Other:			

Details of the incident or threat. Where threats were communicated, quote where possible, use quotation marks to indicated direct quotes. Attach original communications if available.

PART II. PERSONS INVOLVED

SUBJECT (1) Engaging in threatening, aberrant or concerning behavior:

Name:	❏Unknown	ID #:	
Affiliation:	❏Administrator ❏Teacher ❏Staff ❏Student ❏Parent/Guardian ❏Contractor ❏Other:_____ ❏ None/Unknown	**Status:**	❏Current ❏Former ❏Prospective Grade:_____(if student)
School:		**Building/Program:**	
Emergency Contact		**Relationship:**	
Home Address:		**Phone:**	

SUBJECT (2) Engaging in threatening, aberrant or concerning behavior:

Name:	❏Unknown	ID #:	
Affiliation:	❏Administrator ❏Teacher ❏Staff ❏Student ❏Parent/Guardian ❏Contractor ❏Other:_____ ❏ None/Unknown	**Status:**	❏Current ❏Former ❏Prospective Grade:_____(if student)
School:		**Building/Program:**	
Emergency Contact		**Relationship:**	
Home Address:		**Phone:**	

Note: If more than two subjects of concern in this incident, attach additional copies of this page with subject's information.

TARGET (1):

Name:	❏Unknown	ID #:	
Affiliation:	❏Administrator ❏Teacher ❏Staff ❏Student ❏Parent/Guardian ❏Contractor ❏Other:_____ ❏ None/Unknown	**Status:**	❏Current ❏Former ❏Prospective Grade:_____(if student)
School:		**Building/Program:**	
Emergency Contact		**Relationship:**	
Home Address:		**Phone:**	

TARGET (2):

Name:	❏Unknown	ID #:	
Affiliation:	❏Administrator ❏Teacher ❏Staff ❏Student ❏Parent/Guardian ❏Contractor ❏Other:_____ ❏ None/Unknown	**Status:**	❏Current ❏Former ❏Prospective Grade:_____(if student)
School:		**Building/Program:**	
Emergency Contact		**Relationship:**	
Home Address:		**Phone:**	

WITNESS (1)

Name:		❑Unknown	**ID #:**	
Affiliation:	❑Administrator ❑Teacher ❑Staff ❑Student ❑Parent/Guardian ❑Contractor ❑Other:_____ ❑ None/Unknown		**Status:**	❑Current ❑Former ❑Prospective Grade:_____(if student)
School:			**Building/Program:**	
Emergency Contact			**Relationship:**	
Home Address:			**Phone:**	

Witness Interview

WITNESS (2)

Name:		❑Unknown	**ID #:**	
Affiliation:	❑Administrator ❑Teacher ❑Staff ❑Student ❑Parent/Guardian ❑Contractor ❑Other:_____ ❑ None/Unknown		**Status:**	❑Current ❑Former ❑Prospective Grade:_____(if student)
School:			**Building/Program:**	
Emergency Contact			**Relationship:**	
Home Address:			**Phone:**	

Witness Interview

PART III. RECORDS CHECKS (NS=Not Significant; NA=Not Applicable)

RECORDS CHECKS (ALL):	Subject	Target	Notes about Significant findings:
Affiliation	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Photo	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Threat Assessment Team history	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Criminal history (VA)	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Driver license information	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Driver transcript / violations	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Vehicle / Parking information	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
SRO/SSO contacts	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Local Law Enforcement contacts	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Other Law Enforcement contacts	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Protective / No Contact Orders	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Concealed weapons permit	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Weapons purchase permit	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Social media	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Online Search	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Other:	❏Checked ❏NS/NA	❏Checked ❏NS/NA	

RECORDS CHECKs: School Staff

	Subject	Target	
Disciplinary actions	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Grievances filed	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Title IX actions	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Application	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Other:	❏Checked ❏NS/NA	❏Checked ❏NS/NA	

RECORDS CHECKS: Students

	Subject	Target	
Class schedule	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Academic standing / progress	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Transfer records	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Conduct / Disciplinary actions	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Title IX actions	❏Checked ❏NS/NA	❏Checked ❏NS/NA	
Other:	❏Checked ❏NS/NA	❏Checked ❏NS/NA	

Other Sources/Checks/Comments:

PART IV. KEY TRIAGE QUESTIONS SUMMARY SHEET

SUBJECT		Notes:
Identified grievances / motives for violence	❑Yes ❑No ❑Unknown	
Identification with other perpetrators, grievances, or violent acts	❑Yes ❑No ❑Unknown	
Communicated violent ideation or intent	❑Yes ❑No ❑Unknown	
Planning taken to support violence intent	❑Yes ❑No ❑Unknown	
Acquiring means, methods, opportunity or proximity toward violence	❑Yes ❑No ❑Unknown	
Prior violence / disruptive behaviors	❑Yes ❑No ❑Unknown	
Significant behavioral changes: e.g., paranoia, substance abuse, isolation	❑Yes ❑No ❑Unknown	
Despondency and/or suicidality	❑Yes ❑No ❑Unknown	
Diminished alternatives or ability to manage stressors	❑Yes ❑No ❑Unknown	
Recurrent pattern(s) of disruptive/concerning behavior(s)	❑Yes ❑No ❑Unknown	
Stalking / unwanted contact, communication or pursuit	❑Yes ❑No ❑Unknown	
Lack of inhibitors / stabilizers to prevent violence	❑Yes ❑No ❑Unknown	
Other:	❑Yes ❑No ❑Unknown	
TARGET / OTHERS		Notes
Identified targets (person/proxy, place, program, process, philosophy)	❑Yes ❑No ❑Unknown	
Fearful of harm	❑Yes ❑No ❑Unknown	
Responding as if subject poses a safety concern	❑Yes ❑No ❑Unknown	
Engaging in protective actions	❑Yes ❑No ❑Unknown	
Responding in a provocational or defensive manner	❑Yes ❑No ❑Unknown	
Low / inconsistent situational awareness	❑Yes ❑No ❑Unknown	
Other:	❑Yes ❑No ❑Unknown	
ENVIRONMENT		Notes
Organizational climate concerns: e.g., bullying, bias, poor conflict mgmt..	❑Yes ❑No ❑Unknown	
Chaotic or inconsistent structure	❑Yes ❑No ❑Unknown	
Lack of support, guidance or resources	❑Yes ❑No ❑Unknown	
High rates of violence, harassment, disruption, injury or harm	❑Yes ❑No ❑Unknown	
High perceived stress	❑Yes ❑No ❑Unknown	
Disproportionate rate/severity of concerns	❑Yes ❑No ❑Unknown	
Other:	❑Yes ❑No ❑Unknown	
PRECIPITATING EVENTS		Notes
Have occurred	❑Yes ❑No ❑Unknown	
Impending	❑Yes ❑No ❑Unknown	

TRIAGE RECOMMENDATION:

TAT TRIAGE/CASE ID:

❑No identified threat: **Close case**	❑Non-Threat Concerns: **Referral(s)**	❑Unknown/Potential/On-going Threat: **Initiate TAT Case**

THREAT/PRIORITY LEVEL:

❑1: Imminent/Critical	❑2: High	❑3: Moderate	❑4: Low	❑5: Routine / None:

TRIAGE COMPLETED BY:

Name	Position	Signature	Date

Name	Position	Signature	Date

PART V. KEY QUESTIONS FOR THREAT ASSESSMENT INQUIRY

1. **What are the subject's motives, grievances, goals and intent in their behavior?**

2. **Have there been any communications suggesting ideas, intent, planning or preparation for violence?**

3. Has the subject shown inappropriate interest in/identification with:	If yes, describe:
☐ Incidents or perpetrators of targeted/mass violence	
☐ Grievances of perpetrators	
☐ Weapons/tactics of perpetrators	
☐ Notoriety or fame of perpetrators	

4. Does the subject have (or are they developing) the capacity and will to carry out an act of targeted violence?	If yes, describe:
☐ Expressed ideas to engage in violence	
☐ Made plans for violence	
☐ Preparing for violence (means, method, opportunity, access)	
☐ Surveillance, stalking or rehearsal	

5. **Is the subject experiencing or expressing hopelessness, desperation, and/or despair?**

6. **Does the subject have a positive, trusting, sustained relationship with at least one responsible person?**

7. **Does the subject see violence as an acceptable, desirable – or the only – way to solve a problem?**

8. Are the subject's conversation and "story" consistent with his or her actions?

9. Are other people concerned about the subject's potential for violence?

10. What circumstances might affect the likelihood of escalation to violence?

Other Relevant Information:

PART VI. PRELIMINARY DETERMINATION OF THREAT LEVEL

Check one:

☐ Imminent threat ☐ High risk threat ☐ Moderate risk threat ☐ Low risk threat

PART VII. CASE MANAGEMENT INTERVENTIONS & RESPONSE

INTERVENTION/TASK	RESPONSIBLE PERSON	DATE DUE
Subject Interventions		
Target Interventions		
Environment Interventions		
Precipitating Events (Monitoring/Interventions)		

Print name of Team Leader: _____Date: _____

Signature of Team Leader: _____

PART VI. PRELIMINARY DETERMINATION OF THREAT LEVEL (Alternative Form)

☐ Imminent threat ☐ High risk threat ☐ Moderate risk threat ☐ Low risk threat

PART VII. CASE MANAGEMENT INTERVENTIONS & RESPONSE (Alternative Form)

Imminent Risk Threat

☐ Notify law enforcement per regulation to contain threat; and consult with Safety and Security	☐ Protect and notify intended victim(s) and parents and/or guardians of victim(s)	☐ Refer subject for mental health assessment,
☐ Mobilize threat assessment team	☐ Notify subject student's parents and/or guardians	☐ Notify subject/parents of requirements for re-admission to school
☐ Provide direct supervision of subject until removed from campus by law enforcement or parent/guardian.	☐ Notify superintendent or designee	☐ Develop/monitor safety plan
☐ Caution the subject about the consequences of carrying out the threat	☐ Follow discipline procedures as per conduct policy	☐ Assign team member to monitor subject and intervention/safety plan.

High Risk Threat

☐ Notify law enforcement per regulation to contain threat; and consult with Safety and Security	☐ Protect and notify intended victim(s) and parents / guardians of victim(s)	☐ Refer subject for mental health assessment,
☐ Mobilize threat assessment team	☐ Notify subject student's parents and/or guardians	☐ Notify subject & parents of requirements for re-admission to school
☐ Provide direct supervision of subject until removed from campus by law enforcement or parent/guardian.	☐ Notify superintendent or designee	☐ Develop/monitor safety plan
☐ Caution the subject about the consequences of carrying out the threat	☐ Follow discipline procedures as per conduct policy	☐ Assign team member to monitor subject and intervention/safety plan.

Moderate Risk Threat

☐ Mobilize threat assessment team	☐ Protect and notify intended victim(s) & parents / guardians of victim(s)	☐ If needed, refer subject for mental health assessment
☐ Notify subject & parents and/or guardians	☐ Consult with SRO to assist in monitoring/ supervising subject and determining need for law enforcement action.	☐ Assign a team member to monitor subject and status of intervention, as appropriate
☐ Provide direct supervision of subject until parents and/or guardians assume control	☐ Notify superintendent or designee	☐ If warranted by findings of mental health assessment, develop/monitor safety plan
☐ Caution the subject about the consequences of carrying out the threat	☐ Follow discipline procedures	

Low Risk Moderate Risk High Risk/Imminent

☐ Advised RP / Target to consult with threat assessment team, as needed	☐ Consult with Safety and Security specialist and/or SRO, if necessary	☐ Refer for school- or community-based services, as appropriate
☐ Contact subject's parents and/or guardians, if necessary	☐ Refer subject for services to resolve problem, if appropriate	☐ Assign a case manager to monitor subject and status of intervention, as appropriate
☐ Notify intended victim(s) & parents/ guardians, if necessary	☐ Follow discipline procedures	
☐ See that perceived threat is resolved through explanation, apology, or making amends	☐ Develop behavior intervention plan and/or contract, as appropriate	

Print name of Team Leader: _____ Date: _____

Signature of Team Leader: _____

PART VIII. THREAT ASSESSMENT UPDATE (to be updated regularly while case is active)

Instructions:

This section should be completed by the Team Leader, or others, as appropriate.

Date of Update

Disciplinary action(s) taken:

Subject suspended? ☐ Yes ☐ No

Subject recommended for expulsion/Termination? ☐ Yes ☐ No

Subject recommended for further disciplinary action and/or consideration? ☐ Yes ☐ No

Comment:

Special Education? If yes:

Recommendation to reconvene IEP team? ☐ Yes ☐ No

Develop Functional Behavioral Assessment and/or Behavior Intervention Plan for IEP? ☐ Yes ☐ No

If no, should the student be referred to Child Study or Local Screening? ☐ Yes ☐ No

Comment:

Actions with potential target(s) of the threat or students impacted by the threat:

Designated Case Manager / Point of Contact:

Offered supportive counseling? ☐ Yes ☐ No Provided brief supportive counseling? ☐ Provided ☐ Declined

Communicated with targets(s) and parent(s) / guardian(s)? ☐ Yes ☐ No

Altered schedule to minimize contact with subject who made the threat? ☐ Yes ☐ No

Advised targets(s) and/or parent(s) or guardian(s) of their right to contact police? ☐ Yes ☐ No

Name of staff member who provided this information:

Student services/Human Resources staff to monitor target at regular intervals? ☐ Yes ☐ No

Name of staff member who will monitor target:

Informed target(s) and parent(s) or guardian(s) of re-entry date and plan
for re-entry of subject who made the threat, if applicable? ☐ Yes ☐ No

Additional Comments:

Actions with Subject making the threat:
Case Manager / Point of Contact Name:
Alter schedule to minimize contact with threatened target? ☐ Yes ☐ No
Student Services / Human Resources staff to monitor? ☐ Yes ☐ No
Name of staff member who will monitor subject:
School-based/ EAP supportive counseling offered? ☐ Yes ☐ No
Name/position of staff member who will provide counseling to student:
Referral for private or community-based mental health services? ☐ Yes ☐ No
Consult with any other agency? ☐ Yes ☐ No
Agency & Name of Contact:
Other actions planned:
Print name of Team Leader: _____Date:_____
Signature of Team Leader: _____   *(Signature indicates agreement with identified level of threat and the above actions have been taken.)*
This case has been resolved and necessary actions have been taken to provide support or assistance to the subject who made the threat and to any impacted persons.
Signature of case manager (if appropriate): _____ Date: _____
Signature of administrator: _____ Date: _____

RELATED READING ON SCHOOL / CAMPUS THREAT ASSESSMENT

Albrecht, S. (February 2010). Threat assessment teams: Workplace and school violence prevention. FBI Law Enforcement Bulletin. Washington, DC: Federal Bureau of Investigation. Available online at www.fbi.gov/stats-services/publications/law-enforcement-bulletin/february-2010/threat-assessment-teams

Brunner, J. & Lewis, D. (2012, February). Strategic safety: Little things are the big things. *Principal Leadership, 12*(6). Available online at www.nassp.org/Content.aspx?topic=Strategic_Safety_0212

Colorado School Safety Resource Center (November 2011). Essentials of school threat assessment: Preventing targeted school violence. Available online at www.colorado.gov/cs/Satellite/CDPS-SafeSchools/CBON/1251622848436

Cornell, D. & Sheras, P. (2006). Guidelines for responding to student threats of violence. Longmont, CO: Sopris West.

Deisinger, G., Randazzo, M., O'Neill, D. & Savage, J. (2008). The handbook for campus threat assessment and management teams. Boston, MA: Applied Risk Management.

Drysdale, D.A., Modzeleski, W., & Simons, A.B. (April 2010). Campus attacks: Targeted violence affecting institutions of higher education. Washington, DC: United States Secret Service, United States Department of Education, and Federal Bureau of Investigation. Available online at www2.ed.gov/admins/lead/safety/campus-attacks.pdf

Vossekuil, B., Fein, R.A., Reddy, M., Borum, R., & Modzeleski, W. (2002) The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States.. Washington, DC: U.S. Secret Service and U.S. Department of Education. Available online at www.secretservice.gov/ntac/ssi_guide.pdf

Fein, R.A., Vossekuil, B., Pollack, W.S., Borum, R., Modzeleski, W. & Reddy, M. (2004) Threat assessment in schools: A guide to managing threatening situations and to creating safe school climates. Washington, DC: U.S. Secret Service and U.S. Department of Education. Available online at www.secretservice.gov/ntac/ssi_guide.pdf

Mohandie, K. (2000) School violence threat management. San Diego, CA: Specialized Training Services.

National Association of School Psychologists (n.d.). Threat assessment: Predicting and preventing school violence. Available online at www.nasponline.org/resources/factsheets/threatassess_fs.aspx

Nolan, J.J., Randazzo, M.R., & Deisinger, G. (2011). Campus threat assessment and management teams: What risk managers need to know now. University Risk Management and Insurance Association (URIMA) Journal Reprint.

O'Toole, M. E. (2000). The school shooter: A threat assessment perspective. Quantico, VA: National Center for the Analysis of Violent Crime, Federal Bureau of Investigation.

Pollack, W. S., Modzeleski, W., & Rooney, G. (2008). *Prior knowledge of potential school-based violence: Information students learn may prevent a targeted attack.* Washington, DC: United States Secret Service and United States Department of Education. Available online at www.secretservice.gov/ntac/bystander_study.pdf

Reddy, M., Borum, R., Berglund, J. Vossekuil, B., Fein, R., & Modzeleski, W. (2001). Evaluating risk for targeted violence in schools: Comparing risk assessment, threat assessment, and other approaches. Psychology in the Schools, 38(2), 157-172. Available online at www.secretservice.gov/ntac/ntac_threat_postpress.pdf

U.S. Department of Education (2007). Practical information on crisis planning: A guide for schools and communities. Available online at www2.ed.gov/admins/lead/safety/emergencyplan/crisisplanning.pdf

U.S. Department of Education (2013). Guide for developing high quality school emergency operations plans. Available online at www2.ed.gov/about/offices/list/oese/oshs/rems-k-12-guide.pdf

Van Dreal, J. (2011). Assessing Student Threats. New York: Rowman & Littlefield.

Virginia Department of Education (2007). Crisis management and emergency response in Virginia schools. Richmond, VA: Author. Available online at www.doe.virginia.gov/support/safety_crisis_management/emergency_crisis_management/crisis_mgmt_emer-response_guide.pdf

RELATED RESOURCES

Virginia Department of Criminal Justice Services (DCJS)
Virginia Center for School and Campus Safety (VCSCS)

www.dcjs.virginia.gov/virginia-center-school-and-campus-safety/k-12

The DCJS Virginia Center for School and Campus Safety is dedicated to supporting constituents in the K-12 environment through training, with resources and technical assistance, and by guiding best practices. One of the many important components for K-12 schools is Safety and Security – on this portion of the website visitors will find information on School Security Officers, the annual School Safety Audit, and other school safety topics.

A variety of resources (including this guidance document) may also be obtained through the DCJS/VCSCS site, under the K-12 resources located at www.dcjs.virginia.gov/virginia-center-school-and-campus-safety/k-12/resources

National Center on Safe Supportive Learning Environments (NCSSLE)

http://safesupportiveschools.ed.gov/index.php?id=01

The Center is funded by the U.S. Department of Education's Office of Safe and Healthy Students and the U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration (SAMHSA) to:

- provide training and support to state administrators, including 11 grantees funded under the Safe and Supportive Schools grant program; school and district administrators; institutions of higher education; teachers; support staff at schools; communities and families; and students and

- seek to improve schools' conditions for learning through measurement and program implementation, so that all students have the opportunity to realize academic success in safe and supportive environments.

The Center's website includes information about the Center's training and technical assistance, products and tools, and latest research findings.

Youth Violence Project of the Curry School of Education, University of Virginia

http://curry.virginia.edu/research/labs/youth-violence-project

The Youth Violence Project conducts research on effective methods and policies for youth violence prevention and school safety. The project's website contains extensive information about the Virginia model of threat assessment, an approach to violence prevention that emphasizes early attention to problems such as bullying, teasing, and other forms of student conflict before they escalate into violent behavior. School staff members are encouraged to adopt a flexible, problem-solving approach, as distinguished from a more punitive, zero tolerance approach to student misbehavior.

WORKPLACE THREAT ASSESSMENT

Workplace violence is a complex and widespread issue that in recent years has received increased attention from law enforcement, mental health, and human resources professionals. Reports of disgruntled employees or former employees returning to their places of employment with a gun and killing co-workers is one form of workplace violence. Another type, representing approximately 24 percent of workplace violence, is related to personal relationships where an individual gains access to a workplace and commits a crime targeting an employee who is a current or former intimate partner.

The National Institute for Occupational Safety and Health defines workplace violence as violent acts, including physical assaults and threats of assaults, directed toward persons at work or on duty (NIOSH, 2001). Workplace violence ranges from offensive or threatening language to homicide. It may include domestic violence, sexual violence, including sexual harassment or sexual assault, dating violence, and stalking.

Workplace violence often results in serious injuries that may result in disabilities requiring ongoing care. Workplace violence may also result in life threatening injuries and even death.

The Centers for Disease Control, Occupational Safety and Health Administration and the National Institute for Occupational Safety and Health categorize workplace violence into four types based on the relationship among victims, perpetrators, and work settings.

- Type I incidents involve offenders who have no relationship with either the victims or the workplaces.

- Type II incidents involve offenders who receive services from the school.

- Type III incidents involve current or former employees acting out toward their present or past places of employment.

- Type IV incidents involve domestic disputes between an employee and a perpetrator that spill over into the workplace.

Type I incidents are largely addressed in current school board policies and procedures that limit access to schools and prescribe responses to intruders and other criminal acts by non-students and non-employees. All school divisions address Type II acts in student codes of conduct.

Types III and IV are least frequently addressed in school board policies. When compared with models for student threat assessment, non-student threat assessment policy models and protocols for identification and intervention in schools are far less well developed. Virginia has been a leader in implementing broad based threat assessment and management to address all threats in public schools and campuses.

The following page provides a sample policy and procedure specifically regarding domestic violence occurring in (or impacting on) the school or workplace. School Divisions are not required to implement these particular policies or procedures. They are provided as a resource for consideration, and to draw attention to concerns about domestic violence impacting workplace safety.

SAMPLE POLICY FOR ASSESSING WORKPLACE-RELATED THREATS OF DOMESTIC VIOLENCE

Assessment of Workplace-related Threats of Domestic Violence

- A formal process for assessing workplace-related threats of domestic violence shall be established and implemented by the *[school division]* Department of Human Resources in collaboration with the Office of School Safety and Security.

- A Threat Assessment and Management Team shall be established and include *[school division]* human resources, security, and employee assistance, and, as appropriate, mental health and law enforcement representatives. The school board attorney is to serve as an advisor to the Threat Assessment and Management Team.

- The *[school division]* Department of Human Resources, in collaboration with the Office of School Safety and Security, shall implement activities to ensure that all employees are aware of policies requiring the reporting of all workplace-related threats of domestic violence, understand the problem-solving purposes of threat assessment, and know how to report threats. Methods of reporting shall include at least one method for anonymous reporting.

- The Threat Assessment and Management Team is responsible for assessing all workplace-related threats of domestic violence and determining what steps are necessary to prevent violent acts from being carried out. This team will coordinate resources both within and outside of the school division, as appropriate.

- Employees who have secured any protective or restraining order that lists the workplace as a protected area are required to inform the Office of School Safety promptly of such orders. Employees who have not secured such orders but have safety concerns with regard to intimate partner violence are strongly encouraged to report their concerns to the Office of School Safety so that appropriate safety measures can be put in place. Employees can be assured that *[school division]* will not retaliate against employees making such reports and will support victims of intimate partner violence by making workplace safety plans, providing referrals to Employee Assistance and other appropriate community resources, and permitting time off for addressing the threats of violence. No employee shall be subject to retaliation or retribution of any kind for reporting a suspected incident of workplace violence.

- *[School division]* recognizes and respects an employee's right to privacy and need for confidentiality. Therefore, *[school division]* shall maintain the confidentiality of an employee's disclosure to the extent permitted by law. When information must be disclosed to protect the safety of individuals in the workplace, the breadth and content of the information disclosed will be limited to that reasonably necessary to protect the employees and others. The *[school division]* shall make every effort to provide advance notice to the employee of any disclosure required by law or to protect persons in the workplace.

- The Threat Assessment and Management Team shall document the nature of threats known and safety measures taken and assistance provided to employee victims.

SAMPLE PROCEDURES FOR ASSESSING AND RESPONDING TO WORKPLACE-RELATED THREATS OF DOMESTIC VIOLENCE

PURPOSE

To establish procedures for assessing and responding to workplace-related threats of domestic violence in order to maintain a safe environment for victims of violence, fellow employees, and students.

DEFINITIONS

- **Domestic violence** is a pattern of coercive behavior, including acts or threatened acts, that is used by the perpetrator to gain power and control over a current or former spouse, family member, intimate partner, or person with whom the perpetrator shares a child in common. Domestic violence includes, but is not limited to, physical or sexual violence, emotional and/or psychological intimidation, verbal abuse, stalking, economic control, harassment, physical intimidation, or injury.

- **Threat assessment** is a fact-based investigative approach that evaluates whether an individual's behavior poses a risk to their safety or the safety of others. The appraisal of risk in a given situation focuses on an individual's actions, communications, and specific circumstances that might suggest that an individual intends to commit a violent act and/or is engaged in planning or preparing for that event.

- A **workplace safety plan** is a strategy developed in collaboration with the victim to implement workplace safety options including, but not limited to, handling of court protection orders; procedures for alerting security personnel; temporary or permanent adjustment of work schedules and locations; change in parking places; and requests for escorts to and from the workplace location.

PROCEDURES

- Identifying and Reporting Threats

  – Unlike most other types of violence, victims of intimate partner violence commonly will try to conceal their abuse. However, the *[school division]* has an overriding responsibility to respond to and take action to prevent violence that threatens school safety.

  – Employees who have secured any protective or restraining order that lists the workplace as a protected area are required to promptly inform the Office of School Safety and Security of such orders.

  – Employees who have not secured protective or restraining orders but have safety concerns with regard to intimate partner violence are strongly encouraged to report their concerns to the Office of School Safety so that appropriate safety measures can be put in place.

  – All *[school division]* employees are required to report to the Office of School Safety and Security any threats of domestic violence that they witness or of which they have knowledge.

  – Employees can be assured that *[school division]* will not retaliate against employees making such reports and will support victims of intimate partner violence by making workplace safety plans, providing referrals to Employee Assistance and other appropriate community resources, and permitting time off for addressing the threats of violence.

  – The *[school division]* Department of Human Resources, in collaboration with the Office of School Safety and Security, shall implement activities to ensure that all employees are aware of policies requiring the reporting of all workplace-related threats of domestic violence, understand the problem-solving purposes of threat assessment, and know how to report threats. Training for members of the Threat Assessment and Management Team shall include, but is not limited to:
    - Dynamics of intimate partner violence
    - Methods of responding to reports of workplace threats arising from abusive relationships
    - Circumstances requiring reporting to law enforcement

- Employer legal obligations to victims of intimate partner violence and related employee privacy issues
- Key elements of a workplace safety plan

Training and awareness activities for co-workers shall include but not be limited to:

1. Warning signs that an employee may be involved in a violent relationship;

2. Circumstances that appear to be tied to an abusive relationship that should be reported to the Threat Assessment and Management Team; and

3. Community, EAP, and other outside resources that can assist employees in addressing intimate partner violence including legal, psychological, and financial resources.

- Threat Assessment

  - All incidents and acts constituting a violation of law or applicable protective order will be reported immediately to law enforcement.

  - The Threat Assessment and Management Team shall determine whether intimate partner violence poses a risk to the workplace and determine what steps are necessary to prevent violent acts from being carried out. The assessment of risk should include inquiry about whether:

    - a relationship has recently been broken off. This is important because the most dangerous time in an abusive relationship typically occurs when the abused partner tries to separate from an abuser;

    - the abuser has made threats and, if so, how specific and credible are they;

    - the abused employee has sought or been granted a court order of protection and whether the abuser has violated an order in the past;

    - the abuser has a history of violence or other criminal activity;

    - the abuser has access to weapons or has recently acquired one;

    - there is a pattern of stalking behavior; and

    - the abuser has physically or sexually assaulted the employee.

- Response to Threats

  - The Threat Assessment and Management Team will coordinate resources both within and outside of the school division, as appropriate, to put in place a workplace safety plan. Security measures that may be established include, but are not limited to:
    - steps to limit the abuser's access to the workplace;

    - moving the abused employee's work space to a more protected, less vulnerable area;

    - providing a parking space close to building entrance or providing a security escort;

    - removing the employee's name from office telephone directories, changing his or her workplace e-mail address, or screening his or her calls;

    - requiring the employee to keep members of the team informed as to any contacts with and threatening actions of the abuser outside the workplace; and

    - referral to appropriate legal, financial, and counseling resources.

- Monitoring Response Effectiveness and Documentation

  – The Threat Assessment and Management Team shall maintain thorough documentation including all information gathered during incident management and ongoing monitoring, and all security measures taken as well as copies of all restraining, protective, or judicial orders relevant to the specific situation.

  – The Threat Assessment and Management Team will assess the effectiveness of its actions and, as needed, revise policies, procedures, and training. Policies, procedures, and training needs are to be reviewed annually in advance of the beginning of the school year.

See also:

Employee Policies (***specify those dealing with employee conduct and reporting of intimate partner violence)***

School Security and Critical Incident Policies *(**specify those most relevant for threat assessment and response**)*

RELATED READING ON WORKPLACE THREAT ASSESSMENT

ASIS International & Society for Human Resources Management (2011). Workplace violence prevention and intervention. Alexandria, VA: ASIS International. Available online at www.asisonline.org/Standards-Guidelines/Standards

Association of Threat Assessment Professionals (2006). Risk assessment guideline elements for violence: Considerations for assessing the risk of future violent behavior. Sacramento, CA: Author. Available online at http://atapworldwide.org/associations/8976/files/documents/RAGE-V.pdf

Meloy, J.R. & Hoffmann, J. (Eds.) (2013). The International Handbook of Threat Assessment. New York: Oxford.

Romano, S.J., Levi-Minzi, M.E., Rugala, E.A., & Van Hasselt, V.B. (2011, January). Workplace violence prevention. *F.B.I. Law Enforcement Bulletin*. Retrieved from www.fbi.gov/stats-services/publications/law-enforcement-bulletin/january2011/workplace_violence_prevention

Rugala, R.A. & Isaacs, A.R. (Eds) (2003). *Workplace violence: Issues in response*. Quantico, VA: National Center for Analysis of Violent Crime, FBI Academy. Available online at www.fbi.gov/stats-services/publications/workplace-violence

RELATED RESOURCES

Association of Threat Assessment Professionals – www.atapworldwide.org
The Association of Threat Assessment Professionals (ATAP) is a non-profit organization comprised of law enforcement, prosecutors, mental health professionals, corporate security experts, probation and parole personnel, and others involved in the area of threat and violence risk assessment. The purpose of ATAP is to afford its members a professional and educational environment to exchange ideas and strategies to address such issues as stalking, threats, and homeland security. The Association's website includes a Resource Library, Conference presentation materials, and information about membership and events.

National Resource Center on Domestic Violence – www.nrcdv.org
The Center is an independent, non-profit organization that serves as a comprehensive source of information for those wanting to educate themselves and help others on the many issues related to domestic violence.

National Resource Center on Workplace Responses – www.workplacesrespond.org
Funded by the U.S. Department of Justice, Office on Violence Against Women, the Center offers Internet-based information for those interested in providing effective workplace responses to victims of domestic violence, sexual violence, dating violence, and stalking. The site contains a workplace policy creation tool offering choices of model language.

Stalking Resource Center, National Center for Victims of Crime – www.victimsofcrime.org/src
The Center works to enhance the ability of professionals, organizations, and systems to respond effectively to stalking by providing training, technical assistance, and resource materials for professionals working with and responding to stalking.

APPENDIX A. SELECTED VIRGINIA LAWS RELATED TO THREAT ASSESSMENT

§ 22.1-79.4. Threat assessment teams and oversight committees.

A. Each local school board shall adopt policies for the establishment of threat assessment teams, including the assessment of and intervention with individuals whose behavior may pose a threat to the safety of school staff or students consistent with the model policies developed by the Virginia Center for School and Campus Safety in accordance with § 9.1-184. Such policies shall include procedures for referrals to community services boards or health care providers for evaluation or treatment, when appropriate.

B. The superintendent of each school division may establish a committee charged with oversight of the threat assessment teams operating within the division, which may be an existing committee established by the division. The committee shall include individuals with expertise in human resources, education, school administration, mental health, and law enforcement.

C. Each division superintendent shall establish, for each school, a threat assessment team that shall include persons with expertise in counseling, instruction, school administration, and law enforcement. Threat assessment teams may be established to serve one or more schools as determined by the division superintendent. Each team shall (i) provide guidance to students, faculty, and staff regarding recognition of threatening or aberrant behavior that may represent a threat to the community, school, or self; (ii) identify members of the school community to whom threatening behavior should be reported; and (iii) implement policies adopted by the local school board pursuant to subsection A.

D. Upon a preliminary determination that a student poses a threat of violence or physical harm to self or others, a threat assessment team shall immediately report its determination to the division superintendent or his designee. The division superintendent or his designee shall immediately attempt to notify the student's parent or legal guardian. Nothing in this subsection shall preclude school division personnel from acting immediately to address an imminent threat.

E. Each threat assessment team established pursuant to this section shall report quantitative data on its activities according to guidance developed by the Department of Criminal Justice Services.

F. Upon a preliminary determination by the threat assessment team that an individual poses a threat of violence to self or others or exhibits significantly disruptive behavior or need for assistance, a threat assessment team may obtain criminal history record information, as provided in §§ 19.2-389 and 19.2-389.1, and health records, as provided in § 32.1-127.1:03. No member of a threat assessment team shall redisclose any criminal history record information or health information obtained pursuant to this section or otherwise use any record of an individual beyond the purpose for which such disclosure was made to the threat assessment team.
2013, c. 710; 2014, cc. 7, 158; 2016, c. 554.

Note that the following references to the *Code of Virginia* include only the subsections of *Code* relevant to school threat assessment teams.

§ 19.2-389. Dissemination of criminal history record information.

A. Criminal history record information shall be disseminated, whether directly or through an intermediary, only to:

25. Members of a threat assessment team established by a local school board pursuant to § 22.1-79.4, by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805)*,* or by a private nonprofit institution of higher education, for the purpose of assessing or intervening with an individual whose behavior may present a threat to safety; however, no member of a threat assessment team shall redisclose any criminal history record information obtained pursuant to this section or otherwise use any record of an individual beyond the purpose that such disclosure was made to the threat assessment team;
2016, cc. 454, 554, 574.

§ 19.2-389.1. Dissemination of juvenile record information.

Record information maintained in the Central Criminal Records Exchange pursuant to the provisions of § 16.1-299 shall be disseminated only:

(x) to members of a threat assessment team established by a school board pursuant to § 22.1-79.4, by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805), or by a private nonprofit institution of higher education, to aid in the assessment or intervention with individuals whose behavior may present a threat to safety; however, no member of a threat assessment team shall redisclose any juvenile record information obtained pursuant to this section or otherwise use any record of an individual beyond the purpose that such disclosure was made to the threat assessment team;
2016, c. 554.

§ 32.1-127.1:03. Health records privacy.

A. There is hereby recognized an individual's right of privacy in the content of his health records. Health records are the property of the health care entity maintaining them, and, except when permitted or required by this section or by other provisions of state law, no health care entity, or other person working in a health care setting, may disclose an individual's health records.

Pursuant to this subsection:

3. No person to whom health records are disclosed shall redisclose or otherwise reveal the health records of an individual, beyond the purpose for which such disclosure was made, without first obtaining the individual's specific authorization to such redisclosure.

D. Health care entities may, and, when required by other provisions of state law, shall, disclose health records:

35. To a threat assessment team established by a local school board pursuant to § 22.1-79.4, by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805), or by a private nonprofit institution of higher education;
2016, c. 554.

§ 2.2-3705.2. Exclusions to application of chapter; records relating to public safety.

The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law:

7. Security plans and specific assessment components of school safety audits, as provided in § 22.1-279.8.

Nothing in this subdivision shall be construed to prohibit the disclosure of records relating to the effectiveness of security plans after (i) any school building or property has been subjected to fire, explosion, natural disaster or other catastrophic event, or (ii) any person on school property has suffered or been threatened with any personal injury.

17. Records received by the Department of Criminal Justice Services pursuant to §§ 9.1-184, 22.1-79.4, and 22.1-279.8 or for purposes of evaluating threat assessment teams established by a public institution of higher education pursuant to § 23-9.2:10 (Until October 1, 2016, thereafter § 23.1-805) or by a private nonprofit institution of higher education, to the extent such records reveal security plans, walk-through checklists, or vulnerability and threat assessment components.

§ 2.2-3705.4. Exclusions to application of chapter; educational records and certain records of educational institutions.

The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law:

8. Records of a threat assessment team established by a local school board pursuant to § 22.1-79.4 or by a public institution of higher education pursuant to § 23-9.2:10 relating to the assessment or intervention with a specific individual. However, in the event an individual who has been under assessment commits an act, or is prosecuted for the commission of an act that has

caused the death of, or caused serious bodily injury, including any felony sexual assault, to another person, the records of such threat assessment team concerning the individual under assessment shall be made available as provided by this chapter, with the exception of any criminal history records obtained pursuant to § 19.2-389 or 19.2-389.1, health records obtained pursuant to § 32.1-127.1:03, or scholastic records as defined in § 22.1-289. The public body providing such records shall remove information identifying any person who provided information to the threat assessment team under a promise of confidentiality.

§8.01-47. Immunity of persons investigating or reporting certain incidents at schools.

In addition to any other immunity he may have, any person who, in good faith with reasonable cause and without malice, acts to report, investigate or cause any investigation to be made into the activities of any student or students or any other person or persons as they related to conduct involving bomb threats, firebombs, explosive materials or other similar devices as described in clauses (vi) and (vii) of subsection A of §22.1-279.3:1, alcohol or drug use or abuse in or related to the school or institution or in connection with any school or institution activity, or information that an individual poses any credible danger of serious bodily injury or death to one or more students, school personnel, or others on school property shall be immune from all civil liability that might otherwise be incurred or imposed as the result of the making of such a report, investigation, or disclosure.
(2013, c. 665.)

§9.1-184. Virginia Center for School Safety created; duties.

A. From such funds as may be appropriated, the Virginia Center for School Safety (the Center) is hereby established within the Department. The Center shall:

1. Provide training for Virginia public school personnel in school safety, on evidence-based antibullying tactics, and in the effective identification of students who may be at risk for violent behavior and in need of special services or assistance;

2. Serve as a resource and referral center for Virginia school divisions by conducting research, sponsoring workshops, and providing information regarding current school safety concerns, such as conflict management and peer mediation, bullying, school facility design and technology, current state and federal statutory and regulatory school safety requirements, and legal and constitutional issues regarding school safety and individual rights;

3. Maintain and disseminate information to local school divisions on effective school safety initiatives in Virginia and across the nation;

4. Collect, analyze, and disseminate various Virginia school safety data, including school safety audit information submitted to it pursuant to § 22.1-279.8, collected by the Department;

5. Encourage the development of partnerships between the public and private sectors to promote school safety in Virginia;

6. Provide technical assistance to Virginia school divisions in the development and implementation of initiatives promoting school safety, including threat assessment-based protocols with such funds as may be available for such purpose;

7. Develop a memorandum of understanding between the Director of the Department of Criminal Justice Services and the Superintendent of Public Instruction to ensure collaboration and coordination of roles and responsibilities in areas of mutual concern, such as school safety audits and crime prevention;

8. Provide training for and certification of school security officers, as defined in § 9.1-101 and consistent with § 9.1-110;

9. Develop, in conjunction with the Department of State Police, the Department of Behavioral Health and Developmental Services, and the Department of Education, a model critical incident response training program for public school personnel and others providing services to schools that shall also be made available to private schools in the Commonwealth; and

10. In consultation with the Department of Education, provide schools with a model policy for the establishment of threat assessment teams, including procedures for the assessment of and intervention with students whose behavior poses a threat to the safety of school staff or students.

B. All agencies of the Commonwealth shall cooperate with the Center and, upon request, assist the Center in the performance of its duties and responsibilities.
    (2000, c. 519, § 9-173.21; 2001, cc. 436, 440, 844; 2002, cc. 836, 868; 2012, cc. 281, 433; 2013, cc. 676, 710.)

§ 22.1-272.1. Suicide prevention in public schools

Responsibility to contact parent of student at imminent risk of suicide; notice to be given to social services if parental abuse or neglect; Board of Education, in cooperation with the Department of Behavioral Health and Developmental Services and the Department of Health, to develop guidelines for parental contact.

A. Any person licensed as administrative or instructional personnel by the Board of Education and employed by a local school board who, in the scope of his employment, has reason to believe, as a result of direct communication from a student, that such student is at imminent risk of suicide, shall, as soon as practicable, contact at least one of such student's parents to ask whether such parent is aware of the student's mental state and whether the parent wishes to obtain or has already obtained counseling for such student. Such contact shall be made in accordance with the provisions of the guidelines required by subsection C.

B. If the student has indicated that the reason for being at imminent risk of suicide relates to parental abuse or neglect, this contact shall not be made with the parent. Instead, the person shall, as soon as practicable, notify the local department of social services of the county or city wherein the child resides or wherein the abuse or neglect is believed to have occurred or the state Department of Social Services' toll-free child abuse and neglect hotline, as required by § 63.2-1509. When giving this notice to the local or state department, the person shall stress the need to take immediate action to protect the child from harm.

C. The Board of Education, in cooperation with the Department of Behavioral Health and Developmental Services and the Department of Health, shall develop guidelines for making the contact required by subsection A. These guidelines shall include, but need not be limited to, (i) criteria to assess the suicide risks of students, (ii) characteristics to identify potentially suicidal students, (iii) appropriate responses to students expressing suicidal intentions, (iv) available and appropriate community services for students expressing suicidal intentions, (v) suicide prevention strategies which may be implemented by local schools for students expressing suicidal intentions, (vi) criteria for notification of and discussions with parents of students expressing suicidal intentions, (vii) criteria for as-soon-as-practicable contact with the parents, (viii) appropriate sensitivity to religious beliefs, and (ix) legal requirements and criteria for notification of public service agencies, including, but not limited to, the local or state social services and mental health agencies. These guidelines may include case studies and problem-solving exercises and may be designed as materials for in-service training programs for licensed administrative and instructional personnel.
    (1999, c. 425; 2009, cc. 813, 840.)

§ 22.1-279.3:1. Reports of certain acts to school authorities.

A. Reports shall be made to the division superintendent and to the principal or his designee on all incidents involving (i) the assault or assault and battery, without bodily injury, of any person on a school bus, on school property, or at a school-sponsored activity; (ii) the assault and battery that results in bodily injury, sexual assault, death, shooting, stabbing, cutting, or wounding of any person, or stalking of any person as described in § 18.2-60.3, on a school bus, on school property, or at a school-sponsored activity; (iii) any conduct involving alcohol, marijuana, a controlled substance, imitation controlled substance, or an anabolic steroid on a school bus, on school property, or at a school-sponsored activity, including the theft or attempted theft of student prescription medications; (iv) any threats against school personnel while on a school bus, on school property or at a school-sponsored activity; (v) the illegal carrying of a firearm, as defined in § 22.1-277.07, onto school property; (vi) any illegal conduct involving firebombs, explosive materials or devices, or hoax explosive devices, as defined in § 18.2-85, or explosive or incendiary devices, as defined in § 18.2-433.1, or chemical bombs, as described in § 18.2-87.1, on a school bus, on school property, or at a school-sponsored activity; (vii) any threats or false threats to bomb, as described in § 18.2-83, made against school personnel or involving school property or school buses; or (viii) the arrest of any student for an incident occurring on a school bus, on school property, or at a school-sponsored activity, including the charge therefor.

B. Notwithstanding the provisions of Article 12 (§ 16.1-299 et seq.) of Chapter 11 of Title 16.1, local law-enforcement authorities shall report, and the principal or his designee and the division superintendent shall receive such reports, on offenses, wherever committed, by students enrolled at the school if the offense would be a felony if committed by an adult or would be a violation of the Drug Control Act (§ 54.1-3400 et seq.) and occurred on a school bus, on school property, or at a school-sponsored activity, or would be an adult misdemeanor involving any incidents described in clauses (i) through (viii) of subsection A, and whether the student is released to the custody of his parent or, if 18 years of age or more, is released on bond. As part of any report concerning an offense that would be an adult misdemeanor involving an incident described in clauses (i) through (viii) of subsection A, local law-enforcement authorities and attorneys for the Commonwealth shall be authorized to disclose information regarding terms of release from detention, court dates, and terms of any disposition orders entered by the court, to the superintendent of such student's school division, upon request by the superintendent, if, in the determination of the law-enforcement authority or attorney for the Commonwealth, such disclosure would not jeopardize the investigation or prosecution of the case. No disclosures shall be made pursuant to this section in violation of the confidentiality provisions of subsection A of § 16.1-300 or the record retention and redisclosure provisions of § 22.1-288.2. Further, any school superintendent who receives notification that a juvenile has committed an act that would be a crime if committed by an adult pursuant to subsection G of § 16.1-260 shall report such information to the principal of the school in which the juvenile is enrolled.

C. The principal or his designee shall submit a report of all incidents required to be reported pursuant to this section to the superintendent of the school division. The division superintendent shall annually report all such incidents to the Department of Education for the purpose of recording the frequency of such incidents on forms that shall be provided by the Department and shall make such information available to the public.

In submitting reports of such incidents, principals and division superintendents shall accurately indicate any offenses, arrests, or charges as recorded by law-enforcement authorities and required to be reported by such authorities pursuant to subsection B.

A division superintendent who knowingly fails to comply or secure compliance with the reporting requirements of this subsection shall be subject to the sanctions authorized in § 22.1-65. A principal who knowingly fails to comply or secure compliance with the reporting requirements of this section shall be subject to sanctions prescribed by the local school board, which may include, but need not be limited to, demotion or dismissal.

The principal or his designee shall also notify the parent of any student involved in an incident required pursuant to this section to be reported, regardless of whether disciplinary action is taken against such student or the nature of the disciplinary action. Such notice shall relate to only the relevant student's involvement and shall not include information concerning other students.

Whenever any student commits any reportable incident as set forth in this section, such student shall be required to participate in such prevention and intervention activities as deemed appropriate by the superintendent or his designee. Prevention and intervention activities shall be identified in the local school division's drug and violence prevention plans developed pursuant to the federal Improving America's Schools Act of 1994 (Title IV—Safe and Drug-Free Schools and Communities Act).

D. Except as may otherwise be required by federal law, regulation, or jurisprudence, the principal shall immediately report to the local law-enforcement agency any act enumerated in clauses (ii) through (vii) of subsection A that may constitute a criminal offense and may report to the local law-enforcement agency any incident described in clause (i) of subsection A. Nothing in this section shall require delinquency charges to be filed or prevent schools from dealing with school-based offenses through graduated sanctions or educational programming before a delinquency charge is filed with the juvenile court.

Further, except as may be prohibited by federal law, regulation, or jurisprudence, the principal shall also immediately report any act enumerated in clauses (ii) through (v) of subsection A that may constitute a criminal offense to the parents of any minor student who is the specific object of such act. Further, the principal shall report that the incident has been reported to local law enforcement as required by law and that the parents may contact local law enforcement for further information, if they so desire.

E. A statement providing a procedure and the purpose for the requirements of this section shall be included in school board policies required by § 22.1-253.13:7.

The Board of Education shall promulgate regulations to implement this section, including, but not limited to, establishing reporting dates and report formats.

F. For the purposes of this section, "parent" or "parents" means any parent, guardian or other person having control or charge of a child.

G. This section shall not be construed to diminish the authority of the Board of Education or to diminish the Governor's authority to coordinate and provide policy direction on official communications between the Commonwealth and the United States government.
(2013, c. 800; 2014, cc. 674, 719.

§ 18.2-60. Threats of death or bodily injury to a person or member of his family; threats to commit serious bodily harm to persons on school property; penalty.

A. 1.   Any person who knowingly communicates, in a writing, including an electronically transmitted communication producing a visual or electronic message, a threat to kill or do bodily injury to a person, regarding that person or any member of his family, and the threat places such person in reasonable apprehension of death or bodily injury to himself or his family member, is guilty of a Class 6 felony. However, any person who violates this subsection with the intent to commit an act of terrorism as defined in § 18.2-46.4 is guilty of a Class 5 felony.

2.   Any person who communicates a threat, in a writing, including an electronically transmitted communication producing a visual or electronic message, to kill or do bodily harm, (i) on the grounds or premises of any elementary, middle or secondary school property, (ii) at any elementary, middle or secondary school-sponsored event or (iii) on a school bus to any person or persons, regardless of whether the person who is the object of the threat actually receives the threat, and the threat would place the person who is the object of the threat in reasonable apprehension of death or bodily harm, is guilty of a Class 6 felony.

B. Any person who orally makes a threat to any employee of any elementary, middle or secondary school, while on a school bus, on school property or at a school-sponsored activity, to kill or to do bodily injury to such person, is guilty of a Class 1 misdemeanor.

A prosecution pursuant to this section may be either in the county, city or town in which the communication was made or received.
(2002, cc. 588, 623)

PREVENTATIVE MEASURES

BUILDING THREAT ASSESSMENT TEAMS IN SCHOOLS:

WHO'S ON THE TEAM? MISSION, MEMBERSHIP AND MOTIVATION

THE 2015 NATIONAL BEHAVIORAL INTERVENTION TEAM ASSOCIATION (NaBITA) WHITEPAPER

THE NaBITA 2015 WHITEPAPER
WHO'S ON THE TEAM?
MISSION, MEMBERSHIP, AND MOTIVATION
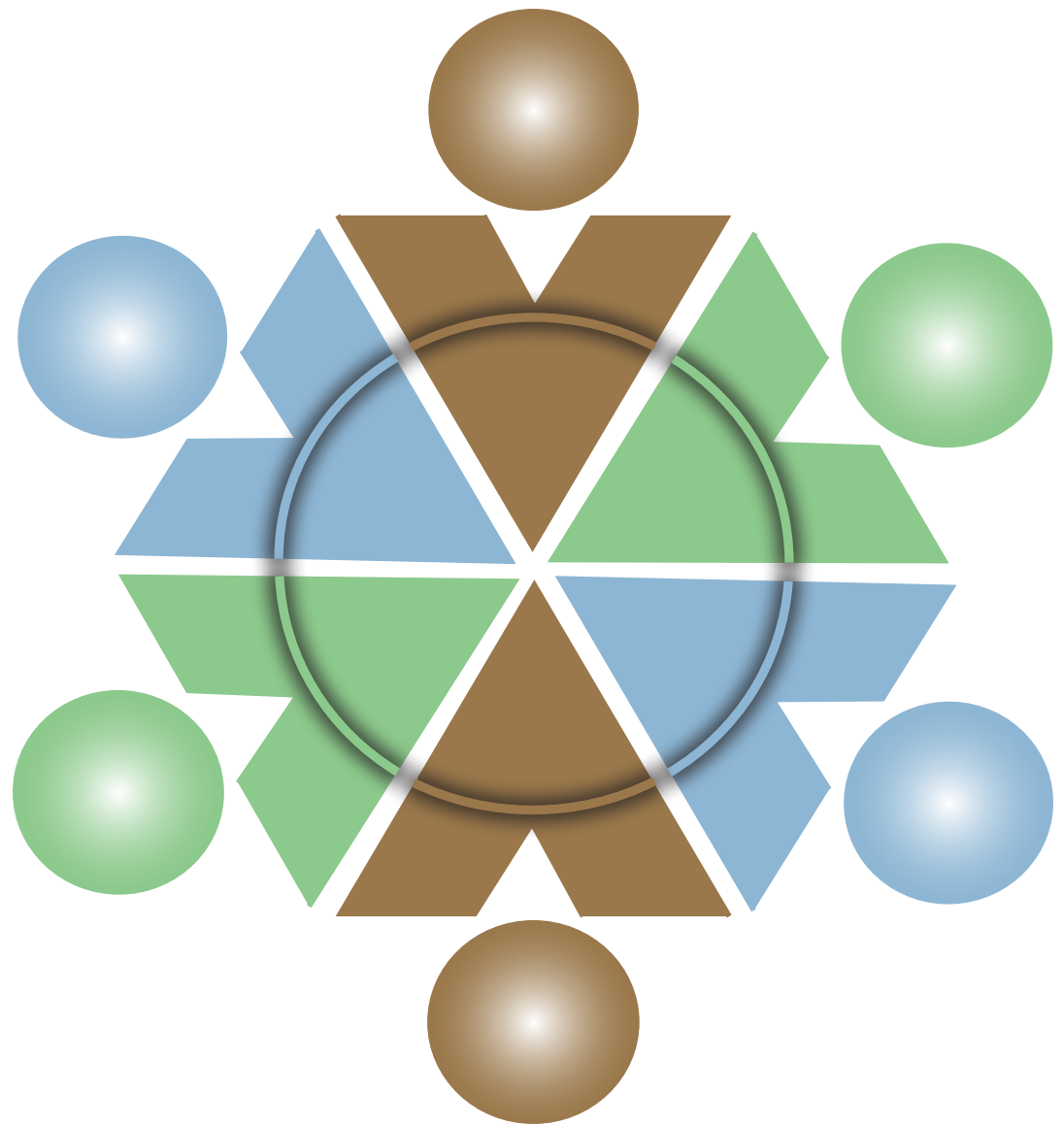
By:
Brian Van Brunt, Ed.D.
Aaron "Chip" Reese, Ed.D.
W. Scott Lewis, J.D.

TABLE OF CONTENTS

INTRODUCTION

Each year, the NaBITA Advisory Board meets to discuss what whitepaper topics are most relevant for the field of behavioral intervention. At times, these are emerging practices or specialized issues such as threat assessment, mental health management, or compliance with federal mandates. Other times, we find ourselves returning to the core issues of training that remain a frequent topic of conversation for our membership. This year, the Advisory Board selected the topic of BIT mission statement development and the more intensive discussion of team membership and motivations as whitepaper topics.

College campuses are constantly refreshing their populations. Every four to six years, there is nearly a 100 percent turnover of the student body (though perhaps less at some community colleges). In addition, many faculty and staff members retire or accept positions at other institutions each year. As a result, BIT focus and composition can change over time with employee turnover; as can its methods for interacting and communicating with the campus community, leaving new students with less understanding than those from previous classes about what the team does and how to engage its help when someone's behavior becomes cause for concern. This whitepaper should help BIT teams refocus on the core issues of ensuring the campus knows about the BIT and its mission.

VISION AND MISSION STATEMENTS

One of the central tasks for teams is the development of vision and mission statements. These statements should drive the BIT's actions and serve as a touchstone for those times where the team begins to drift off course. A mission statement communicates (to the greater college community and beyond) a commitment to intentional action with a goal of ensuring safety and wellbeing. To this end, exemplary teams' missions have evolved to reflect a focus on pattern analysis, faculty and staff concerns, and threat assessment.

'...Exemplary teams' missions have evolved to reflect a focus on pattern analysis, faculty and staff concerns, and threat assessment.'

A vision statement defines what the team will do and why it should exist. Some vision statements have defined goals, while others are more general in nature. In either case, both BIT vision and mission statements should reflect the vision and mission statements of the institution. At times, these statements may be combined into a single, comprehensive statement. Most importantly, the statements — and the subsequent action plans — should be tied to the strategic plan of the institution.

For example, a team mission that reads, "To identify and intervene with students who pose a threat to the campus community," will be more focused on violence and danger to the community. On the other hand, a team that has a mission, "To identify and assist at-risk and struggling students become more connected to services," may have a stronger focus on student assistance and may even be concerned with enrollment retention rather than dangerousness. When considering the mission and/or purpose statement, the team needs to consider the scope and reach of their work. Once that mission/ purpose is identified, the team must guard against becoming the landing place for all reported problems on campus. Just as the mission statement defines the population and capacity of the team, it also determines what the BIT is not.

In 2013, the Jed Foundation brought together some key leaders in the field to create a document titled, "Balancing Safety and Support on Campus: A Guide to Campus Teams." In terms of mission and purpose statement, the document offers this advice:

'When considering the mission and/or purpose statement, the team needs to consider the scope and reach of their work.'

In general, the mission/purpose of campus teams encompasses:

» Gathering information about students of concern. This may specifically focus on threats with the potential to become violent (as is the case with threat assessment teams) or on a broader range of behaviors. As noted below, this may also expand to include behaviors by others on- or off-campus, besides students.

» Assessing the information about each case in a systematic way to determine the most effective response for that particular person and situation.

» Defining the plan/response to address both the needs of the student and the safety of the community. The plan should consider specifics about who, when, where, and how the response will occur.

» Implementing the response in a way that de-escalates a potential crisis, reduces or removes threats, and attends to the needs of the individual who is demonstrating disturbed and/or disturbing behavior. Note that for many campus teams, the actual implementation of a response may be carried out by other individuals or departments; the team itself often acts in an advisory and coordinating role.

» Monitoring the disposition of the case to gauge whether any additional follow-up is needed, whether the response was effective, and what lessons may be learned for future cases, especially in terms of implications for school policies and procedures (p. 3).

The development of a vision and/or a mission statement should serve as an opportunity for a team to engage in a discussion to define the team's scope and focus, and help guide future action. While drawing from other statements is a useful place to start, we

encourage you to wrestle more directly with how your BIT should be defined against the backdrop of your individual campus. In the 2013 Jed Foundation paper, the authors wrote, "Each school will have unique needs that a campus team may meet, depending on its size, history, resources, and potential overlap with other existing campus committees and procedures" (p.3).

Deisinger, Randazzo, O'Neill, and Savage (2008: 47) suggest the following for a mission statement: "Identify a student, faculty member, or staff member who has engaged in threatening behaviors or done something that raised serious concern about their well-being, stability, or potential for violence or suicide." This type of statement is more appropriate for a Threat Assessment Team, or TAT, where the main focus in on responding to existing threats. However, given that the BIT mission is more preventative and educational in nature, focusing on addressing such behaviors before they become threats, that kind of statement is not sufficient for BITs. As an aside, many of the mission statement examples provided in the 2014 NaBITA survey had a similar, limited focus on threat assessment alone. It would be our recommendation that BITs focus on prevention and early identification of warning behaviors in addition to the assessment of threats.

'It would be our recommendation that BITs focus on prevention and early identification of warning behaviors in addition to the assessment of threats.'

The background experience of the team's membership also has an impact on the mission. Some BITs become focused on law enforcement and police response, others on mental health risk, and all seem focused and concerned with the legal and policy implications of their decisions. Regardless of team members' backgrounds, there should be a respect for the intersection between the law, policy, mental health, and law enforcement. This creates opportunities for departments to work together and reduce communication barriers.

Isolated communications occur when each department on campus focuses on its own individual mission, policy, and rules without seeing the members of their communities as part of a larger, more complex system. Individual departments that don't communicate outside their own walls to the detriment of campuswide threat assessment and behavioral intervention, are often referred to as operating in a "silo." Much like the tall grain silos that dot the Midwest, they are single structures serving their function but separated from the larger system of which they are a part.

Meloy, Hoffmann, Guldimann, and James (2011: 19) further define this danger: "There is always the risk of a 'silo effect' — different domains of behavior are never linked together or synthesized to develop a comprehensive picture of the subject of concern, conduct further investigation, identify other warning behaviors, and actively risk-manage the case."

The following data comes from the 2014 NaBITA team survey results (Van Brunt, Sokolow, Lewis, Schuster, and Golston) in response to the questions, "Does your team have a mission statement?" and "If you are willing to share your BIT mission statement, please cut and paste it here." Over 60 percent of teams reported having a mission statement. Several key themes emerged from our analysis of over 200 mission statements shared. BITs who shared mission statements often included the following:

» Scope of team reach (e.g., faculty, staff, and students).
» Discussion of the balance between the needs of the individual and the safety of the community.
» Defining focus on threat assessment.
» Defining focus on early prevention and intervention.
» Mention of connection to the institution's academic mission.

The following examples would be useful for new teams interested in seeing a summary of mission statements being used by BITs across the country. Our thanks to those who shared their team's mission statements in the 2014 NaBITA survey. The team names and identifying school information were deleted to protect the privacy of the respondents who shared their narratives with NaBITA. The term BIT was used for consistency to replace individual team names. These are offered in order of preference. While each of these has their own merits, the more encompassing statements are at the top of the list:

1. The BIT is committed to promoting safety via a proactive, multidisciplinary, coordinated, and objective approach to the prevention, identification, assessment, intervention, and management of situations that pose, or may pose a threat to the safety and wellbeing of our campus community (i.e., students, faculty, staff, and visitors).

2. The BIT is dedicated to improving community through a proactive, objective, supportive, and collaborative approach to the prevention, identification, assessment, intervention, management, and coordinated response of student situations that may pose a threat to the safety and wellbeing of individuals and the campus community.

3. [The] Behavioral Intervention Team is a campuswide team of appointed professionals responsible for identifying, assessing, and responding to serious concerns and/or disruptive behaviors by students who may threaten the health or safety of the campus community.

4. The BIT engages in proactive and collaborative approaches to identify, assess, and mitigate risks associated with students exhibiting concerning behaviors. By partnering with members of the community, the team strives to promote individual student wellbeing and success while prioritizing community safety.

5. The BIT is a multidisciplinary proactive campus threat assessment and behavioral intervention team committed to improving the overall safety of the campus. This is accomplished through a coordinated, objective approach to prevention, identification, assessment, intervention, and management of situations that pose, or may reasonably pose a threat to the safety and wellbeing of the campus community

6. The mission of the Behavioral Intervention Team is to promote safety in our college community through a proactive and coordinated approach to the identification, assessment, intervention, and management of situations that pose, or may reasonably pose, a threat to the safety and well-being of the campus community. The highest goal is to prevent unsafe behavior and develop support plans for students of concern.

7. The mission of the University Behavioral Intervention Team is to provide a caring program of identification, intervention, and response while balancing the needs of the individual with those of the community. The BIT identifies students whose behavioral patterns have raised concern about their wellbeing; centralizes communication to gain a more complete understanding of the whole individual student; and, develops a collaborative outreach plan with campus and community resources to address identified risks.

8. In the interest of cultivating community welfare and safety, the BIT proactively operates to raise awareness of concerning behaviors through training, accountability, and assessments. The team connects, communicates, and engages timely response and intervention to empower positive differences in people's lives and to prevent violence. The team serves as a resource, providing referrals, consultation, and support to the campus community.

9. The BIT is dedicated to a proactive, coordinated and planned approach to the identification, prevention, assessment, management, and reduction of interpersonal and behavioral threats to the safety and wellbeing students, faculty, staff, and visitors. This committee will identify students who are at risk to themselves or others because of their behavior on campus. They may be a physical risk to self or others; they may be at risk because they are disruptive in classes, on campus, or in the residence halls; or they may be at risk because of poor choices that result in danger to self or others.

10. The BIT is a campuswide team that provides consultation, makes recommendations, and coordinates the university's response in situations involving students who engage in concerning, disruptive, and/or potentially harmful behavior. The team serves as a resource to the campus community and is designed for early intervention regarding behavioral issues to help support the health, safety, and success of students.

11. The Behavioral Intervention Team is committed to the wellbeing and safety of all members of the campus community. It has been developed to provide guidance for the students, staff, and faculty regarding how to seek assistance and report student behaviors of concern. In addition, it seeks to sustain a campus network where the campus community can respond proactively to situations involving students of concern by connecting those students to essential support services. It is the intent of the BIT that the campus community work in a coordinated and collaborative fashion to address students of concern in a timely and consistent manner.

TEAM MEMBERSHIP

As with mission statements, it is important to gather a team that matches the needs of the college or university for which the team serves. While data from the 2014 NaBITA survey provides some useful guidelines for those who are in the process of building their team, remember the importance of incorporating the unique nature of each school into organizational decisions. A school at which 68 percent of the student body is part of a Greek organization should include someone from Greek life on the BIT. If over half of the population of the university is known to the disability services office and receive accommodations, then having someone from that department on the BIT makes sense. When looking at team membership, it is critical

'A map or GPS device can serve as a helpful guide to travelers, but they must remain aware of their surroundings and adjust accordingly or risk driving into a lake, dead-ending at a bridge under construction, or missing a turn because a highway exit is not longer there. Likewise, BITs should use guidelines and others' statements for direction, but adjust to ensure the end results comport to their institutions' needs.'

to consider the context of your specific institution. A map or GPS device can serve as a helpful guide to travelers, but they must remain aware of their surroundings and adjust accordingly or risk driving into a lake, dead-ending at a bridge under construction, or missing a turn because a highway exit is not longer there. Likewise, BITs should use guidelines and others' statements for direction, but adjust to ensure the end results comport to their institutions' needs.

Overall, three groups act as the "Id, Ego, and Superego" of the BIT, the Id being the base, primal response, the superego being the aspirational and moral philosophy, and the Ego being the balance between the Id and Superego. These are law enforcement/security, mental health, and student affairs, respectively. At a minimum, all effective teams will have these disciplines represented (with appropriate backups). In terms of team size, the 2014 survey found that eight to nine members was the average team size at most institutions represented.

CORE, INNER, MIDDLE, AND OUTER CIRCLE

One challenge of BITs is ensuring that they have representation from all relevant campus departments but is not so large that meeting, making decisions, and keeping track of who is doing what becomes impossible. For that reason, a BIT that is structures like three concentric circles, with one core group of members and middle and outer circle members who can be pulled in as needed is advisable.

CORE MEMBER CHARACTERISTICS:

They NEVER miss a meeting — that is to say, they are always represented because...

- *They have a backup, often one who attends meetings regularly.*
- *They're able to quickly reach other core members.*
- *They have full access to the BIT database.*
- *They're likely also on the CIRT or TAT.*

CORE MEMBERS

When it comes the core group, or the essential team members, the following are most commonly represented on BITs, according to the 2014 NaBITA survey:

- » Counseling (92 percent of teams).
- » Police/campus safety (88 percent of teams).
- » Dean of students (75 percent of teams).
- » Student conduct (75 percent of teams). (Note: Student conduct and dean of students are often the same person.)
- » Housing and residential life (59 percent of teams).
- » Case managers (20 percent, but a growing trend for larger campuses).
- » Human resources and/or academic administration (29 percent, but important for teams that take reports about staff and faculty as well).

INNER CIRCLE CHARACTERISTICS:

- *They are generally at every meeting.*
- *They represent a constituency that is critical to the team (e.g., Greek life or athletics).*
- *They represent a group that is critical to reporting (e.g., faculty).*
- *They have a proxy, but not a formal backup.*
- *They have access to the database, and likely full access.*
- *They may also be on the CIRT or TAT.*

INNER AND MIDDLE CIRCLE MEMBERS

The next group makes up the inner circle members. Larger teams may include them as core members, but smaller teams often invite these individuals to join meetings as needed. There is a subtle but critical difference between inner and middle that is illustrated in the characteristics section that follows. These members typically include:

- » Academic affairs (53 percent of teams).
- » Health services (40 percent of teams).
- » Vice president of student affairs (40 percent of teams). (Note: Sometimes this is the dean of students as well. At larger schools the VPSA should be a middle group member.)
- » Faculty representative (30 percent of teams).
- » Human resources (29 percent of teams). (Note: Inner circle for teams that do not act on reports regarding staff and faculty, but still may get them.)
- » Student activities (21 percent of teams).
- » Legal counsel (17 percent of teams).
- » Admissions (8 percent of teams).
- » Greek Life (4% of teams).

- *They are invited when they may have insight into a smaller constituent group.*
- *They may have insight into the subject of the report or reporter.*
- *They' represent a group that is important to reporting.*
- *They have limited, if any, access to the database (unless their other job requires it).*
- *They may be on the CIRT or TAT, usually in the same capacity.*

The middle circle is made up of individuals who are either invited to the team only as needed or are included in the weekly team membership due to a special population or contextual issue at a particular institution. For example, the veterans services coordinator may be part of the individual weekly team meetings if the college has a 70 percent veteran population. These middle circle team members include:

» ADA coordinator.
» Financial aid administrator.
» Athletics staff member.
» University chaplain.
» Community mental health staff (e.g., psychiatrist or counselor).
» Title IX official.
» Risk manager.
» Veterans affairs employee.
» Multi-cultural affairs staff.
» First-year programs coordinator.
» Student success and achievement staff.

OUTER CIRCLE CHARACTERISTICS:
- *They do not attend meetings, but core or inner circle members may reach out to them as needed.*
- *They are needed to provide outreach to the student or some related party.*
- *They have NO access to the database unless some other part of their job requires it.*

OUTER CIRCLE MEMBERS

The outer circle members are those who are kept in the loop as needed. These are the individuals that the Family Educational Rights and Privacy Act would consider to have a legitimate, educational need to know some very limited information regarding the response and/or report, and may be asked by the team to provide some form of outreach.

One might argue that they are not really team members at all, as they will not attend the BIT meetings, but they are still important to the team's function. Some examples of outer circle members may be listed above — it is truly campus dependent — but others may include:

» General faculty members.
» Administrative staff and support staff.
» Deans, assistant, and associate deans.
» Academic advisors.
» Coaches and assistant coaches.
» Student organization advisors.
» Family members of the reported person.
» Friends of the reported person.

MOTIVATION

After reviewing what membership composition makes sense for your college or university BIT, it is helpful to review the motivation and challenges faced by each of the various individuals who may find themselves on a BIT. This section describes the central purpose and motivation that should influence members of the BIT, as well as outline some challenges they may face in terms of participating on the team. This is not an exhaustive list, but represents some of more common members of the team or those whose positions require additional explanation to be as effective as possible. With the team members described, it should be understood that each should have policy and practice experience in their respective area, and have the authority to take independent action when needed.

CHAIR

Team leadership is a crucial element for team success. A BIT chair must be vested with the authority to compel students to complete psychological and threat assessments, address academic concerns, and refer students to the conduct office with the recommendation to separate them from the university. A team leader without the authority to act on these issues runs the risk of identifying a high-risk situation and not having the ability to mitigate the risk by responding with an appropriate action. Dunkle, Silverstein and Warner (2008: 593) write:

> The team leader should be a senior student affairs administrator who has high-level authority to manage student behavior and who has a solid understanding of the institution's administrative structure, the institution's policies and procedures concerning student conduct, and the complexity of managing difficult student situations.

The chair should also possess a certain charisma and garner respect and confidence from the other team members and the greater campus community. A leader who does not have the respect and the ability to persuade and motivate others lacks the skills to properly manage the group process of the team. Eells and Rockland-Miller (2011: 16) suggest that a team leader should be "well respected and have outstanding communication skills and judgment."

Leading the BIT must be a priority for the chair that is well understood by the institution. As the institution places the appropriate emphasis on behavioral intervention, it must ensure that the leader is not over-committed in other areas (Warrell, 2012). Likewise, the chair must understand that s/he is leading a team and not holding a regular briefing

on what has taken place since the last meeting. By assembling the right team members, providing training related to each of their positions, and having a system of communication in place that allows lead-time for gathering data, BIT members will arrive at meetings ready to share their information and expertise (Reese, 2014).

The team leader should have a commitment to the team's mission statement and vision, as well as a keen focus on the BIT's strategic plan. The leader does not cancel meetings because it's summer or "there isn't anything to discuss this week." The team leader, like the leader of a police force or firehouse, has the responsibility to keep the team sharp and ready to perform, even during the rare "quiet" times when cases are not pressing or when the activity on campus has slowed. In these cases, the meeting should be dedicated to tabletop exercises and/or other professional development. Preventing campus violence and reducing the potential for at-risk students to escalate demands a certain level of vigilance and dedication, traits that must be sustained in the face of a team that may be tired, overwhelmed, or unmotivated.

The most common question here is, "Is there a specific position that should lead the team?" The answer lies above, but there is a trend that bears mentioning. BIT leaders most commonly come from student affairs. However, a recent trend of hiring case managers or team chairs as a stand-alone position may become the most common practice, especially at schools where the caseload warrants a full-time position. Schools should track time spent on case management to determine need.

Additionally, it is important that the BIT have a designated assistant chair or understood second-in-command. In the event that the chair is away during a regularly scheduled meeting or it is necessary to call a special meeting, this assistant chair must have the ability and authority to act in the chair's absence. The chair should look for opportunities for the assistant chair to lead the BIT. This can be done by allowing the assistant chair to set and send out the agenda, take the leadership role with particular cases, and deliver training to the team.

DEAN OF STUDENTS/VPSA

Both of these positions are commonly involved on BITs. They are often involved in the creation and leadership of the team, pulling together the various campus departments and groups needed to identify and manage at-risk students on their campus, and are often a first line of contact for faculty and staff who are concerned about students who may present a threat or may have violated the student conduct code. The dean of students /vice president for student affairs will be able to bring expertise in student affairs theory,

practice, and policy, as well as educational law related to students. Some schools will appoint the dean of students as the team leader because of that individual's involvement in student judicial matters. However, for the dean of students to be effective in this position, s/he must possess the ability to see through more than just a conduct code lens.

Depending on the size and make-up of an institution, the dean of students or vice president for student affairs may carry too much gravitas to sit on the team. If that individual's presence may prevent others from speaking freely, the team's effectiveness will be greatly diminished. Additionally, the VPSA may need to not be on the team so that there is a buffer between the upset student/family member and the institution's president. The VPSA can serve as an informal appeal (there should be no BIT appellate process, as it is not involved in hearings). In such situations, the VPSA must have a keen understanding of what the BIT does and how, but becomes a middle circle member. This scenario is more common at larger institutions.

A cautionary note: As VPSAs separate from the team, they must be careful not to become mired in the politics of a case, but remember that the BIT reached its conclusions using objective criteria. They should be advocates for the BIT's decisions at the senior level. For example, consider the case of a student who has hit the BIT threshold for a mandated assessment, but whose parents are screaming at the president, arguing there is nothing wrong with their child and threatening to sue. This student and his family should not find an advocate in the VPSA for avoiding the assessment. Instead, the VPSA should explain to the student and his family that an assessment or other course of action is important to the student's success and is a decision that was reached objectively. The VPSA should additionally work to ensure the college president understands how that decision was reached, and that granting arbitrary exceptions to BIT decisions poses too great a risk to the institution.

COUNSELING DIRECTOR

Counseling directors are commonly involved in BITs to provide mental health consultation and connection between the counseling department and the team. This relationship can at times be tenuous due to laws and ethics surrounding mental health professionals and counseling records. The JED Foundation (2008) notes that, "[w]ithout a student's consent, a clinician is rarely able to discuss information learned as part of the therapeutic relationship with campus administrators or even acknowledge that the student is in treatment … In contrast, a clinician can always receive information from any source (e.g., a faculty member) about a student who is currently in treatment" (p.10).

This may raise the question of how a counselor can contribute to a BIT, other than to gain information about a client or notify officials of a client who poses an imminent threat to self or others. For one, counselors can be great storytellers. Without providing any identifiable characteristics, counselors have the ability to share relevant case studies and tendencies of similarly situated persons of concern, which can be of great assistance to the team. In fact, counselors and counseling directors should be constantly be speaking in hypotheticals. If they offer information only when a student is not their client, they are tacitly admitting when a student is their client. However, if counselors or counseling directors just sit in the room without saying anything, then they are not a contributing part of the team.

Due to confidentiality laws and professional ethics, it would be ill advised to have the counseling director serve as the BIT chair. A possible exception to this may be at a school with a large counseling staff, where the director is purely an administrator and sees virtually no clients. Even then, that individual should likely not be the chair, but may have to if s/he possesses the BIT leadership characteristics noted earlier, and no one else is a more appropriate fit for that role.

RESIDENCE LIFE

When a school has a significant number of residential students the residence life department is commonly represented on the team via a hall director or director of housing/residence life. They are well connected to the community and have a first-hand knowledge of students and their social connections and habits. Student affairs professionals understand that human intelligence information gathering from those who are in contact with a person of concern is the best tool the college has at its disposal for behavioral intervention (Reese, 2013). On a recent posting for an assistant director for residence life position at Moravian College on HigherEdJobs.com[1], one of the related responsibilities listed was to, "Serve on the college behavior intervention team and assist in the counseling of students on personal and development matters."

The residence life representative needs to be someone with the authority to move quickly in room reassignment and contract forgiveness, and the ability to gather information from staff members. The director of housing or the deputy is the best candidate for this.

---

1 Moravian College, HigherEdJobs.com *www.higheredjobs.com/admin/details.cfm?JobCode= 176020527&Title=Assistant%20Director%20of%20Residence%20Life.*

HUMAN RESOURCES

HR professionals have less frequent direct involvement in the BIT, but are increasingly being explored as a potential team member given the rise in questionable faculty and staff behavior. A truly safer campus must look beyond at-risk students to include faculty and staff as well. This is a hurdle for most colleges and universities, as the HR department does not always work closely with student affairs.

As an inner circle or core member, HR representatives can offer valuable information on institutional policy and employment law when dealing with a person of concern. It is often the case when the student is the person of concern, but the potential target of the student in question is a faculty or staff member. Other areas of concern are when a student is also an employee, such as a student assistant or resident assistant, or in the rare instance when a faculty member is enrolled in a course and their behavior as a student comes into question. And let us not forget Feb. 12, 2010, when Dr. Amy Bishop shot and killed three colleagues while wounding three others during a faculty meeting at the University of Alabama – Huntsville (Meloy, 2012). HR has employee records that can prove to be extremely valuable when looking at escalating or patterns of reported concerning behavior.

LAW ENFORCEMENT

Law enforcement officers are typically core members, as they are often the first responders to incidents involving violence, potential violence, and threats, and may have valuable relationships with local and state law enforcement. They bring knowledge of incident command and can be useful in reviewing criminal records and concealed carry permits for individuals.

Team members find that their campus police officers are rarely surprised when the name of a person of concern arrives in a report to the Behavioral Intervention Team. They have often already had contact with the individual in question through an incident report.

In addition, their training and experience in subject and witness interviewing provides the team with a wealth of resources and information. The events at Columbine High School in 1999 and the Virginia Tech tragedy in 2007 forced police to tactically change the way they respond to active-shooter situations. As a result, law enforcement personnel today tend to receive training in risk and threat assessment, and look for cooperative ways to deescalate situations before they become deadly (Dowis & Reese, 2015).

DISABILITY SERVICES

The disability services office is often the first responder to escalating behavior when a student known to that department becomes academically frustrated. Many mental health issues and disabilities, such as Tourette's Disorder, Autism Spectrum Disorder, and schizophrenia, can have symptoms that may be viewed by members of the campus community as being threatening. When receiving a report of disability-related behavior, it would be helpful to the BIT to be able to consult with disability services. However, there is no disability accommodation for behavior that violates the student conduct code, is threatening, or is overtly disruptive to the institution. But conferring with disability services on reports of students of concerns allows the BIT to have a greater understanding of why a behavior may be occurring, what intervention technique may be best used, and who might be the appropriate individual to intervene with the student.

Additionally, it's important to understand that when "information from a student's medical or mental health record is shared or used for a purpose other than treatment (e.g., decisions about medical withdrawal or disability accommodations), FERPA applies to the shared records" (The JED Foundation, p. 8).

Teams should be careful about having a representative from the disability services office as a core member, as the message this sends to the community may be that all students referred have some disability or mental illness. This is a concern with counseling as well, but adding disability services as a core member may accentuate that concern. They should have some limited access to the database, however, and the core should always consult to see if a student is registered with the disability services office.

TITLE IX

Unless the person on the team in some other capacity is also the Title IX coordinator or a deputy Title IX coordinator, s/he may be a middle circle member. That said, the coordinator should have access to the chair to put some reported students (and/or faculty/staff) on the BIT radar when necessary. Remember, reporting, being the victim of, and being accused of these types of incidents is traumatizing. The Association of Title IX Administrators (ATIXA) will continue to provide guidance on what and how information should be shared without re-victimizing anyone or having a chilling effect on reporting.

RISK MANAGEMENT/EMERGENCY RESPONSE

A representative from risk management or emergency response may be included on the BIT as a middle or inner circle member when schools are fortunate enough to have an individual dedicated to emergency crisis response and prevention. However, it is

uncommon for universities to have personnel in these roles who are not already tasked with environmental disaster, occupational safety and health administration (OSHA), and often fire response as well.

LEGAL COUNSEL

Members of the legal department are less frequently involved directly on a BIT. Some schools choose to include them with the hope that their early involvement will assist the team in avoiding potential lawsuits. However, having counsel give advice or contribute to the team's decisions is fraught with risk. Diluting attorney-client privilege is one such risk. Additionally, the role of general counsel as the "guardian of the institution's liability concerns" can impede the team's decision-making (Who wants to be the one to disagree with the person charged with defending you in the future lawsuit?).

FACULTY/ACADEMIC TUTORING

Faculty members are commonly involved with the BIT to access information regarding grades and academic performance. They also often serve as the primary contact in working with faculty, department chairs, and provosts. As most institutions are concerned with shared governance, working closely with the faculty senate to select a team member is advisable. The contact could be a dean, department chair, or other academic affairs administrator, who carries enough positional leadership and influence to assist the team with gaining community buy-in for training and reporting. Additionally, it is best if this person has a good understanding and appreciation for student affairs structure and theory.

HEALTH STAFF

These staff members may also be involved on the BIT. This is typically dependent on the relationship with the counseling service. At times, the mental health counselor can represent both interests on the team, but a health center physician or nurse can be a valuable asset to the team as well. Much like the counselor team member, the health center representative may best serve the team by receiving information on students with whom they may already be seeing, and sharing hypotheticals that inform the team. Most often, health center staff members (e.g., nurses, physician's assistants, and doctors) serve as inner or middle circle members.

STUDENT ACTIVITIES

A member of the student activities unit may also be included on the BIT, since this department is often well connected to campus clubs, organizations, and Greek life. While the connection and information s/he brings may be useful, inclusion of someone from this group may raise concerns that a team may be getting too large to quickly

and confidentially address risk. Of course, as mentioned earlier, if a particular unit represents a significant percentage of the campus population, an exception may be worth making. While there may be a particular situation when the team leader would ask that student activities staff members attend a meeting, the dean of students/VPSA should otherwise be able to represent this group.

With all these distinctions between the circles, teams should consider bringing core, inner, and middle (and maybe even some select outer) circle members together once or twice a year to engage in training, do table top exercises, discuss protocols, etc.

FINAL THOUGHTS

The creation of a BIT is often a daunting task for new student affairs professionals to undertake. It is our hope that this whitepaper provides a useful starting place when considering the mission and motivation of the team, and its composition to create a BIT that fits its institution's needs and is aligned with established national trends. While there is no perfect mission statement or exact membership roster that we can offer through NaBITA, we hope this paper provides the insight and guidance needed to determine those answers for your campus.

REFERENCES

Deisinger, G., Randazzo, M., O'Neill, D., and Savage, J. (2008). The Handbook For Campus Threat Assessment and Management Teams. Applied Risk Management, LLC.

Dowis, D. and Reese, A. (2015). Analysis of the Involvement and Contributions of Criminal Justice Programs and Public Safety Departments to Threat and Risk Assessment Teams in Higher Education. Paper presented at the Academy of Criminal Justice Sciences Annual Conference, Orlando, FL.

Dunkle, J. H., Silverstein, Z. B., and Warner S. L. (2008). Managing Violent and Other Troubling Students: The Role of Threat Assessment Teams on Campus. Journal of College and University Law, 34 (3): 585–636.

Eells, G.T. and Rockland-Miller, H.S. (2011). Assessing and Responding to Disturbed and Disturbing Students: Understanding the Role of Administrative Teams in Institutions of Higher Education. Journal of College Student Psychotherapy, 25:8-23.

Meloy, J., Hoffmann, J., Guldimann, A., and James, D. (2011). The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology. Behavioral Sciences and the Law.

Meloy, R. (2012, December). Eight Warning Behaviors of Violence. Paper presented at the 4th Annual NaBITA Conference, Bonita Springs, FL.

Reese, A. (2013). An Evaluation of the Behavioral Intervention Team for a Georgia Regional University. Unpublished doctoral dissertation, Argosy University – Atlanta.

Reese, A. (2014). Coaching for the BIT Chair: Creating an Environment of Clam and Directed Leadership. 6th Annual NaBITA Campus Threat Management Institute, Bonita Spring, FL.

Van Brunt, B., Sokolow, B., Lewis, W., Schuster, S., and Golston, A. (2014). NaBITA Team Survey. *www.nabita.org*.

The Jed Foundation. Student Mental Health and the Law: A Resource for Institutions of Higher Education. New York, NY: The Jed Foundation, 2008.

Warrell, M. (2012). Over-Committed? 3 Questions to Ask Yourself Before Saying Yes. *www.forbes.com/sites/margiewarrell/2012/09/26/over-committed-3-questions-to-ask-yourself-before-saying-yes/*.

ABOUT THE AUTHORS

BRIAN VAN BRUNT, ED.D.

Brian Van Brunt, Ed.D. is the senior executive vice president for professional program development with The NCHERM Group, LLC. He is past-president of the American College Counseling Association (ACCA), the 2015 president of (NaBITA), editor of The Journal of Campus Behavioral Intervention (J-BIT), and managing editor for *Student Affairs eNews (SAeN)*. He has a doctoral degree in counseling supervision and education from the University of Sarasota/Argosy and a master's degree in counseling and psychological services from Salem State University. Van Brunt has served as the director of counseling at New England College and Western Kentucky University. He is the author of several books, including, *Ending Campus Violence: New Approaches in Prevention*, *A Faculty Guide to Addressing Disruptive and Dangerous Behavior*, and *Ending Campus Violence: New Approaches to Prevention*. Van Brunt developed the Structured Interview for Violence Risk Assessment (SIVRA-35), a starting place for law enforcement, clinical staff, and administrators to conduct a more standardized, research-based violence risk assessment with individuals determined to be at an increased risk.

W. SCOTT LEWIS, J.D.

W. Scott Lewis, J.D. is a partner with The NCHERM Group, LLC. He served as the 2013-2014 president of NaBITA, and is a founder and advisory board member of the Association of Title IX Administrators (ATIXA). He is one of the most in-demand higher education risk management consultants in the country. Previously, he served as special advisor to Saint Mary's College in South Bend, Ind., and as assistant vice provost at the University of South Carolina, where he was also on faculty. Lewis' faculty work includes courses in education, law, political science, and business. He brings more than 20 years of experience as a student affairs administrator, faculty member, and consultant in higher education. He is a frequent keynote and plenary speaker, nationally recognized for his work on Behavioral Intervention/Threat Assessment Teams for students in crisis and distress, Title VII, and Title IX issues. He is also noted for his work in the area of classroom management and dealing with disruptive students (and parents), and has trained thousands of faculty and staff members. He presents regularly throughout the country, assisting colleges and universities with legal, judicial, and risk management issues, as well as policy development and implementation. He serves as an author and editor in a number of areas, including legal issues in higher education, campus safety and student development, campus conduct board training, and other higher education issues.

AARON "CHIP" REESE, ED.D.

Aaron "Chip" Reese, Ed.D. is the president-elect of NaBITA and an Advisory Board member. He is a past-chair of the University System of Georgia, Regents Advisory Committee for Student Conduct Officers, and a founding member of the Georgia College Suicide Prevention Coalition. He also serves on the editorial board for *The Journal of Campus Behavioral Intervention (J-BIT)*, and as a faculty member with the NaBITA Campus Threat Management Institute. Chip earned a doctorate degree in educational leadership from Argosy University/Atlanta and a M.Ed. in administration and supervision from Clemson University. He spent nearly 20 years as a college baseball coach before moving into higher education administration as dean of students. Currently, Reese is the assistant vice president for student affairs and dean of students at Columbus State University, and serves on the graduate faculty teaching in the Doctorate in Curriculum and Leadership program. He is the chair of the university's Behavioral Intervention Team and consults with other college and university BITs around the country. Chip has developed an operations manual for BITs and the Actionable Case Workflow Cart, which serve to assist BITs in developing, managing, and implementing their team policies and practices.

About NaBITA

The vision of the National Behavioral Intervention Team Association (NaBITA) is to make our campuses and workplaces safer environments where development, education, and caring intervention are fostered and encouraged. NaBITA brings together professionals from multiple disciplines who are engaged in the essential function of behavioral intervention in schools, on college campuses, and in corporations and organizations for mutual support and shared learning. Whether it is to combat bullying, prevent violence, support individuals with disabilities, empower the success of those suffering from mental health challenges, or assist those who are in crisis, our members are joined in common purpose and exploration of best practices.

NaBITA.org
the National Behavioral Intervention Team Association

The NCHERM Group, LLC
Systems-level solutions for safer schools and campuses

IMPLEMENTING BEHAVIORAL THREAT ASSESSMENT ON CAMPUS: A VIRGINIA TECH DEMONSTRATION PROJECT

Implementing Behavioral Threat Assessment on Campus

A Virginia Tech Demonstration Project

Marisa R. Randazzo, Ph.D.
Ellen Plummer, Ph.D.

VirginiaTech
Invent the Future

IMPLEMENTING BEHAVIORAL THREAT ASSESSMENT ON CAMPUS

A Virginia Tech Demonstration Project

Marisa R. Randazzo, Ph.D.
Ellen Plummer, Ph.D.

November 2009

VirginiaTech
Invent the Future

Table of Contents

We dedicate this book to those who lost their lives in the shootings at Virginia Tech on April 16, 2007; to those who were physically injured on that day; to those who suffered psychological trauma and injury as a result of the shootings; and to their families and loved ones.

Foreword

The April 16, 2007, tragedy at Virginia Tech resulted in unprecedented new attention and new practices related to campus safety and security at higher education institutions. At Virginia Tech we have been working on multiple fronts to learn everything we can from the tragedy. Our efforts have been greatly helped through collaborations with experts from around the country who stepped forward to provide advice and assistance. One of our earliest partners was and continues to be the United States Department of Education, Office of Safe and Drug-Free Schools.

With the support of a grant from the U.S. Department of Education, we have developed and implemented several new models for enhancing safety and overall well-being, both for individuals at risk and for the community as a whole. This book provides a detailed summary of two of the major projects we have implemented: (1) comprehensive threat assessment and (2) case management. The case management program represents the provision of supportive services for students and employees and provides systematic follow-up monitoring of individuals who have received treatment. Case managers attend hearings associated with mental health assessments and maintain appropriate communications with relevant parties. Threat assessment is managed by a multi-disciplinary team of administrators, representing the interests of faculty, students, and staff and chaired by the chief of police. The goal of the team is to assess risks as early as possible and minimize the occurrence of emergency situations. The team has the expertise and the authority to intervene when appropriate. The projects supported by the Department of Education have been supplemented and complemented by programs focused on direct support of all victims of the April 16 tragedy. University funds and a major grant from the U.S. Department of Justice, Office for Victims of Crime enabled us to expand counseling services and to develop support programs for the families of April 16 victims, injured students, and members of the university community who were affected by the events.

We hope that the models described here will be helpful to other institutions as they continue to develop their policies and programs.

We continue to assess our efforts and look forward to ongoing national discussions about the best practices to improve safety and security at our universities and colleges. At Virginia Tech we did not plan to become leaders in this area, but we accept the challenge and the opportunity to share our experiences with others.

Mark McNamee
Senior Vice President and Provost
Virginia Polytechnic Institute and State University
Principal Investigator, *Assessing and Responding to At-risk Behaviors in a Higher Education Setting: Virginia Tech Demonstration Project*

November 2009

About the Authors

Marisa R. Randazzo, Ph.D., is a national expert on threat assessment and targeted violence. Formerly the chief research psychologist for the U.S. Secret Service, Dr. Randazzo has provided threat assessment training to more than 10,000 professionals in higher education, secondary schools, corporations, law enforcement agencies, human resources, mental health, and the intelligence community throughout the United States, Canada, and the European Union. In her 10 years with the Secret Service, she supervised the agency's research on presidential threats, insider threats, school shootings, security breaches, and stalking incidents. She also served as co-director of the Safe School Initiative, the largest federal study of school shootings in the United States, and is co-author of the U.S. Secret Service/U.S. Department of Education model of threat assessment for educational institutions. Dr. Randazzo now heads Threat Assessment Resources International, LLC, providing threat assessment training and case consultation to colleges, schools, corporations, and security professionals. She has testified before Congress; briefed Cabinet Secretaries; and been interviewed by numerous major television, radio, and print news outlets about threat assessment and targeted violence prevention. In 2005, Dr. Randazzo was awarded the Williams College Bicentennial Medal for her work in preventing violence. Most recently, she co-authored *The Handbook for Campus Threat Assessment and Management Teams* (Stoneham, Mass.: Applied Risk Management). Dr. Randazzo earned her B.A. from Williams College and her M.A. and Ph.D. in social psychology from Princeton University. Contact: *775/741-3314 or MRR@ThreatResources.com.*

Ellen Plummer, Ph.D., is assistant provost at Virginia Tech, where she has served as the project director on several federally funded projects designed to assist with the recovery efforts from the shootings that occurred at Virginia Tech in April 2007. In addition to serving as the project director on the Virginia Tech Demonstration Project described in this publication, Dr. Plummer assisted in providing leadership to various aspects of Virginia Tech's response and recovery efforts in the immediate and mid-term responses to the shootings. Prior to her work on these recovery efforts, Dr. Plummer served as special assistant to the provost on university-wide planning efforts and was the direc-

tor of the Women's Center, where she supervised the development of university-wide efforts designed to respond to, prevent, and raise awareness of violence against women. Before joining the Virginia Tech administration, Dr. Plummer worked at Duke University, where she provided support services to survivors of violence and served in several administrative posts. In North Carolina, she also worked with nonprofits, state agencies, and victim rights coalitions on passage of victim rights legislation aimed at supporting victims of rape, sexual assault, and domestic violence. Dr. Plummer teaches in Virginia Tech's higher education program and provides administrative support to university governance and other activities associated with the Office of the Provost. She holds a B.S. degree in human development and family relations and an M.S.W. degree, both from the University of Connecticut. She also holds a doctorate in educational leadership and policy studies from Virginia Tech. Contact: 540/231-6612 or *eplummer@vt.edu.*

Acknowledgments

The authors would like to thank several people, without whom this book would not have been possible. At Virginia Tech, we are grateful for the assistance of Dr. Charles Steger, Dr. Mark McNamee, Dr. Gene Deisinger, Ms. Linda Woodard, Ms. Emily Reineke, Ms. Clara B. Cox, and Ms. Valerie Anderson.

In our personal lives, we are grateful for the tremendous support and encouragement we received from our loved ones—Robert S. Randazzo and Liz Scharman—and in particular for their patience with us in the face of aggressive deadlines and general project stress. There is no question that we could not have written this book without them.

The demonstration project highlighted in this book would not have succeeded without the dedication of all of the individuals at Virginia Tech who committed themselves to thinking creatively and demanding of themselves and each other the highest level of professionalism. To them we extend our gratitude for their efforts and for sharing their experiences with us for this book.

A very special acknowledgment goes to Associate Assistant Deputy Secretary William Modzeleski of the U.S. Department of Education. We have each had separate opportunities to work with Bill—and even more importantly, to learn from Bill—over the course of our careers. His longstanding commitment to preventing violence and making schools safe led him to reach out to Virginia Tech and make this project possible. We are profoundly grateful for having had the opportunity to work together with Bill on this important project.

Marisa R. Randazzo
Ellen Plummer
Blacksburg, Va.
November 2009

Introduction

Founded in 1872, Virginia Polytechnic Institute and State University (Virginia Tech) is a public land-grant institution located in Southwest Virginia. The university serves the Commonwealth of Virginia, the nation, and the world through its tripartite mission of learning, discovery, and engagement. Virginia Tech is best known for its academic strengths in engineering, architecture, and agriculture but provides educational and research excellence throughout its comprehensive array of programs.

The Virginia Tech shootings occurred on April 16, 2007, a cold and windy Monday. As the end of the semester approached, students and members of the staff and faculty were focused on completing the academic calendar and looking forward to warmer weather. By mid-morning, Virginia Tech had become the site of an unprecedented mass homicide. A student shot and killed 27 students and five faculty members and wounded many more before killing himself. The details of these shootings are beyond the scope of this book but can be found in various public source documents and media accounts.[1]

In the weeks and months following the shootings, several extensive reviews and after-action analyses were conducted by Virginia Tech and others to better understand the attack and to try to prevent similar attacks at any institutions of higher education (IHEs). Just as the Columbine High School attack in 1999 served to galvanize efforts toward understanding and preventing K-12 school shootings, so, too, has the 2007 attack at Virginia Tech served to galvanize campus safety efforts and to focus the nation's attention on the issue of preventing campus shootings. In the months following the Virginia Tech shootings, there was much discussion about the threat assessment model developed to prevent K-12 school shootings and its potential utility for higher education settings. Nearly all of the major reports on campus safety issued after the shootings at Virginia Tech advocated for colleges and universities to adapt a version of the K-12 school threat assessment model and

---

1   See, for example, Virginia Tech Review Panel report to the governor (August 2007) for a timeline and analysis of the shootings and other aspects of the incident. The full citation appears in Appendix D.

to develop and train campus threat assessment teams[2] as a key tool in the fight to prevent attacks at IHEs.

The K-12 School Threat Assessment Model

The K-12 school threat assessment model was developed by the U.S. Secret Service and U.S. Department of Education following their research on K-12 school shootings, research that had been prompted by the attack at Columbine High School. Their joint study, known as the *Safe School Initiative (SSI)*, revealed important findings that included the possibility for preventing these mass tragedies. It found that school attacks were typically planned in advance and that the vast majority of school shooters had caused serious concern among friends, associates, family members, and teachers before carrying out their attacks. They also discovered that most school shooters were suicidal prior to their attacks. Some had tried to commit suicide earlier but had failed; others hoped to be killed by law enforcement officers during their attacks; and others were at a point of such desperation that they did not care what happened to them anymore, including incarceration or death.[3]

In dissecting school attacks that have occurred throughout the United States, the SSI found that school shooters often embark on what researchers call a "pathway to violence"—that is, the shooters first came up with an *idea* to do harm to others, to themselves, or both; then developed a *plan* to carry out their idea; then acquired or secured the *means* to do harm (typically using guns and ammunition, with some school shooters also using knives, pipe bombs, and other destructive means); and finally *implemented* the attack. The key to preventing school shootings, the researchers argued, is to determine whether a student is on a pathway toward violence and, if so, to figure out where

---

2   Throughout this book, we use the terms "behavioral threat assessment," "threat assessment," and "campus threat assessment" interchangeably.

3   Vossekuil, B. Fein, R., Reddy, M., Borum, R., & Modzeleski, W. (2002). *The final report and findings of the Safe School Initiative: Implications for the prevention of school attacks in the United States.* Washington, D.C.: U.S. Department of Education and U.S. Secret Service.

he[4] is on that path (e.g., he has only developed an idea with no further progression, or he has a detailed plan and has prepared his guns and ammunition).

From these and other findings, experts from the U.S. Secret Service and U.S. Department of Education developed the K-12 school threat assessment model, a model for how to prevent school shootings by learning about a student when he engages in troubling behavior and then gathering more information to determine whether the student is on a pathway toward violence or self-harm.[5] If the threat assessment team, as the group that gathers and evaluates this information is typically called, believes that the student does pose a threat of harm to himself or to others, the team then develops and implements a plan or strategy to connect the student with resources and assistance that can reduce the threat. Many professionals who work in the field of threat assessment have seen firsthand how the diligent work of school threat assessment teams has prevented school attacks. It is a model that works.

Book Overview

This book documents Virginia Tech's experience in developing and implementing a behavioral threat assessment process in the time following the campus shootings on April 16, 2007. Starting a campus behavioral threat assessment process included creating a multi-disciplinary threat assessment team; strengthening and developing necessary policies and procedures to enhance and support the team's efforts; training the team; identifying and harnessing key resources on and off campus to intervene where necessary; securing case management personnel to implement and monitor intervention efforts; and rais-

---

4   For the purposes of this book, the authors have chosen to use the male pronoun in referring to past school shooters. It is important to note that both genders—male and female—have engaged in school shootings or have plotted school attacks that were thwarted before the implementation phase. But because more boys and men typically engage in targeted attacks or plots than do girls or women, the authors use male pronouns to describe those known to have attacked or plotted attacks.

5   Fein, R., Vossekuil, B., Pollack, W., Borum, R., Modzeleski, W., & Reddy, M. (2002). *Threat assessment in schools: A guide to managing threatening situations and creating safe school climates.* Washington, D.C.: U.S. Department of Education and U.S. Secret Service.

ing awareness on campus regarding the team's existence, its purpose, and the role that everyone on campus shares in reporting troubling behavior to the team.

The information herein was compiled primarily through interviews with Virginia Tech leaders and with individuals appointed as Threat Assessment Team members. It was also derived from threat assessment records and observations of meetings of the Virginia Tech Threat Assessment Team and also the university's Care Team. Finally, some information came from public sources, such as the Virginia Governor's Review Panel, which conducted an extensive analysis of the April 16, 2007, shootings. Where information was derived from publicly available sources, those sources are cited in footnotes and listed in the resource section in Appendix D. The list of those interviewed appears in Appendix C.

The book is organized into chapters that document distinct aspects of Virginia Tech's experience in building a threat assessment capacity on campus. Chapter One outlines the genesis of the demonstration project and details its various aspects. Chapter Two summarizes discussions and critical decision points related to establishing a threat assessment capacity at Virginia Tech. Chapter Three highlights the work done to support and enhance the Threat Assessment Team's efforts. Chapter Four addresses the implementation and development of case management functions related to reducing threats and connecting persons in crisis with necessary resources. Chapter Five discusses the concerns unique to implementing threat assessment on a post-incident campus. And Chapter Six summarizes pitfalls to avoid and highlights ongoing challenges for the Virginia Tech Threat Assessment Team that might affect other campus threat assessment teams. Throughout the chapters, we discuss challenges that Virginia Tech encountered in developing its threat assessment process, highlight key decision points for the university and its Threat Assessment Team, and describe workable solutions developed by the university.

In the course of building its behavioral threat assessment capacity, Virginia Tech created considerable documentation to support its Threat Assessment Team and related efforts. This documentation, which ap-

pears in Appendices B and E, includes an array of institutional policies, the team's mission statement, information distributed university-wide to announce and promote the Threat Assessment Team, wallet reference cards, position descriptions, and other materials. This information is included herein to provide examples to any institution that is developing a behavioral threat assessment capacity or enhancing an existing threat assessment process. It is important to note that every institution is different and that the examples provided here may not be appropriate for a particular institution to use. But these resources can still serve as a starting point for institutions to consider in crafting their own policies, mission statement, public awareness message, and other relevant materials. Additional resources, which are listed at the end of this book, provide general templates for use in the creation of threat assessment processes.

CHAPTER ONE

Background and Project Origination

Background and Project Origination

In the immediate aftermath of the April 16 shootings, a number of key individuals reached out to Virginia Tech and offered assistance that became crucial to the immediate-, medium-, and longer-term recovery of the victims and survivors as well as the entire university community.[6] To help the university facilitate prevention efforts as well, then–U.S. Secretary of Education Margaret Spellings contacted Virginia Tech President Charles Steger and offered the financial resources and expertise of the U.S. Department of Education's Office for Safe and Drug-Free Schools (OSDFS). Secretary Spellings and the OSDFS could see benefits, for Virginia Tech as well as for higher education institutions in general, in partnering to learn how to identify and intervene with at-risk behaviors in a complex higher education setting.

Origination of the Virginia Tech Demonstration Project

To launch this effort, a group of university administrators and faculty members came together within the first few weeks after the shootings to design what would become the Virginia Tech Demonstration Project. Several of these individuals had previously worked with the Office of Safe and Drug-Free Schools on projects related to school safety. These individuals were already familiar with the K-12 threat assessment model and with the positive impact that mental health and support services can have when intervening with at-risk behavior. Through the demonstration project, this group sought to build a capacity for Virginia Tech to be able to assess threats; to establish cross-functional processes to enhance opportunities for early detection of and intervention with at-risk behavior on campus; and to identify or create services to reduce at-risk behavior, whether the risk was for harm to others, harm to self, or both.

In addition to discussions precipitated by state and university reviews of the shootings, the university community learned from resources introduced by the Office for Safe and Drug-Free Schools. These external resources included research data, materials, and individuals with

---

6   To help the university with victim recovery, the U.S. Department of Justice, Office for Victims of Crime, provided Virginia Tech with a grant to fund assistance and recovery resources for victims of the shootings.

committees: (1) the Threat Assessment Team, (2) the Campus and Workplace Violence Prevention Committee, (3) the Health and Safety Committee, and (4) the Emergency Management and Risk Assessment Committee.[7] Each committee is chaired by a person with professional knowledge of and responsibility for the areas addressed by the committee. The Threat Assessment Team is chaired by the chief of police, the Campus and Workplace Violence Prevention Committee is chaired by the chief of police or his designee, the Health and Safety Committee is chaired by the director of environmental health and safety, and the Emergency Management and Risk Assessment Committee is chaired by the director of emergency management. The safety and security structure itself includes elements that existed before the shootings and incorporates new elements aligned with recently enacted state laws and revised university policies and practices. As a university-wide function, threat assessment and the policies and committee structures that support it have evolved since the team was first established in December 2007. In Virginia, state legislation passed in 2008 mandates threat assessment teams and campus and workplace violence prevention committees.

The committee structure established by the university to support safety and security was designed to strengthen the efforts of each committee by establishing formal lines of communication and a visible connection between all safety and security efforts across the institution. The Threat Assessment Team was established in advance of state law and before the university's safety and security committee structure was determined. However, embedding threat assessment and violence prevention efforts in a broad institutional context increases opportunities for raising awareness, strengthens collaborations across safety and security functions, and provides institution-wide infrastructure for assessing threats and preventing violence. A grant from the U.S. Department of Education allowed Virginia Tech to strengthen these existing structures and policies and to launch case management functions for students and employees as a new and integral component of violence prevention. The grant also provided resources for Virginia Tech's newly

7   Please see Appendix B for a diagram of these Virginia Tech committees and the reporting structure among them.

established credentials and experience in school safety. In July 2007, while the university was finalizing the elements of the demonstration project, the OSDFS hosted a forum at Virginia Tech that brought together state and national experts who presented information and led discussions about the prevention of and response to violent behaviors in a higher education setting. This forum, in combination with the discussions occurring on and off campus, provided additional support, expertise, momentum, and guidance for the formation of the elements in the university's demonstration project.

Existing Violence Prevention and Assistance Resources on Campus
It is important to note that, like most institutions, the university was engaged in safety and security efforts before the shootings occurred. As external and internal post-incident reviews noted, the university had policies, procedures, and programs in place for students and employees. For example, at the time of the shootings, the university already had a Care Team, which was formed to assist students in crisis, as well as on- and off-campus mental health referral processes for students and employees; a campus and workplace violence prevention policy; policies addressing the conduct of students and employees; and safety and security outreach and education efforts conducted by various university departments, including the police department.

Also prior to the shootings, the university had identified as a priority the integration of all-hazards emergency planning and response. To support these planning and response efforts and to best support its new threat assessment and case management functions, university leaders designed an over-arching committee structure within which threat assessment and violence prevention are elements.

The Virginia Tech safety and security committee structure was designed and established with the knowledge that violence prevention and threat assessment functions are best actualized in concert with other risk-assessment and safety and security efforts. The university recognized the value of having executive leaders engaged in the oversight of safety and security matters and, thus, established a University Safety and Security Policy Committee that is responsible to and chaired by the university president. Reporting to the committee are four sub-

established Threat Assessment Team and ensured that the team received training, materials, and support to advance its charge.

Key Elements of the Demonstration Project

Several assumptions guided the final articulation of the demonstration project. First, the guidelines for the grant proposal clearly indicated a priority placed on the creation and institutionalization of processes that support the early identification of individuals who might pose a threat. Second, it was important that elements of the project be institutionalized over the course of the grant period, which required the team to identify key elements (such as case management) and secure the commitment of executive leaders to the on-going financial and organizational support for those key elements. Third, because efforts associated with the demonstration project required executive-level support, the senior vice president and provost agreed to serve as principal investigator on the demonstration project. Fourth, the grant would only succeed using a multi-disciplinary approach. Consequently, the demonstration project included several multi-disciplinary teams to provide leadership and guidance to elements within the demonstration project itself. Fifth, Virginia Tech was committed to participating in discussions about safety and security but did not want to present itself as expert on these matters. Rather, the university saw itself (and continues to do so) as the beneficiary of support offered to advance safety and security and is therefore committed to sharing what it has learned and to continue to improve and learn through collaborations with colleagues across the country and around the world.

The final demonstration project design consisted of four elements: (1) a mental health assessment consisting of a survey of students and employees regarding post-trauma symptoms, (2) the creation of a multi-disciplinary threat assessment task force, (3) the creation of case management functions for employees and students, and (4) the dissemination of demonstration project results.

Assessment of Mental Health Needs. The first element—the mental health assessment—consisted of helping to fund a project designed to assess the post-trauma reactions of university employees and students using a survey conducted by researchers interested in establishing

benchmarks for mental health needs following large-scale traumatic events. The research consisted of disseminating surveys to students and employees in early fall 2007, a process that was repeated in summer 2008 (see M.H. Hughes *et al.* reference in Appendix D). Faculty members and campus mental health service providers will be using the data gathered to guide focused interventions and to assist in determining what wellness and mental health interventions might be needed in the longer-term aftermath of the shootings.

Creation of Threat Assessment Capacity. The second element of the demonstration project involved establishing a multi-disciplinary team that would identify and evaluate the violence potential of individuals of concern. The university formally established the Threat Assessment Team in December 2007.[8] The grant proposal anticipated creation of this multi-disciplinary, institution-wide body and provided funds to secure training for its members and for staffing the team. The Threat Assessment Team was created under the direction of the president, with the chief of police as its chair. The team began its work immediately, followed by creating policies and procedures as well as adjusting related university functions. The continuing evolution of supporting policies and functions remains a high priority for the university.

Creation of Case Management Functions. Third, the demonstration project established three full-time case manager positions. Case management proved to be a key ingredient in the success of the project. The grant provided funds to hire two case managers in the Division of Student Affairs and one case manager in the Department of Human Resources. Each manager served a different purpose, but all were assigned responsibilities for serving as links between individuals, services, and processes. By serving as liaisons between individuals and services, by providing support and guidance, and through brokering services, case managers connect individuals with varied units within the university and make referrals, as needed, for behaviors of concern. Case management positions did not exist at the university before the implementation of the demonstration project but now provide important functions in the overall goal of violence prevention.

---

8 See Appendix B for a copy of the Presidential Memorandum that created Virginia Tech's Threat Assessment Team and named its initial members.

Dissemination of Demonstration Project Results. The fourth and final element of the demonstration project outlined the university's interest in participating in national discussions about violence prevention by sharing information about the implementation of the demonstration project. Virginia Tech remains committed to sharing the experiences and lessons it learned from the tragedy. Thus, a goal of the demonstration project has been to collect information and disseminate the ideas, programs, services, challenges, and successes in implementing efforts designed to prevent violence.

Summary

The Virginia Tech Demonstration Project propelled the work of the Threat Assessment Team as part of efforts with institutional impact. Establishing and launching the institution's threat assessment capabilities are covered in depth in the following chapter. University leaders discussed various approaches to establishing a team and made several key decisions that guide Virginia Tech's threat assessment processes.

Critical First Steps in Creating Virginia Tech's Threat Assessment Capacity

Critical First Steps in Creating Virginia Tech's Threat Assessment Capacity

The reports issued by Virginia Tech and by the Virginia Governor's Review Panel on the Virginia Tech tragedy recommended that the university develop and implement a behavioral threat assessment process to prevent campus violence as well as to address threats and other troubling behavior that may arise from students, faculty, staff, or visitors. But even before these reports were published, Virginia Tech President Charles Steger decided that Virginia Tech should develop a threat assessment team. Using the grant that the university had received from the U.S. Department of Education, Office of Safe and Drug-Free Schools to identify and address at-risk behaviors on campus following the shootings, Virginia Tech embarked on a process of creating, training, and implementing a campus threat assessment process.

Envisioning the Process

Before Virginia Tech's president announced the creation of the university's Threat Assessment Team, various university leaders devoted some time to envisioning how they wanted the threat assessment process to work and how they wanted the Threat Assessment Team to interact on campus. Of particular concern was the fact that the university already had a Care Team in place to assist students in crisis and to address student behaviors of concern. The president and other leaders had to determine if they wanted to keep the Care Team or merge it into the new Threat Assessment Team. They also had to decide how they wanted the Threat Assessment Team and Care Team to interact should they decide to keep the Care Team intact. Other key questions included whether one unified threat assessment team should handle all cases involving students, faculty, and staff or if separate teams, one to address student behavior of concern and another to address employee (i.e., faculty and staff) behavior of concern, would be preferable. A dimension of the conversation included how to best respond to concerning behaviors demonstrated by visitors or individuals not associated with the university but about whom there might be a concern (for example, the spouse of an employee). The final key question that university leaders anticipated might spark debate involved the membership of the Threat Assessment Team. Although certain positions

were required by Virginia law, others would be determined by the university president.

Campus leaders credit this exercise of envisioning the Threat Assessment Team and process before beginning to build the team with helping the university to anticipate and prepare for questions and concerns that did eventually arise in building the threat assessment process. Even so, there was considerable debate among leaders over these issues. According to everyone who was involved in the demonstration project and other key university leaders, no one resisted or opposed the president's idea to create a threat assessment capacity. However, considerable debate was generated about whether Virginia Tech should have one threat assessment team that would handle all cases regarding at-risk behavior—whether in students, faculty, or staff—or should have two teams, one to handle

Critical Question: Should an institution establish separate threat assessment teams for student cases and for faculty/staff cases—or one threat assessment team to handle all cases?

University Decision: Virginia Tech opted to establish one team to handle all cases, whether they involve students, faculty, staff, or visitors.

student cases and another to handle employee cases. The "one team or two" issue, as many characterized it, was for some the most critical decision to be made about the university's developing threat assessment process. Debate over this issue appears to have followed similar lines in discussions that occurred in the years prior to the shootings when the university implemented its Campus and Workplace Violence Prevention Policy. Debate over creation of that policy involved some on campus arguing for separate violence prevention policies for student conduct and employee conduct, whereas others argued for a unified policy. Ultimately, Virginia Tech opted for one unified campus and workplace violence prevention policy.

The debate over the issue of one threat assessment team or two was intense at times. Those who advocated for separate teams wanted to focus their resources and efforts on student care and intervention, arguing that students would constitute the majority of cases a unified team would handle. Those advocating for a unified team agreed that the team would likely handle mostly student cases but felt that it was important to have only one team so that those handling faculty and staff cases would get the same amount of experience as their student-focused colleagues by participating on all cases. Those advocating for a unified team also argued that disruptive or troubling behavior could have a ripple effect across campus, regardless of whether it comes from a student, faculty member, or staff member. They believed it was important that there be one team with one philosophy, one focus, and one level of experience. Finally, those advocating for a unified team expressed concern that establishing separate teams could create yet another campus "silo" that could inadvertently block information-sharing between teams.

Ultimately, it fell to President Steger to determine whether Virginia Tech should have one threat assessment team or two, and he decided on one unified threat assessment team. It was clear from the people interviewed that once the president made his decision, those involved in the debate supported it. This support can be attributed to the fact that there was never disagreement over *whether* Virginia Tech should establish a threat assessment capacity, just debate over *how* to do it.

Team members and university leaders interviewed for this project have said that in retrospect, having one team seems to have served Virginia Tech well. Team members have noted that because so many students hold part-time jobs on campus, the representative from Human Resources has been involved in far more student cases than they expected she would be. Had there been separate teams, the Human Resources perspective on student cases may not have been as apparent or logistically could have been more difficult to access. Team members have also noted that working together on one team seems to have enhanced appreciation among team members for each other's perspectives and experiences and has helped to minimize misunderstandings or misperceptions through regular discussion and group decision-making.

Determining Team Membership

The next decision involved who should serve on the team. Similar to the president's executive decision in creating the team and in deciding there should only be one team, the president selected the first team members. Within the Commonwealth of Virginia, laws passed by the Virginia legislature in 2008 (Section 23.9.2 of the Code of Virginia) mandate that all public institutions of higher education have threat assessment teams and specify that certain offices be represented on those teams. Thus, within Virginia at least, questions about which offices would be included on the threat assessment team were answered in the legislation. Consistent with the Code of Virginia, members initially appointed to the Virginia Tech Threat Assessment Team represent the following offices and entities:

» Chief of police

» Dean of students

» Student Affairs representatives (2)

» Academic Affairs representative

» Legal counsel

» Human Resources representative

» Clinical psychologist representative

Even with state law requiring that certain offices or institutional functions be represented on the team, there was considerable debate among Virginia Tech's senior leadership regarding who should represent those offices and who else should serve on the new team. For example, an important resource for the team has been involving the university registrar, and the team has benefited from her ability to provide information, when appropriate, about a student's academic progress. In addition, the registrar's access to student records and knowledge of the laws and regulations associated with confidentiality have been invaluable.

Additional debate centered on whether to include someone on the team who could speak to faculty issues in cases involving threatening or troubling faculty behavior. When it came to team members who could speak to student issues or to staff issues, it was relatively clear which office or personnel should be included. Because several offices

are involved in addressing faculty issues, it was less clear who—if anyone—should be included to speak to faculty issues in cases involving behavior of concern from faculty members. The university president opted for a combination of existing team members: the representative from Human Resources, who was already on the team to speak to staff issues, and the vice president for Academic Affairs, who was already on the team to answer questions about academic issues of students who were reported to the Threat Assessment Team.

One challenge that Virginia Tech faced was ensuring that the right people were on the team and not just having the right offices represented. Those interviewed said that it is critical that team members be able to work together; thus, the personalities of team members matter nearly as much as the areas/departments on campus that they represent. University leaders emphasized that individuals chosen to represent certain offices did not necessarily have to be the highest ranking person within their respective offices if someone else within the office was better suited in terms of his or her personality to sit on the team. In addition, some university leaders expressed concern about the possible difficulty of having personnel serve on the team alongside their supervisors. Several among the leaders argued against having supervisors and their subordinates on the same team to ensure that concerns raised and opinions voiced would never be hindered by workplace hierarchy. That said, university leaders emphasized the importance of team members keeping their supervisors informed about situations that might require their supervisors to act. Such situations could be handled between individual supervisors and their subordinates or as a matter of team procedures.

University leaders have cautioned that an institution can err by having too many members on the threat assessment team, which can reduce its responsiveness as well as make the task of scheduling meetings unnecessarily difficult.

Virginia Tech's president has advocated that selecting members for the team should be a presidential prerogative for any institution that is setting up a team. But in practice, he made decisions regarding team membership in close consultation with the team's chair and with input from university leaders to ensure that their perspectives were included.

Selecting a Team Leader

With respect to appointing a team chair, Virginia Tech opted to go with the chief of the Virginia Tech Police Department. Other university leaders agreed that it was critical that the police department serve as a key player on the threat assessment team and preferably as the team leader.

One challenge the university had not anticipated, however, was the significant amount of time that would be required of its Threat Assessment Team members, even in the early days of the team's existence. Some of those interviewed wondered whether, in hindsight, it was ask-

Implementation Challenge: Institutions may find it difficult to gauge how much time working on the threat assessment team will demand of its members and especially its chair.

University Solution: Virginia Tech helped mitigate the time demands on the team chair by adding administrative and operational support positions to the team.

ing too much of the chief of police to have him chair the team when doing so took so much time. However, there has been unanimity that the police chief was the best person to lead the team in its initial stages for several reasons. First, his position crosses campus constituencies. That is, he does not come from a faculty, staff, or student perspective; rather, his perspective is campus-wide. Second, he has the

rank and stature necessary to make command decisions about cases when necessary and to gain the attention of the university president and other leaders without having to work through layers of hierarchy. Third, he is widely liked and respected on campus (and by team members), lending immediate credibility to the new Threat Assessment Team's efforts. So although naming him to the position of team chair has demanded a tremendous amount of time above and beyond his position as police chief, all who were interviewed agreed that having him serve as the first chair was critical to the team's early success.

Since naming the police chief as chair, Virginia Tech has taken two steps to manage the demands on his time: (1) the university approved

adding a full-time team coordinator position, a position filled by a former Virginia Tech graduate student who was involved in setting up the team and thus was familiar with its work, and (2) the university hired an experienced threat assessment professional from outside the university to fill the position of university threat manager and deputy chief of police and to run the team's day-to-day operations. The Virginia Tech chief of police continues as chair of the Threat Assessment Team but now has considerable operational and administrative support.

Handling Issues of Confidentiality

Team members and university leaders alike addressed the importance and challenge of defining confidentiality early in the process of building their threat assessment capacity. Among those interviewed, individuals who had worked at institutions other than Virginia Tech noted that different institutions have different professional philosophies and practical strategies with respect to confidentiality of information and that these philosophies and practical strategies may have a broader reach than what specific confidentiality laws (federal and state) dictate. Several team members spoke about the importance of examining an institution's particular philosophy on confidentiality before thinking through issues, such as the level of detail of records kept on cases that a threat assessment team would handle, and determining how to store the case records. In the U.S., for example, records created by an institution's law enforcement unit (e.g., its police department or campus security unit) and maintained for law enforcement purposes are not considered to be subject to the Family Educational Rights and Privacy Act (FERPA) provisions that generally protect the privacy of student educational records but also allow students access to their own records for review if requested.[9]

9   See, e.g., Deisinger, G., Randazzo, M., O'Neill, D., & Savage, J. (2008). *The Handbook for Campus Threat Assessment and Management Teams.* Stoneham, Mass.: Applied Risk Management; and, Dunkle, J., Silverstein, Z., & Warner, S. (2008). See also Dunkle, J., Silverstein, Z., & Warner, S. (2008). "Managing violent and other troubling students: The role of threat assessment on campus." *Journal of College and University Law,* 34(3), 585-636, for more detailed discussions regarding U.S. laws that may impact information sharing in campus threat assessment.

Case Documentation and Record-Keeping

Virginia Tech's Threat Assessment Team developed a multi-layered system of documentation for its case records. Each case brought before the team is documented in the official minutes of the meeting where it is discussed. The case is also added to a master spreadsheet, and a record of the case is created in the police records management system of the Virginia Tech Police Department.

For each meeting, the team coordinator types the minutes of the meeting, creating an official meeting record. For each case discussed at the meeting, the minutes include information known at the time about the situation, the team's assessment of the situation, and the plan for managing it. After the minutes are reviewed and approved by the team, a hard copy is placed in a file that includes each case that is discussed. This hard copy file contains all information known about a situation/subject and is kept in the chief of police's office.

The details of each situation discussed by the team are entered into a searchable database that includes the subject's university ID number; whether the subject is currently enrolled or employed at Virginia Tech; his or her Virginia Tech affiliation; how he or she was brought to the attention of the team; the name, if applicable, of the target of the threats or concerning behaviors; any holds or restrictions placed on his or her university accounts; and the dates that the case was discussed by the team. This database is searched any time a new case comes to the team's attention to see if the person of concern has been discussed by the team previously and, if so, to access the previous case record.

Cases reviewed by the Threat Assessment Team and investigated by the Virginia Tech Police Department are recorded in the police records system. These cases are marked confidential and are available for review only by select members of the police department.

Securing Basic and Advanced Threat Assessment Team Training

All who were involved in the demonstration project emphasized the importance of securing professional training for Virginia Tech's new Threat Assessment Team by individuals with demonstrated experience in assessing threats. Since its inception, the team has gone through multiple basic and advanced threat assessment training classes, con-

ducted by three of the nation's top campus threat assessment experts. Advanced threat assessment training included tabletop exercises where the team worked through case scenarios in the same manner that they would an actual case. In addition, various team members attended statewide and regional training conferences on behavioral threat assessment and case management. Training included strategies for balancing the demands of threat assessment work with personal life concerns and for watching out for fellow team members in efforts to maintain healthy quality of life while participating on a threat assessment team.

Summary

The launching of Virginia Tech's Threat Assessment Team required that university leaders make several key decisions. These decisions included determining the process; deciding team membership and leadership; and debating important issues such as confidentiality, record keeping, and training for the team. While these discussions were occurring and initial decisions were made, the Threat Assessment Team was launched and began meeting regularly in January 2008. Team members, with the guidance of university leaders and on- and off-campus resources, worked on the next steps of implementing a robust threat assessment process at Virginia Tech. The mechanics of the team's operations needed to be worked out, and the university community needed to be engaged in understanding and welcoming threat assessment as a campus improvement.

Efforts to Support and Enhance Virginia Tech's Threat Assessment Activities

Efforts to Support and Enhance Virginia Tech's Threat Assessment Activities

Once the Virginia Tech Threat Assessment Team had been created and its membership decided, several critical steps were taken to launch the team's efforts and to overcome initial challenges that it faced.

Empowering the Team to Act

One step that university leaders agree was critical was to clarify the roles and responsibilities of the Threat Assessment Team and its members. The policies that Virginia Tech adopted to create the team and support its efforts empowered the formal Threat Assessment Team to act in a way that was not possible when the process was only informal. Along similar lines, university leaders underscored the fact that it is critical to provide resources so that the team can actually *do* its work. For Virginia Tech, this meant having a back-up for each member of the team in the event a member could not attend a meeting. This also meant ensuring that the team was aware of and could access the new case management resources that the university established through the OSDFS grant (see Chapter 4 for more information on establishing case management resources). Those who were interviewed recognize that assessing whether a person is posing a threat is only one component of the team's work and that the real value in having a team is to be able to take action to reduce that threat once it is identified. Having access to case management resources both on and off campus is critical to a team's ability to reduce any threats.

In addition to empowering the team through threat assessment policies, the Virginia Tech president empowered the team to act through more informal communications and support. The president wanted to ensure that Virginia Tech's Threat Assessment Team could be responsive in a situation and would not be hampered by institutional bureaucracy or hierarchy if the need arose. The president made it clear that team members and leaders can and should act without his permission if necessary and ensured them that he will stand behind their decisions, even if lawsuits arise as a result. At the same time, several university leaders made it clear that the president should be notified of any imminent threat and also needs regular briefings from the Threat

Assessment Team regarding the numbers and types of cases they are reviewing. With that information, the president can better understand the range of situations and troubling behaviors the team has encountered and be aware of any patterns that may emerge or that the team has identified (e.g., if several cases arise from the same department or supervisor). In addition, keeping executive leaders apprised of the work of the team allows the administration to assess the administrative and support needs of the team and to align resources as needed.

Strategic Planning and Ongoing Case Demands

One factor that impacted Virginia Tech's new Threat Assessment Team was a steady stream of active and new cases ever since the team began its operations. Having back-ups for team members has ensured that the team could stay abreast of its caseload and could hold meetings about cases even if certain original team members were absent.

The active caseload from the team's outset made it difficult for the team to find time to craft a mission statement, set out its threat assessment protocols, and engage in other planning activities designed to help set its direction and function. The team has had to devote nearly all available time to investigating, assessing, and managing cases, rather than to any high-level planning activities. Lacking a mission statement had a negative impact on the initial interactions between the Threat Assessment Team and the Care Team and hindered case referrals between the two teams, a factor that has been a source of frustration for both teams. Team members cautioned that they found it critically important to be clear in their mission statement about the purpose of threat assessment. In

Critical Planning Step: Take time to develop a threat assessment mission statement, specifying what cases the team will handle.

University Decision: Although Virginia Tech's team took more than a year to develop a mission statement, its adoption has resulted in greater clarification and agreement over the types of cases the team handles and improved the process of referrals to and from the Care Team.

crafting their mission statement, they wrestled over whether the Threat Assessment Team should handle cases that only involved potential physical harm or violence to others, or should also tackle cases that involved risk of suicide or unintentional self-harm. Defining what cases they would handle also had implications for the work of the student-focused Care Team. Depending on the definition selected, some of the cases previously handled by the Care Team would be handled by the Threat Assessment Team instead. Team members had to be comfortable with the fact that they would not cover those cases not specified by the mission statement and that they would have to entrust those cases to the judgment and actions of other entities on campus.

The Threat Assessment Team ultimately decided to handle cases that posed the possibility of violence or harm to the campus community or others. In addition, the team opted to be the first point of contact for all temporary detention order (TDO) cases (those in which a student, faculty member, or staff member is held for an involuntary emergency psychiatric evaluation). At the time of this writing, cases that appear to entail suicide risk without risk of harm to others or that are about unintentional self-harm (such as a severe eating disorder) are under discussion for handling by the Care Team (cases involving students) or the provisional Employee Resource Team (cases involving faculty or staff). Team members from both the Threat Assessment Team and the Care Team have acknowledged that having a mission statement for the Threat Assessment Team has clarified and streamlined case referrals between the two teams.

Managing the Team's Caseload

The Threat Assessment Team has been busy with active cases ever since it was created, which could be a function of several different factors or a combination thereof. For example, in the wake of the shootings, faculty, staff, and students have been on higher alert regarding threats or other troubling behavior. For new threat assessment teams at institutions that have not experienced—or not recently experienced—a shooting or similar traumatic event, this is less likely to be the case. For those institutions, their caseload would probably begin smaller and grow more gradually than did the caseload for the Virginia Tech Threat Assessment Team.

Threat Assessment Team members pointed to two things that helped them to become more efficient in their threat assessment work: (1) regularly-scheduled meetings and emergency meetings and who could do so) and (2) early training on how to handle threat assessment cases. The advanced training with tabletop exercises in particular was credited by team members and the team chair with giving them confidence in their abilities and in their decisions in cases they already had handled. Trainers with professional experience in assessing threats within a higher education setting were particularly welcomed by team members, who appreciated their knowledge, their experience in higher education settings, and their ability to understand the unique nature of working in a higher education context. The training also allowed them to be more efficient in delegating tasks to specific team members during any given case investigation. It allowed individual members to gain confidence, not only in their own abilities, but also in those of their teammates.

Establishing Procedures and Protocols

Many members of the Threat Assessment Team underscored the importance of establishing, in writing, clear procedures and protocols for how they should conduct their work. They said it was one thing to read about the theory of campus threat assessment, but it was another thing entirely to articulate the nuts and bolts of how to handle each case. Team members also emphasized that these protocols are different from the team's mission statement. The mission statement defines the scope of cases that the team will handle; its contents, therefore, help to guide the team's outreach efforts to the campus community and its message regarding the types of situations and ranges of behavior the team wants reported to it. The team's threat assessment protocols, however, serve as standard operating procedures for how it will proceed once it learns about a given person or situation of concern. The mission statement sets forth *what* cases the Threat Assessment Team will handle; the protocols dictate *how* the team will handle them. Team members interviewed for this project were emphatic that the team needed both—and needed them as early as possible. As stated above, the number of active cases faced by the Threat Assessment Team from the beginning made it difficult to find time to articulate those protocols, but the team's administrative coordinator played a

valuable role in overcoming this problem. After observing several team meetings and reviewing the handling of previous cases, she drafted the team's steps and procedures for the casework. Those draft protocols served as a starting-off point for the team to discuss and refine, an easier task for the team than drafting the protocols from scratch. Members suggested that for threat assessment teams that lack the time to craft protocols and procedures during their regular meetings, they could meet separately to discuss them (such as in a day-long retreat off-campus). Team members felt that it was vital for their operations to have established protocols and advised new teams to establish their protocols as early as possible. Team members emphasized, however, that a new team's protocols should be reviewed after several months or a year in operation so that the protocols can be revised to best reflect procedures and other steps or processes needed to enhance the team's work.

Building University-wide Confidence in the Process/Team

Interviews with university leaders revealed consensus that Virginia Tech already had an informal process in place before the shootings for handling persons of concern, but establishing the Threat Assessment Team made it a more formalized process. Having a formal threat assessment team and case management resources also made the process more widely known, something that is critical to successful threat assessment in general. The team depends on the entire campus community to report troubling behavior and situations to the team before it can gather more information, evaluate the situation, and take appropriate action. The concept of having a threat assessment team was more palatable to the university community once it was clear that

Critical Planning Step: Establishing protocols and procedures that specify how the team will handle its cases.

University Decision: Virginia Tech's new Threat Assessment Team coordinator observed team meetings and reviewed case files, then drafted initial protocols based on those observations. Team feedback and discussion about the draft protocols yielded the final protocols.

the university had always had an informal process for handling individuals (especially students) who had raised concern and that the Threat Assessment Team would make that process more formal, systematic, and transparent.

University leaders and other individuals continue to address issues typical for implementing a coordinated response to concerning behaviors. Frequently asked questions include: To what degree is the Threat Assessment Team a reflection of a "big brother" approach by the university administration? To what degree are records kept? By whom? With whom are information and records shared? Making a referral might engender concerns about "snitching" on a classmate or colleague. These and related concerns are not dissimilar from the types of discussions needed at most institutions when implementing necessary policies and procedures related to reports of harassment and discrimination or other forms of problematic behaviors within any organization.

Encouraging Reporting to the Team

Related to the notion of building confidence in the team and the threat assessment process, those interviewed all stressed that it was critical to encourage people on campus to report concerns to the Threat Assessment Team. As mentioned earlier, a threat assessment team is largely dependent on reports it receives from across campus to effectively do its work. Setting up a successful campus threat assessment capacity must, therefore, include efforts to encourage the entire campus community to report threats and other concerning behavior to the team. Encouraging reporting can take many forms, including conducting general campus-wide awareness sessions, participating in small department meetings, and "piggy-backing" on information-sharing mechanisms or conduits that already work on campus. For Virginia Tech, one key conduit of reports to the Threat Assessment Team was Virginia Tech's Care Team, where many university personnel were already comfortable reporting troubling student behavior. A similar mechanism already existed for reporting concerns about troubling or threatening staff behavior to Human Resources. Yet no such clear mechanism exists for reporting concerns about faculty behavior. Colleagues and students can report their concerns to their respective

department chairs, who, in turn, may report the behavior to the Threat Assessment Team. But no such report is required, just encouraged, so the system depends in large part on the judgment of individuals who receive the initial reports and decide whether or not to refer matters to the Threat Assessment Team.

In order to encourage everyone within the Virginia Tech community to report threats and concerning behavior to the Threat Assessment Team, the team uses multiple mechanisms to promote its activities. In particular, the team has focused efforts on training the campus about what the team does, how prevention is possible, the array of behavior and concerns it wants to hear about, and what happens once it receives a report. In addition, the team has distributed a one-page flyer describing its activities and providing guidance on what kinds of behaviors to report and how to do so (see Appendix E for a copy of the flyer). The team has also focused on dispelling misconceptions or misunderstandings regarding confidentiality laws such as FERPA and HIPAA[10] that have impacted information-sharing at Virginia Tech and other institutions in the past. So far, this general awareness training has been conducted for large audiences of faculty and graduate student teaching assistants, for small departmental meetings, and in one-on-one conversations. The Threat Assessment Team also plans to conduct similar awareness trainings periodically to help counter turnover in the faculty, staff, and student populations and to serve as a reminder of its work.

In addition, the Office of the Dean of Students has been charged with promoting the services of the Care Team, the case management process, and the Threat Assessment Team. To do so, the office created a resource card (see Appendix E for a sample) with the numbers of various people to call regarding distressed students and contact information for the Threat Assessment Team. The card is a resource that has been well received on campus.

---

10   FERPA refers to the Family Educational Records Privacy Act (please see *www.ed.gov/policy/gen/reg/ferpa/index.html* for more information). HIPAA refers to the Health Insurance Portability and Accountability Act (please see *www.hhs.gov/ocr/privacy/* for more information).

Summary

The efforts to support and enhance threat assessment activities included empowering the team to act, managing the team's caseload, establishing initial policies and procedures, building the university community's confidence in the team, and engaging the university community in making referrals. In addition to these policies and procedures required for the smooth and successful operation of the Threat Assessment Team, case management was an important element in the demonstration project and in the implementation of a comprehensive violence prevention scheme for the university. Case management operations were established for both employees and students and proved to be an important collateral function for referring individuals to the Threat Assessment Team. Case management services provide the university with the opportunity to deliver supportive services to individuals while coordinating with the Threat Assessment Team, Care Team, mental health services, and other services. Case management serves as an important element in the overall goal to prevent campus violence.

CHAPTER FOUR

Implementing Case Management Services

Implementing Case Management Services

At the heart of effective threat assessment efforts and violence prevention is case management: coordinating and brokering the resources necessary to intervene with a particular person or situation of concern to reduce the risk or threat posed, connecting the person with necessary help, and monitoring the progress of the intervention plan. Several of the after-action reviews conducted on the April 16 shootings at Virginia Tech highlighted the need to ensure that distressed students receive coordinated on-going care and treatment—essentially, case management. These reviews also noted that failure to provide such coordinated follow-up efforts for distressed students could leave the student and the institution at risk for experiencing further trauma or disruption.[11]

In addition to the recommendations from the various reviews of the April 16 shootings, research and practical case experience tell us that many individuals who plan acts of violence or who engage in threatening or worrisome behavior do so because of personal problems or out of extreme anguish or despair, including suicidal thoughts and plans,[12] and that a key element of effective violence prevention in these cases can be efforts to address that desperation.[13] The good news is that a wide array of resources can mitigate extreme anguish or suicidal thoughts/plans and can help individuals solve their personal problems. Harnessing those resources in a particular threat assessment case is what case management is all about. Case management is

> **"Above all else, institute a case management model and hire a case manager.... Somebody needs to be dedicated full time to following 30, 40, 50-plus students who need assistance."**
>
> James T. (Tom) Brown
> Dean of Students
> Virginia Tech

---

11   See, for example, Virginia Tech Review Panel (2007), retrieved on October 31, 2009, at *www.vtreviewpanel.org/report/index.html.*

12   See, for example, Vossekuil *et al.* (2002).

13   See Fein *et al.* (2002).

particularly effective when it is coordinated and well monitored; that is, when the threat assessment team develops a case management plan that is then implemented, monitored to ensure that it is working and that there are no unintended negative consequences, and adjusted if it is not working as planned.

A major component of the U.S. Department of Education grant to Virginia Tech was to develop and sustain case management resources at the university. The grant funding allowed Virginia Tech to create three case manager positions: two dedicated for student cases and one for employee cases. This model of case management reflects Virginia Tech's residential campus, the structure and function of student support services within the Division of Student Affairs, and the manner in which the university provides human resources. Since the inception of the grant, university personnel have succeeded in institutionalizing all three positions, moving them from grant-funded to permanent status.

The functions associated with case management are important elements in identifying and referring individuals at risk. Many of the university leaders and Threat Assessment Team members who were interviewed stressed the importance of Virginia Tech instituting a formalized case management process to coordinate assistance and monitor intervention for students and employees of concern. For example, Virginia Tech Dean of Students Tom Brown strongly encouraged institutions: "Above all else, implement a case management model and hire a case manager.... Somebody needs to be dedicated full time to following 30, 40, 50-plus students who need assistance." This appears to be the direction in which many higher education institutions are starting to go. According to the AUCCCD Annual Survey for University and College Counseling Center Directors, in the 2006-2007 academic year (the year that included the Virginia Tech shootings), only one higher education counseling center reported having a case manager on staff; in the survey conducted for the 2007-2008 academic year, the number had jumped to 28 counseling centers.[14]

---

14 Rando, R. & Barr, V. (2009). *The Association for University and College Counseling Center Directors Annual Survey, 2008.* Indianapolis, Ind.: Association for University & College Counseling Center Directors.

Case Management for Students

Case management functions for students were established in two departments within the Division of Student Affairs. One case manager is dedicated to responding to and managing cases that involve referrals of students for evaluation and/or hospitalization. Within the student counseling center, the case manager is assigned to attend hearings that are held to determine whether a student requires a psychiatric evaluation. These hearings occur off campus as legislated by the Code of Virginia and regulations governing community mental health services. In addition, the case manager works on coordinating mental health services within and external to the university. Frequently, the case manager serves as a liaison between the student "client" and his or her family and on- and off-campus support services. The case manager assists the counseling center in monitoring a student's progress if a student is required to complete elements of a treatment plan before returning to campus or if he or she is engaged in treatment as a requirement to remain on campus.

The second student-focused case manager is dedicated to the management of cases referred to the student Care Team in the Office of the Dean of Students. The purpose of securing two case managers to address cases involving students was the recognition that it is important to have a link between psychiatric services performed off campus and the on-campus mental health services.

Personnel in the Office of the Dean of Students, which houses the university's Care Team, recommend establishing a case-tracking system to facilitate case management efforts. That office recently began using an electronic case-tracking system that pulls all relevant information about each case onto one screen visible on a computer. At the time of this writing, Virginia Tech was still working on integrating the electronic case management system in the Office of the Dean of Students into the electronic system used to manage referrals to the Office of Student Conduct. But even without that interoperability yet in place, staff members in the dean of students office believe that adding an electronic case-tracking system has significantly enhanced their ability to successfully support and monitor distressed students. Staff members also attribute the overall success of the case management process to

the individuals they selected to fill the case manager positions in their office. In particular, they looked for master's-level persons with student affairs backgrounds and after-hours on-call experience, although they did not necessarily look for someone with case management experience.[15]

Case Management for Employees

The case management function for employees was established in the employee relations area of the Department of Human Resources (HR). One case manager is dedicated to working with employees who come to the attention, for a variety of reasons, of employee relations and other professionals in HR. The case management function within HR is to serve as a liaison between department heads, managers, employees, employee resources on campus, and the state-provided Employee Assistance Program.[16] Within HR, the case manager has provided outreach services to departments across the university and has assisted in coordinating on- and off-campus support services for a variety of concerns. The employee-focused case manager has also helped to advance Virginia Tech's violence prevention efforts by providing workshops to departments, meeting with managers and employees one-on-one, and partnering with wellness and other university-wide efforts to raise awareness of the resources available on and off campus for employees who might benefit from support services.

One challenge noted by many university leaders and Threat Assessment Team members was that compared with the array of resources available to assist in student cases and, to some degree, in staff cases, far fewer resources are available to assist in faculty cases. Several Virginia Tech leaders noted that unless or until a faculty member became a true, real, or obvious threat, the university had very few options available to intervene to address disturbing or worrisome behavior or an emerging concern. In an effort to develop resources to facilitate earlier assistance or intervention, Virginia Tech crafted and succeeded in passing a policy that allows supervisors to require that any employee,

---

including tenured faculty members, be referred to the Employee Assistance Program (EAP) if his or her behavior or conduct is sufficiently disruptive or concerning and if a "process of progressive, corrective discipline has been unsuccessful" or if the "presenting problem is of an urgent or emergency nature" (see Appendix B for Virginia Tech's Employee Assistance Program Policy). A required approval process ensures that the referral process cannot be used in a capricious manner; supervisors wishing to make an EAP referral a condition of continued employment must first gain approval from the relevant vice president (for faculty cases) or associate vice president for human resources (for staff cases).[17]

Facilitating Information-Sharing

While very different in scope and delivery, case management services for students and for employees have proven to be an essential component of Virginia Tech's overall violence prevention effort. One strength of the case management functions currently in place at the university is the variety of backgrounds and perspectives brought by the case managers and the diversity of the offices in which they reside. Providing university-wide prevention services in addition to delivering case-specific management services appears to be a successful model for Virginia Tech and may prove useful for similarly complex and decentralized institutions. Case management services provide necessary communications and connections across the unintentional divides that can exist between and among the university's "silos." In addition, case managers frequently broker services on and off campus for students and employees because of the managers' backgrounds in mental health and familiarity with social work, psychiatric nursing, and other relevant models of case management.

Summary

Case management services for both students and employees are vital to successful threat assessment and campus violence preven-

---

tion efforts. It is important to remember that the purpose of threat assessment is to assist and intervene if someone poses a threat or if they otherwise need help. Case managers can help broker services and connect individuals to on- and off-campus support mechanisms. At Virginia Tech, the demonstration project afforded the opportunity to establish full-time positions dedicated to providing case management services and linking various offices and functions from across the university. The roles of the case managers are different in each office, but the overarching goal is the same: coordinate and provide appropriate information, referral, and support services to promote the success of the individual and the safety of the campus.

Implementing threat assessment and case management functions has required special attention by university leaders and those responsible for carrying out the day-to-day decisions of keeping the campus safe. Many of the individuals involved in implementing the elements of the demonstration project, including threat assessment and case management, were deeply involved in the university's response to the shootings in April 2007. Serving the university community as both first and longer-term responders has shaped the work of those engaged in launching threat assessment efforts and other elements associated with the demonstration project. As the next chapter illustrates, the April 16 shootings at Virginia Tech remain a backdrop against which university policy and program decisions continue to be made.

CHAPTER FIVE

Special Issues Affecting a Post-incident Campus

Special Issues Affecting a Post-Incident Campus

Throughout the steps that Virginia Tech has taken to build, support, enhance, and promote its new Threat Assessment Team and case management services, some particular issues have arisen because Virginia Tech experienced a mass shooting before implementing its threat assessment and case management processes. While many of the obstacles and challenges described in previous chapters are typical of hurdles that institutions may face in establishing a threat assessment capacity, other issues facing Virginia Tech in particular have made creating and running a Threat Assessment Team all the more difficult—and more necessary—because of the magnitude of the tragic incident it experienced and possibly because of the magnitude of that incident. While these experiences may well be unique to Virginia Tech or to campuses that have experienced a shooting or other traumatic event, we believe there is still value for the broader higher education community in reporting on these issues and challenges.

Need for Support Resources for Virginia Tech Personnel

One vital consideration for Virginia Tech in setting up its case management services was to identify and facilitate access to support services for members of the university community who were impacted by the shootings on April 16, 2007. Virginia Tech received a separate grant from the U.S. Department of Justice, Office for Victims of Crime to provide recovery assistance to groups of direct victims of the April 16 shootings. Providing services to the direct victims of the shootings was and is a very high priority for the university. The families of deceased victims, families of injured victims, and those injured in the shootings have received services through the university's Office of Recovery and Support, supported in large part with funds received from the U.S. Department of Justice grant.

In addition, Virginia Tech has come to realize in the years since the mass shooting that a broad array of members of the Virginia Tech community have been significantly affected by the 2007 tragedy. Specifically, many individuals who were on campus or even away from campus but a part of the Virginia Tech community were deeply impacted by the events of April 16, even if they were nowhere near the location

of the shootings. Identifying resources that could provide assistance to this broad array of Virginia Tech community members has become important as well.

Moreover, Virginia Tech has learned that the need for these support services may be a long-term one. Research on responses to trauma has shown that for some individuals impacted by a traumatic event, it can take months or even years for a trauma response to emerge.[18] Even when a response does surface, the trauma response may not look like a "classic" post-traumatic stress response, with flashbacks and significant psychological distress clearly stemming from the trauma. Rather, in some cases, it may appear as a collection of unrelated physical symptoms that have no clear underlying physiological cause. Or the response may simply appear as severe stress or anxiety or as intense anger. These responses can arise in individuals who appeared by all accounts to function well following the traumatic incident but who, years later, may develop extreme anxiety, anger, or physical symptoms that at first glance may not appear to be linked to the traumatic event but, in fact, are. Recognizing this possible delay in response to the April 16 shootings, Virginia Tech has been working to identify and make available an array of support resources for its students, members of the faculty and staff, and families as permanent resources for personnel to access, as needed, over time.

External Scrutiny

Since April 16, 2007, many aspects of campus safety policies and procedures at Virginia Tech have come under scrutiny, from the outside as well as from within the campus. This scrutiny has taken the form of criticism of decisions made and steps taken, but it also has taken the form of many campuses looking to Virginia Tech for expertise in adopting leading-edge campus safety practices and technologies. It is worth noting that this scrutiny has been welcomed by the Virginia Tech leadership in its effort to help all campuses gain a better understanding of campus violence prevention efforts and effective safety measures

through intensive examination of the April 16 shootings. This external scrutiny continues on critical decision-making regarding issues of campus safety. Those in a position to make critical decisions on behalf of the university are aware that whatever future decisions they make may be subject to similar external public scrutiny, as they have been previously.

Cases from Outside Campus

In addition to the regular caseload of students, faculty members, and staff members that a threat assessment team typically handles, the Virginia Tech Threat Assessment Team has had to address concerning behavior from individuals outside campus, including people who post disturbing writings or videos on the Internet as well as people who visit the university and engage in troubling behavior on campus. Some of these individuals have traveled out of desperation or thoughts of suicide in an effort to see the Virginia Tech memorial. Some of these individuals are eventually reported to the Threat Assessment Team because their behavior on campus raises significant concerns. One case, for example, involved a professor from another university who was suicidal and traveled to Virginia Tech with the plan of killing himself in front of the April 16 memorial. In these types of cases, the Threat Assessment Team is called to evaluate the person and situation and to develop a plan to intervene if necessary, even if the person has no relationship with the university.

Post-4/16 Action Imperative

For Virginia Tech, the mass shooting on April 16, 2007, is not the only violent incident the campus has experienced in recent years. Since that time, several student homicides and suicides have occurred. Shortly after the 2007 mass shooting, a student suicide at Virginia Tech gained wide media coverage. In early 2009, a Virginia Tech graduate student murdered another Virginia Tech graduate student in front of witnesses in the university's Graduate Life Center. And in the beginning of the 2009-2010 academic year, two Virginia Tech students were murdered in a national forest campground that is approximately 15 miles from the campus. As of this writing, the campground murders have not been solved; nor is it clear if there is any association with the university other than the fact that the victims happened to be Virginia Tech students.

---

18   E.g., Frueh, B.C., Grubaugh, A.L., Yeager, D.E., & Magruder, K.M. (2009). "Delayed-onset post-traumatic stress disorder among war veterans in primary care clinics." *The British Journal of Psychiatry*, 194, 515-520.

It is understandable that for some individuals at the university, subsequent violent incidents have rekindled memories of the April 16 shootings. In facing these post-4/16 emergencies, some decision makers have had to negotiate varying levels of anxiety brought on by the need to respond to the emergency. Some university leaders present on campus during the April 16 shootings have expressed feeling significant pressure to "do something" every time a subsequent violent incident has occurred. In contrast, for decision makers who have joined the university since the shootings and may not have felt the sharp nature of the criticism, the need to act may be less acute.

Observations of Threat Assessment Team case discussions suggested a similar "action imperative" on the part of many team members, nearly all of whom were present on campus during the 2007 mass shooting. Team members appeared to focus much of their case discussions on identifying and implementing case management options—on what the team and the university could do to intervene and/or help—before the team had evaluated whether the person of concern posed a threat or not. Recognizing its tendency toward action/intervention, the Threat Assessment Team has since moved toward engaging in more formalized assessments of cases before developing and implementing case management plans.

Summary

As a result of the April 16 mass shootings, Virginia Tech has faced some unique challenges in setting up its threat assessment and case management processes. Recognizing these challenges, Virginia Tech has taken an array of steps to help mitigate their impact. The next chapter will focus on other challenges that Virginia Tech's Threat Assessment Team face that are more common to institutions of higher education and to campus threat assessment teams generally. It will also include advice and recommendations from Threat Assessment Team members and from Virginia Tech's leaders on pitfalls that campuses can avoid in setting up a new threat assessment process.

CHAPTER SIX

Potential Pitfalls and Ongoing Challenges

Potential Pitfalls and Ongoing Challenges

Throughout the process of interviewing university leaders and Threat Assessment Team members, those interviewed offered suggestions for institutions of higher education that were considering establishing a threat assessment team or enhancing their existing threat assessment capabilities. These recommendations are captured here in two groupings: (1) pitfalls that Virginia Tech personnel recommend other institutions try to avoid when setting up their threat assessment capacity and (2) future challenges in the field of campus threat assessment in general that may impact any or all institutions of higher education in their efforts to identify and reduce behavioral threats on campus. These suggestions are not intended to be prescriptive but rather are included to provide some guidance and food for thought.

Potential Pitfalls

Complacency

Those involved in building and running Virginia Tech's threat assessment process have noted that it would be easy for a threat assessment team to become complacent, especially when nothing happens. That is, it would be easy for team members to assume that a particular case is not one of concern simply because none of the persons and situations the team has previously addressed turned out to pose a threat or to assume that there was no urgent need to intervene simply because failing to intervene in prior cases had not resulted in any harm or tragedy. Those interviewed stressed the importance for a threat assessment team to remain vigilant and that undergoing periodic tabletop exercises and other types of training could help a team to do so.

Team Name Selection

University leaders noted that it is important for an institution to give careful consideration to the name it gives its threat assessment team. For Virginia Tech, President Steger felt it was important to call its threat assessment team just that: the Virginia Tech Threat Assessment Team. He opted for this name because the specific concept of threat assessment had been advocated so widely in the numerous reports on campus safety released following the Virginia Tech shootings. And once the Virginia legislation was enacted, it required each public

college and university in the commonwealth to establish a "threat assessment team." President Steger, other university leaders, and Threat Assessment Team members all noted, however, that calling it the "threat assessment team" may concern some people on campus or inadvertently give the impression that the team's work narrowly focuses only on threats and not more broadly on a wide array of concerning behavior. Other institutions have opted for names such as Student Assistance Team, Person of Concern Team, and Behavioral Assessment Team. University leaders also emphasized that at Virginia Tech, the Threat Assessment Team was but one component of a much larger campus safety enterprise. They cautioned that just having a threat assessment team is not enough and that to be effective, the team should be integrated into a comprehensive campus safety plan.

Critical Question: What should an institution call its threat assessment team?

University Decision: Consistent with the Code of Virginia, Virginia Tech opted to keep the name "threat assessment team" but advises that other names may be preferable for various reasons.

Ongoing Challenges

Police Involvement on the Team

For Virginia Tech, one ongoing challenge in having the police chief chair the Threat Assessment Team has been the tendency of team members and other university leaders to perceive that the team is

No Silos

Those interviewed all agreed that one of the biggest pitfalls to avoid was to the usual tendency of higher education institutions to operate in information "silos," with different departments and offices taking steps on their own to handle situations without knowing the bigger picture or factoring in steps that other departments may be taking. One of the most important roles that Virginia Tech envisioned for its threat assessment team was to facilitate information sharing across departments and offices and to break down some of those silos, at least in cases that the Threat Assessment Team would handle.

exclusively a law enforcement entity. Team members caution that the police department should not do everything on a threat assessment team, especially when it comes to gathering information about persons or situations of concern. Similarly, those interviewed caution that it is important for all team members to be familiar with relevant state laws governing what information the police department can share with the Threat Assessment Team and include in team records. They noted that team members may be able to access much of that information on their own if it is publicly available (such as state sex offender registry information) and may not have to rely on disclosure from the police department.

The strong association between the police department and the Threat Assessment Team results in having to address concerns about making reports to the team. Faculty and staff members and students need to be reassured that if they call about a person of concern they are not necessarily making a police report or getting themselves or that other person "in trouble." The association with the police department requires that all members of the team and affiliated offices serve as ambassadors for the team's interest in early detection and the provision of supportive services to individuals who may benefit.

Counseling Center Involvement on the Team

Involvement of the counseling center director or staff member on the Threat Assessment Team makes good conceptual sense and works well in theory. But in practice, it can be an ongoing challenge. This may be particularly true on campuses like Virginia Tech that are located in rural areas where the surrounding communities are limited in what they might be able to offer in the way of mental health assessment and treatment services. On those campuses, it will likely fall to the counseling center director (or designated staff member) to conduct mandatory assessments of students, faculty, or staff because few other options may be available outside the campus counseling center. In the case of Virginia Tech, the counseling center director is often asked to conduct mandatory assessments, which requires him to assume a different role than he is in when he serves as a patient's therapist or counselor. The counseling center director has emphasized that when he is asked to conduct a psychological assessment of someone for the

Threat Assessment Team, he has to make it very clear to the person of concern that he is working as an evaluator for Virginia Tech in that situation and not as a therapist. He also must emphasize that anything the person says will not be treated as confidential and must be shared in order for the team and the university to be able to help. When he has followed this process in the case of assessments for students, this approach appears to have worked well as long as the assessor is absolutely clear about whom he/she works for in any given evaluation. The approach has been less clearly effective in the one case of a faculty assessment that the counseling center director was asked to conduct.

Need for Additional Case Management Resources

At the time of this writing,[19] one concept that was being debated at Virginia Tech was whether to create a Care-type team for faculty and staff members in need of assistance. Recognizing the importance of early intervention in preventing harm and self-harm and understanding the need to have an array of intervention resources, Virginia Tech has faced an ongoing challenge in finding and using a variety of resources to support or intervene with faculty and staff members who have raised some concern. The university chose to address this issue by exploring the idea of a provisional Employee Resource Team (ERT) to provide a more formal means to address faculty and staff members who appear to be in crisis or in need of some assistance. Similar to the genesis of Virginia Tech's Threat Assessment Team, the university's ERT would be a more formal version of an informal multi-disciplinary group that already met on a regular basis to discuss concerns related to faculty and staff behaviors. Virginia Tech's senior leaders are still weighing the pros and cons of having an ERT, with no clear consensus yet formed.

Related to this issue has been consideration concerning whether to require or mandate counseling in certain situations. Recently, 80 percent of counseling center directors surveyed from across the United States reported that they do mandatory *assessments*[20] of persons of concern, but there are no good data on the percentage that engage in manda-

---

19 October 2009.

20 Rando & Barr (2009).

tory counseling. Like other institutions of higher education, Virginia Tech will have to think through the policies and ethics of mandatory counseling. It is important to note that it is both ethical and acceptable to mandate *counseling* in other arenas, such as in substance abuse and mental health diversion cases where someone who has broken the law (for certain violations where a substance addiction or psychological problem is suspected of playing a role in the crime committed) is ordered by the court to undergo mandatory counseling as a condition for avoiding prison and eventually getting the charges dropped.

Legislative Issues

One final challenge raised by several university leaders was the importance of staying current with developments in the state legislature that could impact the work of an institution's threat assessment team. In Virginia Tech's experience, there was an initial push within the Virginia legislature to require the state's public colleges and universities to include representatives of affected populations (e.g., students, faculty members, staff members) on their threat assessment teams. Most at Virginia Tech were opposed to including such representatives, arguing that doing so could have a chilling effect on the team's ability to discuss confidential information. Through regular contact with their legislators, Virginia Tech officials were able to voice these concerns. Eventually, the Virginia legislature backed away from that requirement. Other issues may arise during the course of a threat assessment team's work, or the team may opt to lobby its state legislature to change laws.

As of this writing, there were three proposals before the Virginia legislature that could impact threat assessment teams at colleges and universities. The first is a proposal that the state's Freedom of Information Act be amended to exclude all records and electronic communications of a threat assessment team from records open to public inspection. The second is a proposal that law enforcement officers, who are members of a threat assessment team, be granted the authority to share certain criminal history information with the team. The third is a proposal that the state legislation on health records privacy be amended to permit mental health professionals who sit on a threat assessment team to have the authority to share relevant information in student records with the team. Good communication

with the legislature can help threat assessment teams to stay current with legislative proposals that may impact their work and to help to educate policymakers about additional needs or obstacles.

Summary

In some ways, a threat assessment team's work is never done. There will always be challenges that can make a team's work more difficult; however, there are steps that a team can take—and cheerleaders it can recruit to champion its work—to help overcome those obstacles and even make its work more effective. Virginia Tech's Threat Assessment Team and leaders offered several cautions on pitfalls that can be avoided with some simple advance planning or strategic thinking. They also acknowledge that their work continues, both at the case level and at the higher level, in terms of strategic planning to ensure that their efforts to prevent violence are as effective as possible.

CONCLUSION

Conclusion

April 16, 2007, marked a turning point in campus safety, not only for Virginia Tech, but also for all higher education institutions in the United States (and arguably in some countries outside the U.S. as well). The mass shootings at Virginia Tech prompted tremendous attention and focus on issues of campus security in general and in particular on identifying and intervening with at-risk behaviors in students, faculty members, and staff members. As the attack at Columbine High School served as a wake-up call for K-12 safety and security issues, so, too, has the Virginia Tech attack forced all of us to focus more on campus safety and on violence and suicide prevention. As nearly all the major reports on campus safety released since the Virginia Tech attacks have advocated, higher education institutions are encouraged to develop campus threat assessment teams and devote resources and personnel toward making them work. Fortunately, as Virginia Tech's efforts to institute and sustain a campus threat assessment program have shown us, the task at hand is feasible.

Throughout the time since Virginia Tech experienced its mass shootings, campus personnel and outside experts have worked diligently to create, support, and continue to refine the Virginia Tech Threat Assessment Team and to hone its ability to identify, evaluate, and intervene with persons, situations, and behaviors of concern. The team's development and evolution continue to this day. Virginia Tech leaders, Threat Assessment Team members, and others are quick to point out that they do not see themselves as experts in the field of campus safety or of campus threat assessment. But they recognize that their new identity as the site of the most lethal attack on a U.S. institution of higher education puts them in a unique position as a laboratory of sorts for new developments in the field of campus safety.

The grant from the U.S. Department of Education, Office of Safe and Drug-Free Schools allowed Virginia Tech to embark on a comprehensive effort to identify and address at-risk behavior in their students, faculty members, staff members, and also visitors. This effort included not only establishing, training, and supporting their Threat Assessment Team, but also creating multi-faceted case management services that could serve both Virginia Tech students and employees.

Case management services are at the heart of effective threat assessment and violence prevention efforts. Although much has been written since the Virginia Tech attack about the value of higher education institutions developing threat assessment teams, far less attention has been paid to the value of establishing case management resources and adding full-time case management staff on campus. It is important to note that Virginia Tech leaders, Threat Assessment Team members, and Care Team members alike credit establishing and institutionalizing this case management capacity with allowing Virginia Tech to assist a wide array of persons in need on campus. Our Virginia Tech colleagues suggest that institutions of higher education give serious consideration to adding case management positions to their university rosters when setting up a threat assessment capacity.

As we have documented here, the road to developing a well-functioning threat assessment team is not always easy. But it is doable, especially with persistence and a willingness to continually evaluate and refine the process. As more higher education institutions develop and implement threat assessment teams and as more research is conducted on incidents of campus violence, we will all learn more about what makes for effective campus threat assessment teams and what strategies can raise team functioning to an even higher level. It is our hope that the openness of Virginia Tech in sharing its experience in developing, implementing, and refining its threat assessment process will help add to the knowledge base in the field of campus threat assessment and will enhance campus safety in general.

APPENDICES

APPENDIX A

Virginia Laws

Appendix A: Virginia Laws

CODE OF VIRGINIA REFERENCES

§ 23-9.2:8. Policies addressing suicidal students.

The governing boards of each public institution of higher education shall develop and implement policies that advise students, faculty, and staff, including residence hall staff, of the proper procedures for identifying and addressing the needs of students exhibiting suicidal tendencies or behavior. The policies shall ensure that no student is penalized or expelled solely for attempting to commit suicide, or seeking mental health treatment for suicidal thoughts or behaviors. Nothing in this section shall preclude any public institution of higher education from establishing policies and procedures for appropriately dealing with students who are a danger to themselves, or to others, and whose behavior is disruptive to the academic community.

(2007, c. 705.)

§ 23-9.2:9. Institutional crisis and emergency management plan; review required.

The board of visitors or other governing body of each public institution of higher education shall develop, adopt, and keep current a written crisis and emergency management plan. Every four years, each institution shall conduct a comprehensive review and revision of its crisis and emergency management plan to ensure the plan remains current, and the revised plan shall be adopted formally by the board of visitors or other governing body. Such review shall also be certified in writing to the Department of Emergency Management. The institution shall coordinate with the local emergency management organization, as defined by § 44-146.16, to ensure integration into the local emergency operations plan.

(2008, cc. 450, 526.)

§ 23-9.2:10. Violence prevention committee; threat assessment team.

A. Each public college or university shall have in place policies and

procedures for the prevention of violence on campus, including assessment and intervention with individuals whose behavior poses a threat to the safety of the campus community.

B. The board of visitors or other governing body of each public institution of higher education shall determine a committee structure on campus of individuals charged with education and prevention of violence on campus. Each committee shall include representatives from student affairs, law enforcement, human resources, counseling services, residence life, and other constituencies as needed. Such committee shall also consult with legal counsel as needed. Once formed, each committee shall develop a clear statement of: (i) mission, (ii) membership, and (iii) leadership. Such statement shall be published and available to the campus community.

C. Each committee shall be charged with: (i) providing guidance to students, faculty, and staff regarding recognition of threatening or aberrant behavior that may represent a threat to the community; (ii) identification of members of the campus community to whom threatening behavior should be reported; and (iii) policies and procedures for the assessment of individuals whose behavior may present a threat, appropriate means of intervention with such individuals, and sufficient means of action, including interim suspension or medical separation to resolve potential threats.

D. The board of visitors or other governing body of each public institution of higher education shall establish a specific threat assessment team that shall include members from law enforcement, mental health professionals, representatives of student affairs and human resources, and, if available, college or university counsel. Such team shall implement the assessment, intervention, and action policies set forth by the committee pursuant to subsection C.

E. Each threat assessment team shall establish relationships or utilize existing relationships with local and state law enforcement agencies as well as mental health agencies to expedite assessment and intervention with individuals whose behavior may present a threat to safety.

(2008, cc. 450, 533.)

§ 23-9.2:11. First warning and emergency notification system required. By January 1, 2009, the governing boards of each public institution of higher education shall establish a comprehensive, prompt, and reliable first warning notification and emergency broadcast system for their students, faculty, and staff, both on and off campus. Such system shall be activated in the case of an emergency and may rely on website announcements; e-mail notices; phone, cellular phone, and text messages; alert lines; public address systems; and other means of communication. In addition, each institution shall designate individuals authorized to activate the warning system and provide such individuals with appropriate training for its use.

(2008, cc. 413, 450.)

ADDITIONAL VIRGINIA STATE LAWS (went into effect 7/1/2008)

» HB 559 Emergency custody orders, temporary detention orders, and involuntary commitment; criteria: *http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb559*

» HB 1005 Higher educational institutions; notification to parent of mental health treatment for student: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+HB1005*

» SB 539 Higher educational institutions; board of visitors, etc. to establish violence prevention committee: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+SB539*

» SB 636 Higher educational institutions; requesting complete student record from high school: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+sb636*

» HB 1449/ SB 256 Public institutions of higher education; crisis and emergency management plans: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+SB256*

» HB 576 Mental health records; health provider shall disclose information to provide care, etc. of minor: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+HB576*

» HB 499/ SB 246 Involuntary commitment; establishes new standard for outpatient commitment: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+HB499*

» HB 1058 Higher educational institutions; release of educational records: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+HB1058*

» HB 583 Emergency custody orders; extension of time: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+HB583*

» SB 141 State hospitals; discharge plans upon release: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+SB141*

» HB 709/ SB 226 Firearms; answering mental health questions on consent form required when purchasing, etc.: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+SB226*

» HB 815 Voluntary admission; report to Central Criminal Records Exchange: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+bil+HB0815*

» SB 216 Voluntary admission; report to Central Criminal Records Exchange: *http://leg1.state.va.us/cgi-bin/legp504.exe?081+sum+SB216*

Appendix B

Sample Policies

Appendix B: Sample Policies

Campus and Workplace Violence Prevention Policy
www.policies.vt.edu/5616.pdf

Virginia Polytechnic Institute and State University No. 5616 Rev.: 2
Policy and Procedures **Date: March 19, 2008**

Subject: Campus and Workplace Violence Prevention Policy

1. Purpose

It is the intent of Virginia Polytechnic Institute and State University to provide a safe and secure environment for university employees, students, and visitors by establishing preventative measures, holding perpetrators accountable, and providing assistance and support to victims. This policy specifically addresses the university's position on the prevention, reduction, and management of violence to provide a safe working and learning environment for our students, employees, and visitors at all university owned, controlled, or leased properties, including satellite locations. In implementing this policy, the university is guided by the Commonwealth of Virginia's Policy 1.80 Workplace Violence and Policy 2.30 Workplace Harassment. The conduct of students is covered, in depth, by the University Policies for Student Life. The Division of Student Affairs, Office of Judicial Affairs is responsible for the implementation of the UPSL. Nothing in this policy amends the University Policies for Student Life.

2. Policy

Virginia Tech does not tolerate acts of violence or hostility committed by or against employees, students, contractual workers, temporary employment agency workers, volunteers, visitors, or other third parties on university owned, controlled, or leased properties, or while conducting university business at any location, including representing the university at conferences or off-site meetings, or riding in university owned or leased vehicles. This policy applies to the personal conduct of an employee while functioning in the course and scope of employment, whether on or off campus, and to any off-duty violent conduct that adversely impacts a university employee's ability to perform his or her assigned duties and responsibilities. The personal conduct of

students involving violations occurring off university property will be addressed under University Policies for Student Life if university officials decide that university interests are involved. Student employees, including graduate students with assistantships, may also be covered under relevant employee policies.

It is intended that all useful management strategies be employed to identify and prevent incidents of workplace and campus violence, reduce the effects of violence on victims, and provide consequences to those who threaten or perpetrate violence. University managers, employees, and students are responsible for reporting indications of possible hostile behavior and must not be subjected to any acts of retaliation for reporting concerns. The university will use available resources such as the Employees Assistance Program, law enforcement offices, the university's Women's Center, relevant offices within the Division of Student Affairs, and applicable human resources and student programs and policies in responding to alleged acts of violence.

2.1 Prohibited Conduct and Sanctions

Violence includes, but is not limited to, intimidation, threats, physical attack, domestic and dating violence, stalking, or property damage and includes acts of violence committed by or against university employees, students, contractual workers, temporary employment agency workers, customers, relatives, acquaintances, or other third parties on university facilities. Prohibited conduct includes, but is not limited to, intentionally

» Injuring another person physically;

» Engaging in verbal or physical behavior that creates a reasonable fear of injury to an identifiable person;

» Engaging in verbal or physical behavior that subjects an identifiable individual to extreme emotional distress;

» Engaging in threatening or violent behavior based on race, ethnicity, gender, sexual orientation, or other protected status;

» Defacing or damaging property;

» Threatening to injure an individual or to damage property;

» Committing injurious or threatening acts related to sexual assault, stalking, dating or domestic violence, or sexual harassment;

» Brandishing a weapon or firearm; and

» Retaliating against any individual who, in good faith, reports a violation of this policy.

Verbal behavior also includes use of any method of communication such as e-mail, comments posted on websites, or other paper or electronic media. A violation of this policy shall be considered unacceptable conduct and subject to the disciplinary actions under the appropriate faculty, staff, and student policies, up to and including dismissal.

» University staff and classified employees are subject to disciplinary action as outlined in the Commonwealth of Virginia Standards of Conduct and Performance Policy 1.60.

» University faculty members are subject to disciplinary review as outlined in the Faculty Handbook or Research Faculty Handbook.

» Hourly and wage employees, including adjunct faculty, are "at will" employees and may be disciplined or dismissed.

» Undergraduate and graduate students are subject to disciplinary actions as outlined in the University Policies for Student Life.

Individuals who violate this policy may also be subject to arrest for trespass and/or violation of the appropriate state criminal statute and/or may be barred from campus. For employees, an act of off-duty violent conduct may be grounds for disciplinary action, up to and including dismissal per applicable personnel policies.

2.2 Prohibition of Weapons

The university's employees, students, and volunteers, or any visitor or other third party attending a sporting, entertainment, or educational event, or visiting an academic or administrative office building, dining facility, or residence hall, are further prohibited from carrying, main-

taining, or storing a firearm or weapon on any university facility, even if the owner has a valid permit, when it is not required by the individual's job or in accordance with the relevant University Policies for Student Life. Any such individual who is reported or discovered to possess a firearm or weapon on university property will be asked to remove it immediately. Failure to comply may result in a student judicial referral and/or arrest or an employee disciplinary action and/or arrest.

2.3 Authorized Exceptions to Prohibition on Possession of Firearms or Weapons

An employee may possess a firearm or weapon if it is

» Used by an employee who is a certified law enforcement officer employed by the Virginia Tech Police Department;

» Required as a part of the employee's job duties with the Commonwealth of Virginia; or

» Connected with training received by the employee in order to perform the responsibilities of their job with the university.

Employees and students may possess and use appropriate tools, such as saws, knives, and other such implements, necessary for the performance of their job duties or school work, or for student recreational purposes approved under University Policies for Student Life. Certain agricultural workers have been authorized to use firearms, and hunting on university property may be authorized by the appropriate university officials. Some employees reside in university-owned houses and are permitted to keep personal firearms on these premises; however, this exception does not extend to employees living in university residence halls. As stated in the University Policies for Student Life, students may not possess, use, or store firearms or weapons on university property; however, firearms and other weapons may be stored with the Virginia Tech Police Department to be checked out for use off campus. Organizational weapons of the Virginia Tech Corps of Cadets, approved by the commandant, are not prohibited by this policy. Other exceptions must be approved by the vice president for administrative services, in consultation with appropriate university offices.

2.4 Prevention, Risk Assessment, and Response

As part of a larger and institution-wide commitment to a safe campus and workplace environment, the university is committed to the development of preventative measures, including a campus and workplace violence prevention and risk assessment committee, security planning for at-risk individuals, pre-employment screening, and general programs to increase employee and student awareness. The vice president for administrative services will chair a campus-wide Workplace Violence Prevention and Risk Assessment Committee, which will be appointed by the president and will be responsible for

» Conducting an annual review to identify potential or existing risks, including gathering and analyzing reports and data to identify high-risk departments, activities, or locations;

» Recommending and implementing employee and student awareness and training programs on campus and workplace violence;

» Implementing plans and protocols for responding to credible threats and acts of violence (crisis management plan);

» Reviewing and developing threat assessment and response policies and procedures;

» Reviewing periodic summary reports from Student Affairs, campus police, Human Resources, and other offices;

» Communicating internally with employees and students; and

» Evaluating the effectiveness of the university's workplace/campus violence prevention programs.

2.4.1 Threat Assessment Team

The president will appoint a Threat Assessment Team and its chair. The team will include representatives from the Virginia Tech Police Department, Academic Affairs, Student Affairs, and Human Resources and a clinical psychologist from the University's Counseling Center. Legal counsel will serve as an advisor to the Threat Assessment Team. The team is charged with developing comprehensive fact-based assess-

ments of students, employees, or other individuals who may present a threat to the university and is empowered to take timely and appropriate action, consistent with university policy and applicable law.

2.5 Identifying and Reporting Risks

All individuals are encouraged to be alert to the possibility of violence on the part of employees, former employees, students, customers, and strangers. Employees and students shall place safety as their highest concern and shall report all acts of violence and threats of violence. All reports of violence will be handled in a confidential manner, with information released only on a need-to-know basis within the campus community and in accordance with federal and state laws and regulations. Management shall be sensitive and responsive to the potential for fear of reprisal by employees or students who report threats or acts of violence. This policy prohibits retaliation against any person who, in good faith, reports a violation of this policy. Every effort will be made to protect the safety and anonymity of anyone who comes forward with concerns about a threat or act of violence.

2.6 Responsibilities

It is the responsibility of every administrator, faculty member, staff member, and student to take any threat or violent act seriously and to report acts of violence or threats to the appropriate authorities as set forth in this policy. Department heads, directors, and supervisors are also responsible for communicating the policy to all employees under their supervision, ensuring that facilities are as safe as feasible, identifying and providing violence prevention training to employees as appropriate, and ensuring that all employees are aware of how to report potential threats. The Virginia Tech Police Department will coordinate all university action in case of a violent incident on campus or in the work place, establish and publish procedures for campus and workplace violence prevention and threat assessment, and investigate threats or incidents of violence. Only the Virginia Tech police or other law enforcement agencies should attempt to apprehend the alleged offender. Human Resources will coordinate employee-related preventive measures, including conducting criminal conviction checks in accordance with university policy, providing awareness programs to new employees, coordinating referrals to the employee assistance program, advising em-

ployees and managers, making referrals to the Threat Assessment Team and providing case management, and coordinating with other university and community resources to support victims of violence.

Student Affairs will coordinate student-related preventive measures including training for professionals, student employees (e.g., residence advisors), and students through the on-call process and through other education and training methods. The Office of Judicial Affairs is responsible for responding to and adjudicating violations of the University Policies for Student Life. Student Affairs will maintain the Care Team, the goal of which is to coordinate support services and administrative response to crises involving students, make referrals to the Threat Assessment team, and provide case management. The Office of Emergency Management (OEM) will develop and coordinate the university's emergency response plan, advise departments on the development of unit plans, provide templates to support the development of departmental plans, and coordinate emergency preparedness training for university administrators and departments in partnership with Student Affairs, University Relations, Virginia Tech Police Department, Environmental Health and Safety, Human Resources, and other offices. OEM will develop a plan for awareness and training programs for employees and students. The Virginia Tech Women's Center will respond to requests for assistance from staff, student, and faculty victims of violence or threats of violence by providing counseling, advocacy, safety planning, and other support as needed to victims of sexual assault, rape, dating or domestic violence, or other forms of campus or workplace violence. The center will coordinate services with on- and off-campus partners such as the Virginia Tech Police Department and other law enforcement agencies, the court system, the on-campus judicial process, medical and hospital services, and shelter services.

3. Procedures
3.1 Reporting Incidents

Any individual who believes there is an immediate danger to the health or safety of any member of the university community should call the Virginia Tech Police Department at 911. General questions about the Campus and Workplace Violence Prevention Policy should be directed to the Office of Emergency Management or the Virginia

Tech Police Department. Questions about specific issues may also be directed to

» Occupational Safety Division (EHSS) 540/231-5985
» Human Resources 540/231-9331
» University Legal Counsel 540/231-6293
» Virginia Tech Police Department 540/231-6411
» Virginia Tech Women's Center 540/231-7806
» Office of Judicial Affairs 540/231-3790
» Dean of Students Office 540/231-3787

3.2 Support for Victims of Violence

The university shall make efforts to provide a campus and workplace free from violence and to protect and support victims and those threatened or exposed to acts or threats of workplace violence by offering security measures and identifying appropriate resources for providing support and assistance. Victims may also need special accommodations or adjustments to their work or class schedule, location, or working conditions in order to enhance their safety. The university shall accommodate these requests and needs whenever possible and appropriate.

3.3 Security Planning for Potentially At-risk Employees and Students

Some employees can be at risk for violence/hostility because of the nature of their jobs. Other employees or students can be at risk because they are subject to violence, threats, or harassment from a current or former spouse or partner or other non-employee. The Virginia Tech Police Department, Human Resources, the Women's Center, and other offices will work with at-risk students, and employees and their supervisors, to develop safety plans that address the specific risks they face.

3.4 Pre-employment Screening and Criminal Conviction Checks

Human Resources administers the university's Policy 4060 Criminal Conviction and Drivers' Records and will work with hiring managers to ensure that sensitive positions are identified and criminal conviction checks conducted in accordance with the policy. Hiring managers are responsible for conducting pre-employment reference checks and advising Human Resources when potential problems are identified.

4. Definitions

An **at-risk individual** is defined as an employee, student, or other person who is a potential target or victim.

Assault is committed when one person 1) tries to or does physically strike another or 2) acts in a threatening manner to put another in fear of immediate harm. Aggravated assault is defined as a completed or attempted attack with a weapon and an attack without a weapon in which the victim is seriously injured.

Campus is defined as any location, either permanent or temporary, owned or leased by Virginia Tech. This includes, but is not limited to, the buildings, grounds, and the surrounding perimeters, including the parking lots, field locations, classrooms, residence halls, and alternate work or class locations.

A **credible threat of violence** is defined as a knowing and willful statement or course of conduct that would cause a reasonable person to believe that he or she is under threat of death or serious bodily injury. A course of conduct is any series of acts over a period of time, however short, that evidences a continuity of purpose, such as following or stalking an individual to or from the workplace/campus, telephone calls to the employee or student, and correspondence with the employee or student, whether by public or private mail, e-mail, interoffice mail, or fax.

Employee, for purposes of this policy, is defined as any salaried or wage faculty or staff member, graduate students paid on assistantships, and student workers.

Firearms are defined as any gun, rifle, pistol, or handgun designed to fire bullets, BBs, pellets, or shots, including paint balls, regardless of the propellant used.

Intimidation is engaging in actions that include, but are not limited to, stalking or behavior intended to frighten, coerce, or induce duress.

Physical Attack is unwanted or hostile physical contact such as hitting, fighting, pushing, shoving, or throwing objects.

Property Damage is intentional damage to property and includes property owned or leased by the university, employees, students, volunteers, visitors, or vendors.

Sexual assault is defined as any forcible sexual activity that occurs without the consent of the victim. It includes, but is not limited to, unwanted kissing and fondling; forcible vaginal, oral, or anal intercourse; and forcible penetration with an object or finger. Consent is an agreement reached without force, coercion, or intimidation between persons. Forcible sexual activity occurs when consent is not reached or when the victim is mentally incapacitated or physically helpless.

Stalking is defined as repeatedly contacting another person when the contact is unwanted. Additionally, the conduct may cause the other person reasonable apprehension of imminent physical harm or cause substantial impairment of the other person's ability to perform the activities of daily life. Contact includes but is not limited to communicating with (either in person, by phone, or by computer) or remaining in the physical presence of the other person.

Student is defined as any individual who has accepted an offer of admission as an undergraduate, graduate, or professional student and who has not yet graduated or officially transferred to another institution. If a student's enrollment lapses for more than one calendar year, the student will no longer be subject to disciplinary action under this policy.

Student employee is defined as any work-study student, student wage employee, or graduate student paid on an assistantship on the university payroll.

Third Parties are individuals who are not state employees or students, such as relatives, acquaintances, contractual workers, vendors, visitors, volunteers, customers, clients, or strangers.

Threat is the expression of intent to cause physical or mental harm. An expression constitutes a threat without regard to whether the party communicating the threat has the present ability to carry it out, and without regard to whether the expression is contingent, conditional, or future.

University facilities are any location, either permanent or temporary, owned or leased by Virginia Tech. This includes, but is not limited to, the buildings, grounds, and the surrounding perimeters, including the parking lots, field locations, classrooms, alternate work or class locations, and university owned or leased vehicles.

Victim is defined as an individual who has experienced or witnessed an act or acts of violence or threats of violence as outlined in this policy.

Violence includes, but is not limited to, intimidation, threats, physical attack, domestic violence, or property damage and includes acts of violence committed by university employees, students, clients, customers, relatives, acquaintances, or strangers against university employees in the workplace but does not include lawful acts of self-defense or the defense of others.

Weapons are defined as any instrument of combat or any object not designed as an instrument of combat but carried for the purpose of inflicting or threatening bodily injury. Examples include, but are not limited to, firearms, knives with fixed blades or pocket knives with blades longer than four inches, razors, metal knuckles, blackjacks, hatchets, bows and arrows, nun chahkas, foils, or any explosive or incendiary device.

Workplace is any location, either permanent or temporary, where an employee performs any work-related duty. This includes, but is not limited to, the buildings and the surrounding perimeters, including the parking lots, field locations, classrooms, alternate work locations, and travel to and from work assignments. It further includes university owned or leased vehicles.

Presidential Policy Memorandum 251 (see images of original two-page memo on pages 86 and 87); retrieved from *www.policies.vt.edu/policymemos/ppm251.pdf*

VirginiaTech

Charles W. Steger, President
210 Burruss Hall (0131)
Blacksburg, Virginia 24061
Office Phone: 540/231-6231 Fax: 540/231-4265
E-mail: president@vt.edu   www.vt.edu

PRESIDENTIAL POLICY MEMORANDUM NO. 251

TO: All Virginia Tech Employees and Students

FROM: Charles W. Steger

DATE: January 31, 2008

SUBJECT: Appointment of a University Threat Assessment Team

Approved by the President: December 10, 2007
Effective Date: Immediately
Expiration Date: Indefinite

Background

Following the tragic events of April 16, 2007, several reports were issued by Governor Kaine's independent Virginia Tech Review Panel and the three internal review committees that I appointed, which included recommendations for the designation of teams and/or advisory committees relating to violence prevention and/or response. In June 2005, the Virginia Tech Board of Visitors had approved the Campus and Workplace Violence Prevention Policy (Policy 5616), and in July 2005 a Campus Workplace Violence team was subsequently established. However, the Governor's Panel Report recommended specifically that all institutions for higher learning in Virginia have a threat assessment team that includes representatives from law enforcement, human resources, student affairs, academic affairs, legal counsel, and mental health functions.

For several months following the April 16 tragedy, the university had an ad hoc committee functioning as a threat assessment team. At my request, David Ford, Vice Provost for Academic Affairs, in consultation with Provost staff, Student Affairs, Police and Legal Counsel, subsequently developed a proposal for a formal threat assessment team structure. At the December 10, 2007 Policy Group meeting, the Policy Group reviewed and I approved the proposal to establish a single university threat assessment team that would serve both students and university employees.

Invent the Future

-2-

Composition and Charge of the Threat Assessment Team

Listed below are the positions that I have named to the Threat Assessment Team and the incumbents in those positions.   The Chief of the Virginia Tech Police Department serves as the Chair of the Team.

- Chief of Police (Team Chair) – Wendell Flinchum
- Dean of Students - Tom Brown
- Human Resources Representative – Pat Burton
- Student Affairs Representative – Rick Ferraro
- Clinical Psychologist Representative – Chris Flynn
- Academic Affairs Representative – David Ford
- Legal Counsel Representative – Kay Heidbreder
- Student Affairs Representative – Ed Spencer

Requests may be made to the President to adjust the permanent membership of the committee in the future if necessary. Also, when warranted for individual cases, the chair may request additional representatives from the Graduate School, Cranwell International Center and/or other university colleges/departments.

The Threat Assessment Team serves both students and employees and is charged with the task of convening, assessing the situation at hand, and taking immediate preventative action when a threat of imminent danger exists. The Team has full authority to act on behalf of the university and shall report all actions to me. The Team will proceed immediately to review existing teams at peer institutions, to establish team protocol, and to define and schedule appropriate team training. The Team will have read-only access to the CARE team electronic database, which shall be the sole repository for comprehensive information on at-risk students.

I greatly appreciate those appointed to the Threat Assessment Team serving the university in this important role.

#####

University Student Conduct System & Interim Suspension Policy
www.hokiehandbook.vt.edu/conductsystem

Interim Suspension Policy

The university retains the authority to impose an interim (immediate) suspension if such action is necessary to preserve the safety of persons or property. In this instance, the students will be afforded an interim suspension hearing and the opportunity to show why their continued presence on campus does not constitute a threat to themselves, others, or property. The interim suspension hearing is separate from a formal student conduct hearing. A formal student conduct hearing will be provided as soon as possible.

Students may be interimly suspended from the university or selected campus facilities with proper notice. The following steps explain the procedure for imposing an interim suspension:

1. When a situation, as defined above, occurs, the responding university official contacts the dean of students or his/her designee to assess the situation. If the situation is sufficiently serious, the dean of students, in consultation with others, can determine if an interim suspension hearing is necessary.

2. The interim suspension hearing will be held as quickly as possible and will be presided over and a decision rendered by the associate vice president for student affairs or his/her designee. The student, the responding university official, and other witnesses, as deemed appropriate by the dean of students or the associate vice president for student affairs, will attend the hearing. If the student is unable or unwilling to attend the hearing, depending upon the circumstances, the hearing may proceed without the student. During the hearing, the student will be given an opportunity to demonstrate why his or her continued presence on campus does not constitute a threat to himself or herself, others, or property. As part of the hearing, the student may be required to submit to an immediate medical/psychological evaluation. The evaluation may include a 24-hour period of observation. The student will be evaluated by the director

of the Cook Counseling Center or his/her designee. Results of this evaluation will be shared with the appropriate university officials. Agreeing to this evaluation does not preclude interim suspension, additional disciplinary action, or a decision to impose a medical withdrawal from the university. If the student agrees to an evaluation, the interim suspension may be delayed until the evaluation is completed.

3. Based on the outcome of the interim suspension hearing and/ or the evaluation, the student may be suspended from the university, medically withdrawn, and/or banned from selected campus facilities until a formal student conduct hearing can be convened. If a student is suspended, he or she will receive written notice of this decision by the associate vice president for student affairs or his/her designee. If interimly suspended, the student will be escorted out of the facility and/or off campus by a Virginia Tech police officer. The decision of interim suspension will be final. There will be no appeal.

4. The outcome of the interim suspension hearing will be shared with the Office of Student Conduct which will schedule, as soon as possible, a formal student conduct hearing to determine the final consequences of the initiating inappropriate behavior.

University Safety & Security Policy Structure

Virginia Polytechnic Institute and State University No. 5615 Rev.: 5
Policy and Procedures **Date: February 27, 2009**

Subject: University Safety and Security

1. Purpose

Virginia Polytechnic Institute and State University (Virginia Tech) is committed to the safety and welfare of students, faculty, staff and visitors through the establishment of reasonable practices that (1) support a safe and secure environment in all buildings and grounds owned, leased, and/or operated by Virginia Tech; (2) promote safety through policies and programs; (3) provide an appropriate level of security at university activities; and (4) safeguard the university's property and physical assets. The University Safety and Security Policy provides an overview of existing university safety and security policies and programs that demonstrate compliance with Sections 23-9.2:9-11 of the Code of Virginia and the Higher Education Act of 1965 as amended. This policy describes the authorities and responsibilities to carry out programs and operations that promote safety and security of individuals and property and establishes an operational committee for coordination and oversight of university safety and security policies and procedures. The policy also defines the specific responsibilities of the Virginia Tech Police Department (VTPD) and other university offices with responsibilities for campus safety and security, including compliance with the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act.

2. Policy

The university is committed to promoting the safety and security of the Virginia Tech community within a supportive and accessible living, learning, and working environment. It is further committed to safeguarding physical resources, identifying conditions or circumstances that may pose risks to the safety and security of the university, and preparing the university to effectively respond to emergencies.

University facilities must be used in a safe and appropriate manner so as not to endanger the university community or the general public. All faculty, staff, students, and other members of the Virginia Tech community share responsibility for the safety and security of the institution and must conduct university activities and operations in compliance with applicable federal and state regulations and university policies.

2.1 Authorities and Responsibilities

By state statute, the Virginia Tech Board of Visitors is charged with the care, preservation, and improvement of university property and with the protection and safety of students, faculty, and staff on university property. As part of an institution-wide commitment to a safe and secure campus, the university has established offices specifically charged with security and safety responsibilities and created a committee structure to provide general oversight and leadership for the university's security, safety, and violence prevention efforts.

2.1.1 Committee Structure

Safety and Security Policy Committee: The University Safety and Security Policy Committee is an operational committee appointed by the president to serve as a coordinating and policy body, with responsibilities for establishing the framework for an overarching university safety, emergency management, and security program for all Virginia Tech facilities (on and off campus, owned, and leased) and ensuring that it is implemented through the appropriate offices; evaluating the overall safety and security infrastructure; and providing oversight to the work of university operational committees responsible for environmental health and safety, violence prevention, emergency management, and other safety and security related efforts. The committee also serves as the Emergency Response Policy Group as defined in Virginia Tech's Emergency Response Plan. The members of the committee will hold senior administrative roles with the authority to make policy decisions and commit resources in the core operational areas that are generally responsible for the safety and security of the campus community. The committee is chaired by the president; in the president's absence, the committee is chaired by the vice president for administrative services. University legal counsel will serve as an advisor to the committee.

Specific committee responsibilities include

» Reviewing, evaluating, and determining requirements concerning safety and security assessments, plans, programs, and education, including changes that may affect the quality of the university's living, learning, and working environment;

» Overseeing reviews of the university's assessment of vulnerabilities, hazards, and risks related to the safety and security of individuals and the physical campus;

» Ensuring that sufficient university resources and funding are available to perform necessary emergency management, safety, and security functions and that these resources are consistent with anticipated regulatory changes;

» Overseeing the education and prevention of violence on campus in accordance with Section 23-9.2:10 of Code of Virginia, including providing direction to the Campus and Workplace Violence

Prevention Committee and the Threat Assessment Team on the development and implementation of violence prevention policies, procedures, education, and guidance regarding recognition and reporting of individuals whose behavior may pose a threat, assessment of such individuals, and means of action to resolve potential threats;

» Overseeing the Safety and Security Policy and other policies that have implications for emergency management, safety, and security, including, but not limited to, facilities use, sponsorship of entertainment and events, threatening or intimidating conduct, facilities access control, environmental health and safety, and violence prevention;

» Reviewing and establishing guidelines and standards for departmental emergency response and continuity of operations plans;

» Evaluating the effectiveness of the university's safety and security plans and programs; and

» Advising the president on safety and security issues.

Threat Assessment Team: The Threat Assessment Team, established by the president through President's Policy Memorandum #251 (Appointment of a University Threat Assessment Team) in accordance with Section 23-9.2:10 of the Code of Virginia, serves the entire university community, including visitors and guests. The team reports to the Safety and Security Policy Committee, which is chaired by the president and is responsible for implementing assessment, intervention, and action policies to assess individuals whose behaviors may present a campus threat. Campus and Workplace Violence Prevention Committee: The Violence Prevention Committee is an operational committee established by university Policy 5616, Campus and Workplace Violence Prevention, and is one of the components of the violence prevention committee structure approved by the board of visitors in accordance with the provisions of Section 23-9.2:10 of the Code of Virginia. The committee is appointed by the vice president for administrative services and reports to the Safety and Security Policy Committee. It is charged with education and prevention of violence on campus and is

responsible for developing and implementing threat assessment; violence prevention; and education procedures, programs, and guidance. The committee has oversight responsibilities for university compliance with Policy 5616, Campus and Workplace Violence Prevention. Health and Safety Committee: The Health and Safety Committee is an operational committee established by university Policy 1005, Health and Safety, with the authority to oversee university compliance with health and safety policies. The committee is appointed by the vice president for administrative services and reports to the Safety and Security Policy Committee. Emergency Management and Risk Assessment Committee: The Emergency Management and Risk Assessment Committee is an operational committee, appointed by the vice president for administrative services and reporting to the Safety and Security Policy Committee. It is responsible for oversight of emergency management and risk assessment activities, programs, and initiatives. The committee will continually evaluate the needs of the university, developing appropriate planning, programmatic response, and mitigation strategies designed to reduce risks and to continually improve the disaster resiliency of Virginia Tech.

2.1.2 Virginia Tech Departments and Offices with Safety and Security Responsibilities

The university's commitment to the safety and welfare of the university community is demonstrated by an organizational and programmatic structure that defines the authorities and responsibilities of university departments to carry out programs and operations that promote the safety and security of individuals and property. Major units reporting to the vice president for student affairs and the vice president for administrative services provide related support functions and direct services. The Office of Research Compliance, reporting to the vice president for research, oversees university community compliance with applicable laws, regulations, and guidelines associated with research and teaching. Those departments with primary safety and security roles are described below. Virginia Tech Police Department (VTPD): The VTPD is a full-service, nationally accredited law enforcement agency empowered by the Code of Virginia to enforce federal, state, and local laws; to make arrests; conduct criminal investigations; and perform other law enforcement activities. VTPD has concurrent

jurisdiction in designated areas with law enforcement agencies in Montgomery County and the towns of Christiansburg and Blacksburg and has the same authority as law enforcement agencies in the county and towns. The VTPD's Directives Manual delineates the character of working relationships with other law enforcement agencies. The VTPD responds to and investigates alleged criminal offenses on property owned or leased by the university. The university, through its police department, monitors and records student off-campus criminal activity, including student organizations with off-campus housing, by communicating and assisting local law enforcement, as needed. The annual crime statistics report required by the Clery Act is published by the VTPD (see section 2.2.1 Federal Directives). The VTPD is responsible for implementing and administering any security policy or procedure that is on university property.

Offices of Housing & Dining Services and Residence Life: The Offices of Housing & Dining Services and Residence Life in Student Affairs allocate resources necessary to ensure the safety and security of campus residence halls. Resident advisors will be trained to be security conscious and should be alert to propped security doors, acts of vandalism, and unauthorized guests. Resident advisors are also trained to perform safety audits of residence rooms, coordinate emergency evacuation and warning procedures, and facilitate the performance of fire and other drills. Women's Center: The Women's Center is the primary department that provides crisis intervention, counseling, and advocacy services to students, faculty, and staff who have been affected by sexual assault, relationship violence, stalking, cyberstalking, and harassment. The Women's Center is also responsible for providing outreach and education to the campus community on violence against women issues and reviewing campus policies related to these issues. The Women's Center provides anonymous information to the Virginia Tech Police Department on crimes that occur on campus or off campus in a facility owned or operated by a registered student organization that have not been reported to the Office of Judicial Affairs. Office of Insurance and Risk Management: The Insurance and Risk Management Office handles all insurance matters, including claims and liability risk evaluations for university activities. It provides evaluation and training in risk management and insurance on behalf of Virginia Tech and

its corporations. It has specific responsibility for current property and casualty insurance policies and coverage for Virginia Tech property and automobiles. It has further responsibility to administer the property, general liability, automobile, boiler and machinery, medical malpractice, and related insurance programs of Virginia Tech and associated claims. Environmental Health and Safety Services (EHSS): EHSS develops policies, programs, and training to support university compliance with federal and state laws, regulations, and standards. EHSS supports university efforts to identify, evaluate, and control hazards, including environmental monitoring services, waste disposal, industrial hygiene monitoring, and the evaluation and management of potential health and safety hazards. EHSS evaluates safety risks and provides training to faculty, staff, and students to reduce the risk of accident, injury or illness, fires, hazardous materials incidents, and laboratory accidents. The EHSS department also collects statistics for the annual fire safety report provided as part of the police department's annual report (see section 2.2.1 Federal Directives). Office of Emergency Management (OEM): The Office of Emergency Management is responsible for the implementation and coordination of emergency management efforts for the university, including developing, testing, and maintaining the university's hazard mitigation, emergency preparedness, and continuity of operations plans. Additional responsibilities of OEM include scheduling and coordinating tests of emergency response and evacuation procedures on an annual basis; activating and coordinating the university's emergency operations center; developing protocols and procedures relating to emergency management; designing and coordinating training and exercises; serving as a liaison with federal, state, and community emergency organizations; creating a comprehensive emergency preparedness and response communications and awareness program for employees and students; and coordinating and guiding the efforts of employees who are assigned unit emergency management responsibilities. OEM will work with Police, Environmental Health and Safety, Facilities, and other offices to coordinate risk, safety, and security assessments of campus facilities and programs and will provide reports and recommendations to management and the University Safety and Security Policy Committee. Internal Audit: The Internal Audit Department reviews access control/key control and

limited aspects of physical security and health and safety as part of its risk-based audits and compliance reviews to ensure that the auditee department is in compliance with the university, state, and/or federal regulations. Any audit findings and recommendations are addressed directly to the auditee and may be included in the audit report, which is submitted to and reviewed by the board of visitors.

2.1.3 Departmental and Individual Responsibilities

Departmental responsibilities: Directors/department heads, and individuals in supervisory roles are responsible for ensuring that personnel within their departments are aware of safety and security policies and the procedures for reporting safety problems, accidents, emergencies, crimes, and threats. They are also responsible for ensuring that emergency preparedness and continuity of operations plans are developed in accordance with university guidelines and communicated to all personnel in order to ensure familiarity with and coordination between departmental personnel and emergency responders. In compliance with the university's Emergency Response and Continuity of Operations plans, departments are responsible for developing internal procedures to communicate with members of their departments. Departmental supervisors are responsible for implementing security and safety policies and programs in work areas under their supervision/control. Individual responsibilities: Individuals are responsible for being aware of and complying with university policies and procedures, and applicable law. Employees and students also have an obligation to accurately and promptly report crimes, emergencies, potential threats, or risks to the appropriate university office(s). Numerous employee and student policies outline responsibilities and acceptable behavior, and standards of conduct. Violations of university policy are subject to the disciplinary actions under the appropriate faculty, staff, and student policies, up to and including dismissal. The conduct of students is covered, in depth, by the University Policies for Student Life. Each fall semester, employees and students are made aware of safety and security policies and procedures through the "Annual Notice on Community Standards – Health, Safety, and Security" that is e-mailed by Student Affairs, Human Resources, and the Virginia Tech Police Department to all members of the university community.

2.2 Federal and State Directives and University Policies

In addition to a strong campus law enforcement program, the university has implemented a number of measures that comply with federal and state directives to promote campus safety and security.

2.2.1 Federal Directives

The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act): The Clery Act defines the specific responsibilities for colleges and universities to make the campus community aware of crimes that have occurred and necessitate caution on the part of students and employees, and for providing annual reports on campus crime statistics. As required by the act, "immediate notifications" will be provided to the community in the event that a situation arises, either on campus or off, that, in the judgment of the chief of the VTPD, constitutes an ongoing or continuing threat. Section 2.4.2 of this policy describes the methods used to provide emergency notifications. The warning may be issued through the use of a variety of sources, which may include, but are not limited to, VT Alerts, the university e-mail system, posters, university website, or phone mail systems. Depending on the particular circumstances of the crime, especially in all situations that could pose an immediate threat to the community and individuals, University Relations may also post a notice on the Virginia Tech homepage or utilize the VT Alerts automated notification system.

The chief of the VTPD will be responsible for publishing annual crime statistics as required by the Clery Act, as well as the number of arrests and judicial referrals for alcohol, drug, and weapons violations. Annual statistics on hate crimes will also be published for larcenies, vandalisms, simple assaults, and intimidation, as well as any other crime involving bodily injury to a person in which the victim is intentionally selected because of the actual or perceived gender, religion, sexual orientation, ethnicity, or disability. The chief of the VTPD must also publish and make generally available to all current students and employees an annual report of campus security policies and crime statistics (covering the reporting period January 1 to December 31) and make copies of this annual report available to any prospective student or employee. Crime statistics are available for both the main campus in

Blacksburg and off-site instruction locations. This information is available both in hard copy and on the VTPD website. Crime statistics are gathered based on reports provided to campus security authorities, including VTPD, Judicial Affairs Office, Office of Residence Life, Virginia Tech Women's Center, and the Dean of Student's Office. Statistics are also gathered from law enforcement jurisdictions in which Virginia Tech owns, leases, or controls property or those with jurisdiction on adjacent property. The Higher Education Act of 1965 as amended: University emergency management procedures comply with the provisions of this act, including statements of campus policies for emergency response and publication of evacuation procedures; emergency communications and timely notifications in the event of a significant emergency or dangerous situation involving an immediate threat to the health or safety of students or staff occurring on campus and testing of emergency evacuation procedures on an annual basis. Campus Fire Safety Right-to-Know Act (as included in The Higher Education Opportunity Act): Annual fire safety reporting to the campus community, prospective students, and the secretary of education is required. The annual fire safety report will include both data from a log of fire related events over the last two years as well as other campus fire safety information. Statistics will be collected by EHSS and reported by the Virginia Tech Police Department with the crime statistics as part of the police department's annual report.

2.2.2 State Directives and Policies

University policies, programs, and procedures comply with Commonwealth of Virginia Executive Order 44 (2007) Establishing Preparedness Initiatives in State Government, state personnel policies including Policy 1.80 Workplace Violence, and Sections 23-9.2:3 and 23-9.2:9-11 of the Code of Virginia, as amended.

2.2.3 University Policies

The university has established policies that specifically address environmental and occupational safety, violence prevention, and employment practices. There are additional policies that cover authorized and emergency closings, safeguarding institutional assets and information, prohibited conduct regarding alcohol and drugs, anti-discrimination and harassment prevention, and student life. A comprehensive listing

of related policies is provided in Section 5.0, References. Health and Safety: Policy 1005, Health and Safety, establishes responsibilities for preventing job-related accidents, illnesses, and injuries; increasing safety awareness; meeting requirements of environmental, occupational health, and safety laws and regulations; and reducing institutional liability. It also describes the safety responsibilities for members of the university community and visitors to university-owned or occupied property. Violence prevention: In accordance with Section 23-9.2:10 of the Code of Virginia and Commonwealth of Virginia Policy 1.80 Workplace Violence, the university has established policies and procedures for the prevention of violence on campus. Policy 5616, Campus and Workplace Violence Prevention, specifically addresses the university's position on the prevention, reduction, and management of violence to provide a safe working and learning environment for our students, employees, and visitors at all university owned, controlled, or leased properties, including satellite locations. Policy 4345, Employee Assistance Program, University Policies for Student Life, and Care Team and Threat Assessment Team protocols provide policies and procedures for the assessment and intervention with individuals whose behaviors may pose a threat to themselves and/or the campus community. Faculty and staff hiring procedures: Policy 4060, Background and Driving Record Investigation, addresses the use of criminal background and driving record checks during the employment process. Applicants for faculty and staff positions are required to answer questions regarding previous convictions. Criminal background and/or driving record checks are conducted on candidates selected for certain wage and salaried positions as a condition of employment. Determination of either a job-related conviction or falsified conviction information on the application may result in denial or forfeiture of university employment. Certain positions may be designated as safety-sensitive and may be subject to additional provisions. Policy 4330, Guidelines for the Use of Volunteers, provides for conviction checks for volunteers performing security sensitive duties and defines the liability coverage for volunteers.

Student enrollment application procedures: Applicants for admission to Virginia Tech's undergraduate, graduate, and College of Veterinary Medicine programs must complete specific questions regarding prior

disciplinary actions in high school, college, or university; juvenile and adult arrests and convictions; court-ordered supervised or unsupervised probation; or under the terms of a finding under advisement.

2.2.4 Safety and Security Programs

University offices provide programs to aid departments and individuals in understanding their responsibilities to be aware of and comply with safety and security policies and procedures and with applicable law. Programs to inform students and employees about campus crime prevention, and safety and security and to encourage individuals to be responsible for their own safety and to report conditions that affect the safety and security of others are offered on a regular basis. Informational materials, adapted for student and employee audiences, are provided in presentations and print and electronic formats.

2.2.5 Facilities Design Standards and Building Access Control

Security and access control design standards have been developed for new and renovated buildings owned by the university. Designs are reviewed by the VTPD for compliance with security requirements. The VTPD will evaluate the Offices of Housing & Dining Services and Residence Life security measures to ensure residence hall security. Entrances to residence floors shall be locked at all times. Exterior doors in all residence hall buildings shall remain locked except in those buildings that house university offices. In addition, exterior entrances are allowed to be unlocked during official move-in hours each fall. Residents of the building and their escorted guests, as well as authorized persons, access the building by utilizing the card access system. Resident advisors (RAs) and Campus Watch Security make rounds during evening hours to verify that exterior entrances are locked and secured. Academic and administrative buildings are open to the public during operating hours and are generally secured after operating hours and during extended breaks. Policy 5620, Access Control/Key Control, defines how keys to university buildings will be issued, monitored, and maintained. The Key Control Office in Facilities Services and the VTPD implement and oversee access and key control procedures.

2.3 Use of University Facilities

Virginia Tech sponsors or hosts numerous programs, events, and

activities or allows its facilities to be used for programs, events, and activities. The event planner is responsible for coordinating with the appropriate university offices (e.g., Virginia Tech Police Department, Office of Emergency Management, Risk Management, and University Unions and Student Activities Event Planning Office) to ensure that appropriate arrangements are made for event security, emergency planning, and liability. Departments are responsible for notifying the VTPD of events occurring in their facility/space. The VTPD is responsible for determining the appropriate security for events. The Office of Insurance and Risk Management provides guidance on the planning, documentation, and training activities that demonstrate duty of care, as well as assistance with certificates of insurance for events. Other university policies that provide guidance for events or programs include but are not limited to

» Policy 5000, University Facilities Usage and Event Approval – provides guidelines for the use of university facilities for activities sponsored by registered student organizations, university departments, university-associated organizations and non-university groups or organizations.

» Policy 5010, Summer Conferences – provides guidelines for summer programs held on the Virginia Tech campus in residence and dining halls.

» Policy 8215, Major Entertainment Sponsorship – the Department of Student Activities determines the conditions and criteria, including safety and security, under which major entertainment events may be sponsored at Virginia Tech.

» Policy 8220, Security Requirements for Events Sponsored by Student Organizations – requires advanced planning to ensure adequate security to protect students and guests during events sponsored by student organizations.

2.4 Emergency Preparedness and Response
Virginia Tech's emergency management plans and programs address mitigation and prevention, preparedness, response, and recovery. The plans describe management structures, emphasize preparedness, and

identify interdependencies of functional areas and external partners. In compliance with the Higher Education Act of 1965 as amended, Virginia Tech's emergency preparedness and response procedures established by the Office of Emergency Management and outlined in the Emergency Response Plan provide for

» Immediate notification of the campus community upon the confirmation of a significant emergency or dangerous situation involving an immediate threat to the health or safety of students or staff occurring on the campus, unless issuing a notification will compromise efforts to contain the emergency;

» Annually publicizing emergency response and evacuation procedures using methods appropriate to reach students and employees; and

» Annually testing emergency response and evacuation procedures.

2.4.1 Emergency Management Plans
In accordance with Executive Order 44(2007) Establishing Preparedness Initiatives in State Government and Section 23-9.2:9 of the Code of Virginia, the university shall develop, adopt, and keep current a written crisis and emergency management plan; every four years the university shall conduct a comprehensive review and revision of its plan, which shall be adopted formally by the Virginia Tech Board of Visitors. It is the responsibility of the Office of Emergency Management to oversee the review and update of these plans. Procedures to guide departments in developing emergency preparedness and continuity of operations plans are established by the university's Office of Emergency Management to be consistent with federal and state requirements. Departments are responsible for maintaining these plans in accordance with university guidelines and timelines.

Hazard Mitigation Plan: The university's Hazard Mitigation Plan was approved by the Federal Emergency Management Agency (FEMA) in October 2006. The plan includes an analysis of natural and man-made hazards and the development of policies, programs, and practices to assess and mitigate these risks.

Continuity of Operations Plan (COOP): The university's Continuity of Operations Plan (COOP) establishes operational and restoration procedures for essential functions. The university plan focuses on basic COOP elements: management framework, essential functions, critical systems, alternate facilities, orders of succession, delegations of authority, and vital records. The university's COOP must be updated annually.

Emergency Response Plan: The Emergency Response Plan (ERP) establishes a management framework and outlines procedures for managing major emergencies that may threaten the health and safety of the campus community or disrupt business operations on the Blacksburg campus. The university's ERP must be updated annually. Every four years, the university must conduct a comprehensive review and revision of its emergency management plan, and the revised plan must be adopted formally by the board of visitors and certified in writing to the Virginia Department of Emergency Management in accordance with Section 23-9.2.9 of the Code of Virginia.

2.4.2 Emergency Communications

In accordance with the Higher Education Act of 1965 as amended and Section 23-9.2:11 of the Code of Virginia, the university has implemented a comprehensive communications system to provide prompt warning notifications and alerts of emergencies or threats to the campus community using a variety of methods, including but not limited to e-mail notices; phone, cellular phone, and text messages; alert lines; classroom electronic message signs; posters; university website notices; and other methods. Depending on the particular circumstances, especially in all situations that could pose an immediate threat to the community and individuals, University Relations may utilize the "VT Alerts" automated notification system. The Office of University Relations and/or VTPD will notify the campus community of emergencies or crimes that have occurred and necessitate caution, evacuation, or other action on the part of students, employees, and campus visitors. Annually, the Offices of University Relations and Human Resources provide communications to the university community regarding university procedures for authorized closings and receiving emergency alerts.

3. Procedures

Individual employees and students have an obligation to accurately and promptly report crimes, emergencies, potential threats, or risks to the appropriate university office(s). Detailed procedures are included in the policies referenced in the body of this policy, the additional related policies included in section 5.0 References, and on the websites of the university offices engaged in supporting campus safety and security.

CRIMES: Virginia Tech encourages the community to report all crimes to the Virginia Tech Police Department at 911 for emergencies and 231-6411 for non-emergencies. Certain crimes may be reported online at *www.police.vt.edu*. Voluntary confidential and/or anonymous reporting is available at stopabuse.vt.edu or by using the TIPS crimeline at 232-TIPS.

DISTRESSED EMPLOYEES: Concerns about the behavior of or statements made by Virginia Tech employees including teaching and research faculty employees, administrative or professional employees, classified and university employees, and wage employees may be reported to Human Resources at 540/231-9331. Matters needing immediate attention should be directed to the Virginia Tech Police Department at 540/231-6411.

DISTRESSED STUDENTS: The Dean of Students Office takes reports of students who may be in distress. The dean of students reporting system allows faculty members and critical staff members identified by department heads to submit information about a student whose exhibited behaviors or statements may be of concern (in or outside the classroom). Contact may be made by phone (540/231-3787) or the reporting system available within the Hokie SPA/Faculty Access menu. Matters needing immediate attention should be directed to the Virginia Tech Police Department at 540/231-6411.

EMERGENCIES OR PERSONS OF CONCERN: Students, faculty, staff, and visitors may report emergencies, criminal actions, and suspicious behavior to the Virginia Tech Police Department by dialing 911 from any campus phone or by activating the blue emergency phones located on campus. It should be noted that if 911 is dialed from a cellular phone

or pay phone, the call will be routed to an off-campus police department or dispatch center. If this should occur, the caller should describe the nature of the emergency to the dispatcher and ask to have the call transferred to the Virginia Tech Police Department. In order to avoid this type of delay, campus patrons may consider programming cellular phones to the Virginia Tech Police Department at 540/231-6411. All non-emergency calls to the Virginia Tech police should also be directed to 540/231-6411. Virginia Tech personnel who work at off-campus sites should inquire with local officials about the proper procedures for requesting emergency assistance, including the use of cellular phones. Most Virginia locations use 911 for emergency calls. However, use of cellular phones at off-campus sites to request emergency assistance may involve delays similar to those described above, depending on how the call is routed.

INCIDENTS INVOLVING PROPERTY, AUTOMOBILES, OR POTENTIAL PUBLIC LIABILITY: All incidents involving university property, automobiles, or potential public liability should be reported to Risk Management as outlined on the Risk Management website. (*www.controller.vt.edu/Risk*)

WORKPLACE ACCIDENTS, INJURIES, OR ILLNESSES: An injured employee is required to immediately report an accident or illness to the direct supervisor. Upon the employee's notification of the injury to the departmental supervisor, the department is required to offer the employee a Workers Compensation Panel of Physicians. Those employees needing immediate medical treatment for serious injuries may visit the emergency room and will need to report the injury as Workers' Compensation at the time treatment is received. Once an employee reports a job-related injury, the supervisor must immediately file the Employer's Accident Report, Form VWC No. 3 with Human Resources within 24 hours of the date/time of the injury (see *www.hr.vt.edu/benefits/workerscomp/index.html* for procedures and contact information).

OTHER RESOURCES FOR REPORTING:
SafeWatch: Online means for identifying and anonymously reporting violations of university policies and community expectations related

to harassment, discrimination, or similar behaviors. (*www.safewatch.vt.edu/form.html*)

Stop Abuse: Individuals may contact Stop Abuse at the Virginia Tech's Women's Center (540/231-7806) regarding concerns about sexual assault, relationship violence, stalking, cyberstalking/online harassment, and sexual harassment. If help or support is needed after 5 p.m. during the week or on the weekend, the Women's Resource Center of the New River Valley's 24-hour hotline at 540/639-1123 should be used.

4. Definitions

Physical Campus: All buildings and grounds owned, leased, and/or operated by Virginia Tech. Risk Assessment: The process of identifying types of risks or hazards that could affect the institution, including (1) Hazard Identification, the determination of potential risks, hazard events, or liabilities; (2) Hazard Characterization, the evaluation of which personnel, property, income, or assets are most vulnerable to injury or damage from these hazards by severity and frequency; (3) Hazard Exposure Assessment, estimation of potential losses; and (4) Risk Characterization, the prioritization of various risk exposures.

Risk Management: The policies, procedures, and practices associated with the identification, analysis, and assessment of risk exposures and appropriate strategies to eliminate, control, minimize, or avoid unacceptable risks. Control strategies may include risk assumption, risk avoidance, risk retention, risk transfer, or any other strategy or combination of strategies to manage future events. Threat Assessment: A fact-based investigative, analytical approach that evaluates whether an individual's behavior poses a risk to his or her safety or the safety of others. The appraisal of risk in a given situation should focus on an individual's actions, communications, and specific circumstances that might suggest that an individual intends to commit a violent act and/or is engaged in planning or preparing for that event.

5. References

Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act Commonwealth of Virginia's Policy 1.80 Workplace Violence Commonwealth of Virginia Policy 2.30 Workplace Harassment. Drug-Free Workplace Act of 1988 Code of Virginia, Sections 23-9.2:3

and 23-9.2:9-11 Governor's Executive Order 44 (2007) Higher Education Act of 1965 as amended University Policies: Health, Safety, Violence Prevention Policies 1005 Health and Safety Policy 5616 Campus and Workplace Violence Prevention Policy Presidential Policy Memorandum 251: Appointment of University Threat Assessment Team Individual Conduct (or Prohibited Conduct) 1015 Alcohol Policy 1020 Policy on a Drug-Free University 1025 Anti-Discrimination and Harassment Prevention Policy 1035 Student-Athlete Conduct 1036 Student-Athlete Substance Abuse Policy 8300 University Policies for Student Life Classified and University Staff Policies and Handbook Faculty Handbook and Special Research Faculty Handbook Reporting and Investigation 4060 Background and Driving Record Investigation 4061 Drug and Alcohol Guidelines for Commercial Drivers' License Holders 4330 Guidelines for the Use of Volunteers 5600 Response to Bomb Threats 7035 Privacy Policy for Employees' Electronic Communications Security Arrangements 5000 University Facilities Usage and Event Approval 5010 Summer Conferences 5403 Policy on Employee Housing 5500 State Vehicle Management 5605 Residence Hall Fire and Fire Alarm Procedures 5620 Access Control: Key Control Policy 5610 Policy on Animal Escape Notification 8215 Major Entertainment Sponsorship 8220 Security Requirements for Events Sponsored by Student Organizations

Virginia Tech Safety & Security Committee Structure

BOV
- Approves Emergency Management Plan
- Approves committee structure for education & prevention of violence

President

University Safety & Security Policy Committee
- Chaired by president; in his absence, chaired by vice president for administrative services
- Provides general oversight of operational committees responsible for safety, security, emergency management, & violence prevention to support coordination & compliance
- Reviews, evaluates, & determines requirements concerning safety & security assessments, plans, & programs for all Virginia Tech facilities (on & off campus, owned & leased)
- Provides direction on development of violence prevention policies, procedures, education, & guidance regarding recognition & reporting of individuals whose behavior may pose a threat, assessment of such individuals, & means of action to resolve potential threats
- Ensures that sufficient university resources & funding are available to perform necessary emergency management, safety, & security functions & that these resources are consistent with anticipated regulatory changes
- Oversees Safety & Security Policy & other policies that have implications for safety & security including but not limited to facilities use, sponsorship of entertainment & events, threatening or intimidating conduct, facilities access control, environmental health & safety, & campus violence prevention
- Serves as Emergency Response Policy Group under Virginia Tech's Emergency Response Plan

Emergency Management & Risk Assessment Committee
- Chaired by director of emergency management
- Provides oversight, coordination, & leadership for risk assessments & promotion of activities & services that reduce or eliminate risks
- Prepares the university through emergency planning efforts, training, & exercises
- Develops coordinated & effective emergency response capabilities

Health & Safety Committee
- Chaired by director of EHSS
- Oversees implementation & compliance with Health & Safety Policy

Campus & Workplace Violence Prevention Committee
- Chaired by police chief or designee
- Develops & implements violence prevention & education procedures, programs, & guidance; publishes statement of mission, membership, & leadership
- Oversees implementation & compliance with Violence Prevention Policy

Threat Assessment Team
- Chaired by police chief or designee
- Implements assessment, intervention, & action policies for individuals whose behaviors may present a threat to the safety of the campus community; works with enforcement & mental health agencies to expedite assessment & intervention

VPAS (Feb 2009)

APPENDIX C

List of Interviewees

Appendix C: List of Interviewees

Interviews with University Leaders and Threat Assessment Team Members for Demonstration Project Book:

» Brown, James Tomas: Dean of Students

» Burton, Patricia: Employee Relations Manager

» Ferraro, Richard: Assistant Vice President for Student Affairs

» Flinchum, Wendell: Chief of Police

» Flynn, Chris: Director, Cook Counseling Center

» Heidbreder, Kay: University Legal Counsel

» Hincker, Larry: Associate Vice President, University Relations

» Hyer, Patricia: Associate Provost for Academic Administration

» Keene, Frances: Director, Office of Student Conduct

» McNamee, Mark: Senior Vice President & Provost

» Modzeleski, William: Associate Assistant Deputy Secretary of the U.S. Department of Education's Office of Safe and Drug Free Schools

» O'Rourke, Kim: Chief of Staff, Office of the President

» Plummer, Ellen: Assistant Provost

» Reineke, Emily: Threat Assessment Team & Victim Services Special Projects Coordinator

» Spencer, Edward: Vice President for Student Affairs

» Steger, Charles: President

» Woodard, Linda: Assistant Vice President for Administrative Services & Chief of Staff

Supplemental Interviews:

» Davis, Sharrika: Associate Dean of Students

» Dean, Wanda: University Registrar

» Wubah, Daniel: Vice President & Dean for Undergraduate Education

APPENDIX D

Additional Resources

Appendix D: Additional Resources

References and Suggested Readings:[1]

Association of Threat Assessment Professionals (2006). *Risk assessment guideline elements for violence: Considerations for assessing the risk of future violent behavior.* Los Angeles: Authors.

Braverman, M. (1999). *Preventing workplace violence: A guide for employers and practitioners.* London: Sage.

Calhoun, F.S. & Weston, S.W. (2003). *Contemporary threat management: A practical guide for identifying, assessing and managing individuals of violent intent.* San Diego: Specialized Training Services.

Corcoran, M.H. & Cawood, J.S. (2003). *Violence assessment and intervention: The practitioner's handbook.* New York: CRC.

DeBecker, G. (1997). *The gift of fear: And other survival signals that protect us from violence.* New York: Dell.

Deisinger, G., Randazzo, M., O'Neill, D., & Savage, J. (2008). *The Handbook for Campus Threat Assessment and Management Teams.* Stoneham, Mass.: Applied Risk Management.

Dunkle, J., Silverstein, Z., & Warner, S. (2008). "Managing violent and other troubling students: The role of threat assessment on campus." *Journal of College and University Law, 34*(3).

Fein, R., Vossekuil, B., Pollack, W., Borum, R., Modzeleski, W., & Reddy, M. (2002). *Threat assessment in schools: A guide to managing threatening situations and to creating safe school climates.* Washington, D.C.: U.S. Department of Education and U.S. Secret Service.

Flannery, R.B. (1995). *Violence in the workplace.* New York: Crossroad.

---

1 This list modified from *The Handbook for Campus Threat Assessment and Management Teams* (Deisinger, Randazzo, O'Neill, & Savage, 2008).

Frueh, B.C., Grubaugh, A.L., Yeager, D.E., & Magruder, K.M. (2009). "Delayed-onset post-traumatic stress disorder among war veterans in primary care clinics." *The British Journal of Psychiatry, 194.*

Hoffman, A.M., Schuh, J.H., & Fenske, R.H. (Eds.) (1998). *Violence on campus: Defining the problems, strategies for action.* Gaithersburg, Md.: Aspen.

Hughes, M.H., Jones, R.T., Kessler, R.C., Fairbank, J.A., Pynoos, S., Steinberg, A.M., Brymer, M., Rothwell, V. (2009, in preparation). *Mental Health Needs Assessment in the Aftermath of the April 16 Events at Virginia Tech, A Brief Preliminary Report.*

International Association of Campus Law Enforcement Administrators (1993). *Handling institutional violence on campus.* Hartford, Conn.: IACLEA.

International Association of Campus Law Enforcement Administrators (1996). *Handling violence in the workplace.* Hartford, Conn.: IACLEA.

International Association of Campus Law Enforcement Administrators (2008). *Overview of the Virginia Tech Tragedy and Implications for Campus Safety: The IACLEA Blueprint for Safer Campuses.* Hartford, Conn.: IACLEA.

Lazenby, R. (Ed.) (2007). *April 16: Virginia Tech remembers.* New York: Plume.

Leavitt, M., Gonzales, A., & Spellings, M. (2007). *Report to the President: On Issues Raised by the Virginia Tech Tragedy.* Washington, D.C.: U.S. Department of Justice.

Meloy, J.R. (2000). *Violence risk and threat assessment.* San Diego: Specialized Training Services.

Missouri Campus Security Task Force (2007). *Securing our Future: Making Colleges and Universities Safe Places to Learn and Grow.* Jefferson City, Mo.: Author.

Mohandie, K. (2000). *School violence threat management.* San Diego: Specialized Training Services.

Monahan, J., Steadman, H.J., Silver, E., & Applebaum, P.S. (2001). *Rethinking risk assessment: The MacArthur study of mental disorder and violence.* New York: Oxford.

Monahan, J. (1995). *The clinical prediction of violent behavior.* London: J. Aronson.

Oklahoma Governor's Task Force on Campus Life and Safety and Security (2008). *Final Report.* Oklahoma City, OK: Author.

O'Neill, D., Fox, J., Depue, R., Englander, E., et al. (2008). *Campus violence prevention and response: Best practices for Massachusetts higher education.* Boston, Mass.: Massachusetts Department of Higher Education.

National Association of Attorneys General (2007). *Report and Recommendations of Task Force on School and Campus Safety.* Washington, D.C.: Author.

New Jersey Campus Security Task Force (2007). *Report Submitted to Governor Jon S. Corzine.* Trenton, N.J.: Author.

Pavela, G. *The Pavela Report.* Available at *http://collegepubs.com/the_pavela_report.*

Pettit, L.K. (2007). *Expecting the Unexpected: Lessons from the Virginia Tech Tragedy.* Washington, D.C.: American Association of State Colleges and Universities.

Quinsey, V.L., Harris, G.T., Rice, M.E., & Cormier, C.A. (1998). *Violent offenders: Appraising and managing risk.* Washington, D.C.: American Psychological Association.

Rando, R. & Barr, V. (2009). *The Association for University and College Counseling Center Directors Annual Survey, 2008.* Indianapolis, Ind.: Association for University & College Counseling Center Directors.

State of Florida Gubernatorial Task Force for University Campus Safety (2007). *Report on Findings and Recommendations.* Tallahassee, Fla.: Author.

State of Illinois Campus Security Task Force (2008). *Report to the Governor*. Springfield, Ill.: Author.

State of Kentucky Governor's Task Force on Campus Safety (2007). *Report to the Governor: Examination of Safety and Security at Kentucky's Public and Private Postsecondary Institutions*. Frankfort, Ky.: Author.

State of New Mexico Governor's Task Force on Campus Safety (2007). *Recommendations for Action: Emergency Preparedness in Higher Education*. Santa Fe, N.M.: Author.

State of North Carolina Campus Safety Task Force (2008). *Report of the Campus Safety Task Force Presented to Attorney General Roy Cooper*. Raleigh, N.C.: Author.

The Jed Foundation (2008). *Student mental health and the law: A resource for institutions of higher education*. New York: The Jed Foundation.

U.S. Department of Justice, Office of Community Oriented Policing (2005). *National Summit on Campus Public Safety: Strategies for colleges and universities in a homeland security environment*. Washington, D.C.: Author.

Virginia Tech Review Panel (2007). "Mass Shootings at Virginia Tech: April 16, 2007." Report presented to Virginia Governor Timothy M. Kaine. Available at *www.governor.virginia.gov/TempContent/techpanelreport.cfm*.

Vossekuil, B., Fein, R., Reddy, M., Borum, R., & Modzeleski, W. (2002). *The final report and findings of the Safe School Initiative: Implications for the prevention of school attacks in the United States*. Washington, D.C.: U.S. Department of Education and U.S. Secret Service.

APPENDIX E

Threat Assessment Materials

Appendix E: Threat Assessment Materials

General Awareness Message to the Virginia Tech Campus

(retrieved from *www.vtnews.vt.edu/campus_notices/campusnotice.php?item=2588*). The format below appears in the online Virginia Tech News, "Campus Notice" section:

Threat Assessment Team:
Committed to the safety and well-being of the campus community

Early intervention is essential

Preventing violence and supporting the safety and well-being of the campus community are responsibilities of all members of the Virginia Tech community. Campus safety is enhanced through community members identifying behaviors of concern and reporting the concerns in a caring and timely manner. Early identification of such concerns allows Virginia Tech to intervene more effectively to address behaviors that are threatening or significantly disruptive to the learning, living, and working environment of Virginia Tech.

The Threat Assessment Team

Virginia law and Virginia Tech policy both require the institution to have a threat assessment team to identify, assess, and intervene with individuals whose behavior poses a threat to the safety of the campus community.

The Virginia Tech Threat Assessment Team is staffed by representatives from several university departments, with leadership from the Virginia Tech Police Department. The mission of the multidisciplinary Threat Assessment Team is to determine if an individual poses a threat to self, others, or the Virginia Tech community and to intervene to avert the threat and maintain the safety of the situation. The team responds to behaviors exhibited by students, employees, visitors, and non-affiliated persons in an attempt to prevent violence so that the Virginia Tech campus remains a safe and secure working and learning environment.

Identifying concerning behavior

There are many behaviors that may cause concern for the safety and well-being of an individual or the campus as a whole. The following is not an exhaustive list but provides examples of concerning behaviors or situations:

» Unusual or abrupt changes in behaviors or patterns;

» Extreme reaction to a loss or traumatic event;

» Preoccupation with weapons, violent events, or persons who have engaged in violent acts;

» Uncharacteristically poor performance;

» References to harming others or planning a violent or destructive event;

» Evidence of depression, hopelessness, or suicidal thoughts/plans;

» Inappropriate responses such as prolonged irritability, angry outbursts, or intense reactions;

» Strained interpersonal relations, isolating behaviors, or low self-esteem;

» Significant change in life circumstances such as loss of job or relationship.

Again, these are just examples of behaviors that may cause concern. If you observe or become aware of situations that cause concern for safety, consult with colleagues, supervisors, or university officials and report your concerns.

Reporting concerns: "It may be nothing, but…"

If you have concerns about a person or situation, even if you think it may be nothing, you are encouraged to share the information. The information you provide, no matter how trivial it may seem by itself, may be critical to understanding a broader range of problematic or threatening behavior.

How to share your concern

If you are aware of an emergency or immediate safety concerns, call 911 and report the danger to law enforcement.

If you are concerned about threatening behavior or a disturbing situation that is NOT an emergency event, contact the Virginia Tech Police Department at 540/231-6411. Virginia Tech police are committed to preventing violence and other crimes when possible.

What you need to share

When providing information, please include the name of the person you are concerned about, the behaviors you observed, and your name. While the Threat Assessment Team does accept anonymous reports, if you don't identify yourself, the team has fewer options for addressing the situation you are concerned about.

What will happen to the information you share

Your identity and the information you share will be treated privately with your safety in mind. The information will be used to address the situation in a respectful and helpful manner. The university's Threat Assessment Team will gather more information about the situation and implement a plan to enhance the safety of the campus community.

On-campus resources for violence prevention:

» Police Department: *www.police.vt.edu*, 540/231-6411

» Cook Counseling Center: *www.ucc.vt.edu*, 540/231-6557

» Dean of Students Office: *www.dos.vt.edu*, 540/231-3787

» Human Resources: *www.hr.vt.edu*, 540/231-9331

» Women's Center: *www.womenscenter.vt.edu*, 540/231-7806

» Residence Life: *www.studentprograms.vt.edu/housing*, 540/231-6205

Referrals for Students Resource Card/Sticker

Resources for Student Referrals

In case of an immediate emergency, call Virginia Tech Police Department: 231-6411

For consultations or to report a distressed student, follow your college or departmental protocol and/or call

Your department head/chair

Your college dean

Dean of Students Office (for all student concerns)...231-3787
Cook Counseling Center (for psychological concerns)..231-6557
Services for Students with Disabilities (for academic accommodations)...........................231-3788
Campus Alcohol Abuse Prevention Center (for substance abuse issues).........................231-2233
Judicial Affairs (for violations of Student Code of Conduct)..231-3790
Virginia Tech Women's Center (for cases of sexual assault or gender issues)..................231-7806
Residence Life (for concerns about the health and well-being of on-campus students)* 231-6205

*For concerns about the health and well-being of students living off campus, the Dean of Students Office can arrange for the Blacksburg Police Department to check on off-campus students if deemed appropriate.

Please tell students about these offices, or call the office while the student is with you to make sure he or she gets an appointment. For questions or to request more stickers/cards please contact the Dean of Students Office at 231-3787.

VirginiaTech
Invent the Future™

APPENDIX F

Position Descriptions

Appendix F: Position Descriptions

Staff Job Position

Position Title: **Case Manager**
Status: **Faculty, Full-time**
Department: **Cook Counseling Center**
Division: **Student Affairs**
Revised: October 2008

I. Summary of Position

Work with multiple Virginia Tech departments and multidisciplinary community agencies to provide coordination of services to high-risk students.

II. Organizational Relationships

Responsible to: Assistant director of psychiatry
Assignments received from: Assistant director of psychiatry and director of center
Interacts with: Multidisciplinary staff of psychologists, counselors, psychiatrists, nurse practitioners, office personnel, community providers, and hospital staff.
Nature of supervision: Weekly supervision with assistant director of psychiatry and director of center

III. Duties and Responsibilities

A. Essential Functions:

» Assist in coordination of services for high-risk students.
» Facilitate referrals for continuity of care for students recently hospitalized.
» Follow up and track referrals for students with identified high-risk needs.
» Maintain full and accurate case notes for clients.
» Attend court hearings for involuntarily hospitalized students.
» Coordinate services with the Dean of Students Office, Resi-

dence Life, Cranwell International Center, Women's Center, Schiffert Health Center, Disability Services, and Judicial Affairs for students with high-risk needs.

» Conduct mandatory assessments for identified students referred to Cook Counseling Center by Dean of Students Office, Judicial Affairs, members of the Threat Assessment Team, and Virginia Tech Police Department.

» Serve as a liaison between community mental health providers and Cook Counseling Center.

B. Essential Functions – Administrative

» Provide outreach/educational seminars as needed.

» Attend all counseling center staff meetings, retreats as scheduled.

» Serve on divisional/university committee(s).

» Attend continuing educational and professional development opportunities.

» Perform other duties as assigned by counseling center director.

IV. Qualifications

A. Required Education, Experience, Skills, and Abilities

» Ph.D. in counseling or clinical psychology, marriage and family therapy, counselor education; master's degree in social work, counseling; or clinical nurse specialist with experience in case management; licensed or license-eligible in the Commonwealth of Virginia

» Interest in and experience with the mental health needs of traditional aged college students preferred

» Ability to work collaboratively with other mental health professionals and community resources

V. Physical Requirements

Physical ability to do essential functions with or without accommodations

Office of the Dean of Students

Case Manager

Reports to Associate Dean of Students

Student Advocacy

» Serve as primary resource for managing student issues related to crisis intervention and coordination with other university departments.

» Respond to walk-in and phone calls for student advocacy.

» Serve as a member of Care Team.

» Obtain and review updates on distressed students from members of the Division of Student Affairs Care Team.

» Participate in Dean of Students Office on-call rotation.

University and Community Collaboration

» Manage referrals of distressed students from administration, faculty, staff, and other members of the university community and provide feedback to referral agents.

» Facilitate information flow between Care Team and academic departments.

» Coordinate with Cook Counseling Center case manager as well as representatives from various other departments, including Judicial Affairs, Residence Life, Shiffert Health Center, Women's Center, Virginia Tech Police Department, and appropriate academic administrators from colleges and departments.

» Coordinate with external community agencies and law enforcement as appropriate.

Administrative

» Implement interventions and coordinate services to students as needed.

» Maintain comprehensive overview of students in distress.

» Coordinate follow-up and tracking of students in distress.

» Oversee record-keeping process for students in distress.

Job Title: Human Resources Case Manager

Nature of Responsibilities:

Address the needs of staff members who have problems in areas such as performance, workplace conflict, and psychosocial issues through a variety of interventions, referrals, and follow up services. Responsibilities will include needs assessment, case management, and collaboration and consultation with Human Resources services, other university entities, the EAP program, and community providers.

Specific Duties:

1. Collecting, evaluating, and recording all facts pertaining to employee situations. Maintaining factual case records and preparing necessary statistical reports

2. Formulating intervention plans in order to minimize and/or resolve problems

3. Contacting and collaborating with other university departments to expedite resolution of problems. Maintaining a directory of community resources available to employees

4. Providing referrals to support services within the university as well as community agencies

5. Following up prior cases to monitor progress/resolution

6. Facilitating communication between employees, supervisors, and managers and across departments to address/resolve employee issues

7. Interpreting university policy regarding employees and making recommendations when policy changes are needed

8. Preparing an annual report of services provided

9. Facilitating RTW for employees, subsequent to a leave of absence due to psychological or medically related matters

10. Providing information about medical or mental health resources for employees with financial, language, and/or transportation barriers

11. Providing support and guidance to university troubleshooters in matters pertaining to case management maintenance and access to records, when appropriate.

12. Following legal, clinical, and ethical guidelines

General Qualifications:

Master's degree in education, counseling, social work, public health, or related field

Preferred:

Licensure (LCSW, LPC, PhD)

Experience:

Three to five years experience as an EAP provider or in counseling or a closely related field with a demonstrated knowledge of systems; experience managing response to crisis situations and/or trauma recovery; experience working as part of a case management support team.

Specific Skills and Competencies:

Ability to work within and assist others in navigating through complex systems; understanding of treatment programs, mental health terminology, including diagnostic categories; general knowledge of medical privacy guidelines and ability to communicate difficult/sensitive information.

Job Title: Threat Assessment Specialist

The threat assessment specialist is affiliated with the Virginia Tech Police Department; the position provides professional expertise and leadership to the university Threat Assessment Team and assists in operational assessment and intervention with individuals whose behavior poses a threat to the safety of the campus community; provides consultation in cases of potential threats of violence involving university employees, students, visitors, and others who might be referred to the team; develops workshops and provides consultation for administrators, faculty, staff, students, and community organizations regarding identification and referral of at-risk or distressed individuals and de-escalation of volatile situations; provides crisis intervention to crime victims and witnesses; and oversees the management of sensitive information for the university's Threat Assessment Team. In coordination with appropriate university units, position is responsible for developing a plan for communications, outreach, and education to foster the university's efforts in violence prevention. The threat assess-

ment specialist will be available to respond to emergencies after-hours and on week-ends. The threat assessment specialist may also serve as a collaborator with faculty in related research, outreach, and academic endeavors.

Responsibilities

Threat Assessment/Management Services:

» In consultation with the chief of police, convenes and serves on the university's Threat Assessment Team; serves as TAT chair in absence of chief; and provides leadership and support to Campus and Workplace Violence Committee.

» Provides threat assessment and management of potential violent situations; assesses likelihood of subject's danger to self or others; and coordinates with appropriate university departments (e.g., Human Resources, Cook Counseling Center, Dean of Students Office, Judicial Affairs, police, Office of Senior Vice President and Provost, and others as appropriate), CARE team, local, federal and state law enforcement agencies, and mental health agencies to initiate voluntary or involuntary hospitalization.

» Coordinates, reviews, and evaluates clinical and external forensic assessments, makes recommendations for interventions, and monitors compliance with recommended treatment.

» Responds to, assesses, and triages information from members of the university community concerned about actual or potential incidents of violence.

» Provides information and referrals to appropriate law enforcement agencies, Student Affairs, Human Resources, student health, counseling center, student judicial affairs, and other university offices as needed; may also assist with and serve as a resource to support employee relations functions.

» Coordinates the development of threat assessment and violence prevention procedures, protocols, and resources for the assessment of potentially violent individuals and appropriate interventions or actions to resolve the potential threat.

» Serves as a resource to Threat Assessment Team, CARE Team, and faculty/staff assistance team.

» Provides victim/witness assistance services to increase the comfort and cooperation level.

» Oversees the design and development and assessment of 24-hour threat response system.

» Serves on university committees, task forces, and other bodies as appropriate.

Outreach and Consultation:

» In coordination with appropriate university and off-campus units, develops a plan for communications, outreach, and education for the prevention of violence on campus.

» Trains and consults with Human Resources, law enforcement, Student Affairs, and other professionals on issues related to threat assessment and management, de-escalation of volatile situations, managing mental health issues in the learning or working environment, and similar topics.

» Develops and conducts educational programs for the university community on topics related to threat assessment and management, crisis intervention, and de-escalation of volatile situations. Provides information and training to faculty, staff, and students about when, how, and to whom troubled individuals should be reported.

» Consults with legal counsel, administrators, and University Relations staff on the release of information that may be sensitive.

» Works with academic faculty engaged in related academic, research, or outreach endeavors related to threat management.

Administration:

» Conducts programmatic evaluation and recommends policy and practice changes.

» Provides guidance on the development of an information management process that gathers, analyzes, documents, and disseminates sensitive information; manages this process for the Threat Assessment Team.

» Maintains records, produces reports, and organizes and disseminates TAT case management information.

» Supervises the VTPD/Victim's Services project coordinator.

Qualifications

Required:

» Master's required (doctorate preferred) in clinical, social, or counseling psychology; counselor education; clinical social work; or closely related discipline from an accredited program

» Working knowledge of threat assessment and threat management theory and practice and experience in assessment and management of cases involving potential violence

» Demonstrated abilities to review and interpret clinical assessments and formulate interventions to minimize risk of violence and to provide crisis intervention and response, case management counseling in field/crisis settings, and information and referral

» Demonstrated ability to develop comprehensive and multi-faceted communications, awareness, and education programs around topics of violence prevention for varied audiences

» Demonstrated ability to interact effectively with diverse individuals and groups to reach acceptable solutions to problems

» Demonstrated ability to think strategically and respond operationally to issues or situations posing a threat to the safety of the campus community

Preferred:

» Experience within a higher education setting working with multi-unit, multi-disciplinary teams

» Demonstrated ability to develop and manage projects that will involve complex and sensitive issues, knowledge of relevant laws and regulations, and coordination with multiple departments

» Ability to receive Virginia licensure as required by profession within 18 months of employment

VTPD/Victims Services Special Projects Coordinator

Position details:

Full time, calendar year, restricted professional faculty position

The VTPD/Victims Services Special Projects Coordinator reports to the chief of police. The primary purpose of the position is administration and management of matters pertaining to the university Threat

Assessment Team (TAT) and the Campus and Workplace Violence Prevention Committee (CWVP). In addition, this position will serve as the police department's coordinator of matters pertaining to the completion of activities as outlined in Virginia Tech's Demonstration Project grant with the U.S. Department of Education, Office of Safe and Drug Free Schools, and support for victims services projects supported by the Department of Justice grant. Duties include data management; management of meetings; organizing and implementing team trainings; coordination of administrative activities with on- and off-campus partners, including federal granting agencies and supporting team members, as needed (investigator, chief, or others).

The coordinator serves as liaison from the VTPD to partners implementing victims services, recovery, and resiliency efforts including the provost's office, Human Resources, Student Affairs, and academic and administrative offices as well as possible local, state, and federal off-campus partners such as the Virginia Department of Criminal Justice Services and other state and federal agencies. Grant-supported efforts with the U.S. Department of Education and U.S. Department of Justice might include the organization of statewide meetings, conferences, and publications to meet grant goals.

Responsibilities:

» Supports information needs of VTPD, TAT, and VP Committee by managing data collection, compiling and analyzing data, writing reports, and presenting results to administrators and TAT/Violence Prevention Committee. Ensures that information management procedures comply with federal and state requirements and university policies.

» Supports communication and awareness efforts by developing information sessions and presentations, assisting with or making presentations to students or employees, and developing communications materials in a variety of media.

» Enhances collaboration of university offices, TAT, CWVP Committee, and other entities by developing and implementing information-sharing mechanisms, providing updates, ensuring that cross-over agenda items are shared, following up on assignments and deadlines, and identifying resources.

- » Assists with grant activities, including development of proposals, gathering information from Virginia Tech grant participants, and preparing assigned segments of reports and budgets.
- » Develops and maintains appropriate manuals, forms, procedures, and reports for the TAT.
- » Other duties might include assisting with the administration and management of VTPD agency accreditation, information requests, coordination and preparation for meetings with agency stakeholders, and other duties as assigned by the chief.

Qualifications:

- » Bachelor's degree required, with preference for master's degree or professional experience equating to a graduate degree in one of the following areas: psychology, management, human resources, student personnel, higher education administration, public administration, or related discipline
- » Knowledge of applicable laws and regulations regarding student and employee policies and records
- » General knowledge of threat assessment programs and practices
- » Experience working with sensitive and confidential information
- » Ability to manage projects, including report preparation
- » Familiarity with a variety of data analysis and reporting software
- » Strong written and oral communication skills
- » Ability to develop and make effective presentations to diverse populations
- » Evening and week-end work may be required.
- » Must have a background investigation including a criminal background check.

PREVENTATIVE MEASURES

CAMPUS THREAT ASSESSMENT AND MANAGEMENT TEAMS: WHAT RISK MANAGERS NEED TO KNOW NOW

Campus Threat Assessment and Management Teams: What Risk Managers Need to Know Now

Jeffrey J. Nolan
Dinse, Knapp & McAndrew, P.C.

Marisa R. Randazzo
Sigma Threat Management Associates, P.A.

Gene Deisinger
Sigma Threat Management Associates, P.A.

URMIA

Some quirk in human nature allows even the most
unspeakable acts of evil to become banal within minutes,
provided that they occur far enough away
to pose no personal threat.

—Iris Chang (1968–2004),
American Historian and Journalist

Campus Threat Assessment and Management Teams:
What Risk Managers Need to Know Now

Jeffrey J. Nolan, Esq., Dinse, Knapp & McAndrew, P.C.; Marisa R. Randazzo, PhD, Sigma Threat Management Associates, P.A.; and Gene Deisinger, PhD, Sigma Threat Management Associates, P.A.[1]

Abstract: After the tragic shootings at Virginia Tech in 2007, many colleges and universities recognized that having threat assessment and management (TAM) teams in place to address potentially threatening behavior and situations among faculty, staff, and students on campus was a best practice. This article focuses on three main aspects of TAM teams on college campuses and what risk managers can do to encourage the success and effectiveness of those teams. The article discusses the legal duties that colleges and universities have in connection with violent incidents on campus. It also focuses on the development of a TAM process, the common challenges facing TAM team members, and how risk managers can help mitigate and minimize campus risks by assisting TAM teams.

Introduction

Many institutions of higher education recognized after the April 2007 tragedy at Virginia Tech that having a threat assessment and management (TAM) team is a best practice, and many have recently created teams or enhanced the operations of existing teams. Simply having a TAM team is not enough, though. Institutions must educate the campus community about the team, follow best practices as to the staffing and operation of the team, adopt appropriate related policies, and create and handle team-related documents well. Further, institutions must do more to educate their communities about the proper balance between community safety and the rights of persons of concern, so that misunderstandings about privacy and disability laws, for instance, do not unduly restrict the ability of institutions to take the steps necessary to promote campus safety. Failing to follow best and promising practices in this sensitive area can increase the serious risks of harm and legal liability.

> **Colleges and universities undoubtedly strive to do what they can to keep their campuses safe; enhancing campus safety is the most important goal of the TAM process.**

This article is divided into three sections. The first section outlines the legal duties that colleges and universities have in connection with violent incidents on campus and discusses how related standards of care for TAM processes are likely to be developed in the litigation context. The second section provides a primer on the TAM process, with an emphasis on the identification of resources that TAM teams can rely upon in seeking to comply with current best practices. The third section identifies common challenges faced by TAM teams and makes recommendations about how risk managers can promote campus safety and minimize risk by helping TAM teams to overcome those challenges.

I. Legal Duties and Standards of Care
a. Legal Duties

Colleges and universities undoubtedly strive to do what they can, within the bounds of reason and limited resources, to keep their campuses safe for students, employees, and visitors. Enhancing campus safety is, without doubt, the most important goal of the TAM process. While legal liability considerations are, of course, secondary to safety concerns, legal issues are important, and risk managers can better assist campus TAM teams if they understand the legal issues implicated by campus violence and the work of TAM teams.

It will come as no surprise to risk managers that colleges and universities are generally held to have various duties to exercise due care to provide a campus environment that is reasonably safe from foreseeable acts of violence. The most universal source of such duties is the common law, i.e., the legal principles developed and expressed over time by state court judges in the form of case law, rather than by legislators in the form of statutes. The specific details of common law necessarily vary

from state to state, and an analysis of every state's laws would be well beyond the scope of this article. A resource known as the Restatement of Torts does, however, provide a valuable starting point for understanding the principles that are likely to be applied, in general, in many states. Through several editions of the Restatement, a body known as the American Law Institute (ALI) has endeavored to summarize what it considers to be the most cogent principles of common law that are being applied by judges in the United States. In turn, judges often rely upon Restatement sections and analysis when deciding what the law *should* be, and many formally adopt Restatement sections as the law in particular states. Thus, while some states may reject certain Restatement duties and analyses from time to time, it is fair to view the Restatement as summarizing well where the law generally is, and where it is likely to go, in most states.

The most current version of the Restatement of Torts is the *Restatement (Third) of Torts: Liability for Physical and Emotional Harm*. Many of the Third Restatement's sections have been in essentially final form since the mid-2000s, and the bulk of the work as a whole was officially adopted by the ALI in May 2011. Many courts cited and relied upon Third Restatement sections even before they were in official, final form, so we will focus on the Third Restatement's provisions in the remainder of this discussion.

Obviously, if an institution of higher education itself causes harm to a student or campus visitor through the acts or omissions of an institutional employee, then the institution is liable for negligence if the employee failed to exercise reasonable care and created a risk of physical harm.[2] The underlying duty can be thought of as a relatively passive duty to avoid doing harm. When thinking about campus violence, however, we ordinarily do not think about acts perpetrated by institutional employees. Instead, we usually think about violence perpetrated by third parties such as students or outsiders. This begs the question: does an institution of higher education have an *affirmative* duty to prevent physical harm to students or visitors that is caused by third parties?[3]

The Third Restatement answers this question by stating a facially comforting general rule, but it then goes on for pages about all the "exceptional" circumstances in which liability may attach. The Restatement provides that "[a]n actor whose conduct has not created a risk of physical harm to another has no duty of care to the other unless a court determines that one of the affirmative duties provided in §§ 38–44 is applicable."[4] The duties of most importance to the campus TAM context are those described in sections 40-43 of the Third Restatement. This article will discuss each in turn.

i. Duties Based on a Special Relationship with the Injured Person

Section 40 provides in part that "an actor in a special relationship with another owes the other a duty of reasonable care with regard to risks that arise within the scope of the relationship," and, most significantly for this discussion, provides that one of the "special relationships" giving rise to such a duty is the relationship of "a school with its students."[5] While the word "school" could be read as not including institutions of higher education, a comment to section 40 makes clear that the ALI intended the section to be applicable to colleges and universities. Fortunately, the comment at least recognizes that "because of the wide range of students to which it is applicable, what constitutes reasonable care is contextual—the extent and type of supervision required of young elementary school pupils is substantially different from reasonable care for college students." Further analysis of the section also recognizes that "[c]ourts are split on whether a college owes a duty to its students," and that those courts which do find a duty do so based on a broad variety of sometimes questionable rationales.[6] Thus, while the ALI might want to suggest that the context variable "special relationship"-based duty it envisions *should* always apply to the relationship between institutions of higher education and their students, it recognizes fairly, and fortunately, that the law is far from settled on this point. Nonetheless, given trends in the law and the fact that it is better to be safe than sorry, institutions should plan and conduct themselves as if courts would recognize *some* level of duty to protect students from other students or third parties and leave legal arguments about the issue to counsel in the event of litigation.

Third Restatement section 40 also states that businesses and other possessors of land that hold their premises open to the public have a "special relationship" with, and duty to reasonably protect, those who are lawfully on the premises.[7] Colleges and universities that maintain open campuses would often fit within this category of businesses. Further, the Restatement recognizes that landlords have a duty to exercise reasonable care to protect their tenants from foreseeable criminal activity.[8] These duties have been recognized often by courts for many years. This is one reason why courts which are hesitant to find a "special relationship" based on the student-university relationship alone but which want to find some basis for liability in a particular case, essentially shoehorn hazing and criminal assault cases into a "business invitee" or "landlord-tenant" framework.[9] In sum, risk managers should recognize that business owner and landlord-tenant-based theories continue to provide fertile ground for those claiming that institutions owe a duty to exercise reasonable care to prevent foreseeable attacks on campus.

ii. Duties Based on a Special Relationship with the Person Posing the Risk

Third Restatement section 41 focuses on circumstances when an entity may have a "special relationship" with the person who is posing the risk and a corresponding duty to exercise reasonable care to prevent that person from harming others. One example of relevance to this discussion focuses on the special relationship that employers have with employees. Most commonly, employers are liable for the acts of employees if those acts are within the scope of employment, i.e., the acts are motivated at least in part by a desire to serve the employer.[10]

> **Third Restatement section 41 focuses on circumstances when an entity may have a "special relationship" with the person who is posing the risk and a corresponding duty to exercise reasonable care to prevent harm to others.**

Acts of targeted violence are, obviously, outside the scope of most jobs.[11] Section 41 of the Third Restatement recognizes, however, that employers can still be on the hook for acts outside the scope of an employee's employment "when the employment facilitates the employee's causing harm to third parties."[12] "Facilitation" in this sense can be as simple as providing access to physical locations, such as, for example, where an employee can gain access to dormitories, classrooms, or other campus spaces by virtue of his or her employment.[13] Given how easy it would be to satisfy this standard, institutions should assume that they would generally be deemed to have a duty to exercise reasonable care in the hiring, training, supervision, and retention of employees.[14] For purposes of this discussion, this means that institutions should recognize that they will likely be held to have a duty to use reasonable care by, for example, engaging their threat assessment team when an employee's statements or conduct raises questions as to whether he or she may pose a threat to others.

Another "special relationship" recognized by Third Restatement section 41 is that which a mental health professional has with patients.[15] The corresponding duty follows from state statutes and court decisions that implement the concept outlined in the California Supreme Court's well-known decision in <u>Tarasoff v. Regents of the University of California</u>, 551 P.2d 334 (Cal.1976). In general, <u>Tarasoff</u>-like principles either require or permit mental health professionals to breach the professional-patient privilege[16] where such professionals obtain information indicating that a patient may pose an imminent risk of harm to an identified individual or individuals. The broadly worded comments to Restatement section 41 suggest that professionals should use "reasonable care" to warn identified victims and/or take other steps

within their power to prevent specific, imminent harm. Institutions must recognize, though, that there is significant variation from state to state as to whether and how such duties are codified in statute or described by courts. One important thing for risk managers to take away from this discussion is that they should determine what the mental health professional-patient rules are in their state and ensure that mental health professionals on their TAM teams and on their campus have a sound and common understanding of those rules. Risk managers can also help the TAM team craft strategies to allow mental health providers on campus—such as counseling center staff—to assist the team in a more general advisory capacity in situations where they cannot disclose case-specific information.

iii. Duties Based on Undertakings

Sections 42 and 43 of the Third Restatement describe duties that could have substantial relevance in the TAM team context. These sections provide that a person who undertakes to provide services to another that the person knows or should know reduce the risk of physical harm to the other or to a third person (e.g., a TAM team that involves itself in assessing and managing potentially threatening behavior) has a duty to use reasonable care in providing those services if: (a) the failure to exercise such care increases the risk of harm beyond that which existed without the undertaking to provide those services, or (b) the person to whom the services are provided or another relies on the actor's exercising reasonable care in the undertaking. These "gratuitous undertaking" duties are adapted from sections of the Second Restatement of Torts that have been relied upon by many courts over the years, specifically sections 323 and 324A. Section 323 in particular has been applied, significantly, in cases involving colleges

> **Risk managers can help the TAM team craft strategies to allow campus mental health providers to assist the team in a general advisory capacity in situations where they cannot disclose case-specific information.**

and universities.[17] It is therefore fair to conclude that these duties will continue to be accepted widely by courts in the form presented in the Third Restatement.

In the TAM team context, it could (and undoubtedly will) be argued that a team's undertaking to assess risks posed by persons of concern could fall within the scope of these duties. To fit squarely within these duties, the team's activities would have to either *increase* the risk of harm or *be relied upon* to the detriment of an injured person. However, it is possible to imagine that an injured person could claim that statements made or actions taken by the TAM team in dealing with a threat management scenario gave the injured person a "false sense of security" that made the person, arguably, more vulnerable to an attack and/or that the injured person relied upon the TAM team for protection and, as a result, did not take independent protective action. Every case would be argued based on its facts, and there are many elements that would have to be satisfied before liability would actually attach, but risk managers should be aware of these potential duties when working with their campus TAM teams. If this sounds like a "no good deed goes unpunished" scenario, that is because it is to some extent; nonetheless, colleges and universities have no choice but to undertake threat assessment activities and to perform them well, as discussed below.

b. Standards of Care

This section will focus on how TAM-related standards of care are likely to be developed in the litigation context. Risk managers in those states in which a campus TAM team is required by law[18] will have no trouble explaining to administrators why they should create and support TAM teams. Those in other states might wish to cite the following discussion.

The Restatement of Torts duties described in the previous section maintain that where an affirmative duty to avoid a risk is imposed by a special relationship, an actor has an obligation to exercise due care. But what does "due care" mean in the context of campus threat assessment and management? There is no nationwide, federal statute, and only the Virginia statute lists, in general terms, activities that TAM teams should perform in that state. Thus, the TAM team "standard of care" issue is relatively wide open. Whether a TAM team's activities in a particular case met a broadly defined standard of care will, therefore, be subject to debate. In the context of litigation, that debate is likely to be played out by the competing opinions of expert witnesses. Thus, risk managers should be familiar with the resources that experts would likely cite as defining the standard of care.

On the threshold question of whether colleges and universities should *have* threat assessment teams, there is not much room for debate. Many of the investigative reports that were conducted in the wake of the 2007 Virginia Tech shootings contained recommendations to the effect that campuses should create and/or support campus TAM teams. These reports are summarized well in "The IACLEA Blueprint for Safer Campuses" (IACLEA Special Review Task Force, April 18, 2008) (Blueprint), a document published by the International Association of Campus Law Enforcement Administrators (IACLEA).[19] The Blueprint was designed as a synthesis of the various reports done regarding the Virginia Tech shootings, and it contains numerous recommendations for campus safety from IACLEA. The Blueprint contains 20 campus safety-related recommendations, which should be consulted generally by risk managers who are assessing whether their campus safety operations are consistent with best and promising practices. On the specific topic of TAM teams, the Blueprint recommends that "[i]nstitutions of higher education should have a behavioral threat assessment team that includes representatives from law enforcement,

> **What does "due care" mean in the context of campus threat assessment? There is no nationwide, federal statute. Thus, the TAM team "standard of care" issue is relatively wide open.**

human resources, student and academic affairs, legal counsel, and mental health functions. Specifically, campus public safety should be included on the team." It is safe to assume that in the litigation context, many competent experts would be likely to testify that this recommendation, based as it is on consideration of numerous post-Virginia Tech reports, represents a consensus as to what higher education institutions should be doing, in part, to prevent violence on campus.

Similarly, a June 2011 US Department of Education Family Policy Compliance (i.e., FERPA) Office publication titled "Addressing Emergencies on Campus" notes that the "Department encourages… postsecondary institutions to implement a threat assessment program, including the establishment of a threat assessment team that utilizes the expertise of representatives from law enforcement agencies in the community and that complies with applicable civil rights and other Federal and State laws." This publication also articulates the Department's view that "[u]nder a properly-implemented threat assessment program, schools can respond to student behavior that raises concerns about a student's mental health and the safety of the student and others that is chronic or escalating, by using a threat assessment team." This publication does not itself go into greater detail on why a TAM team should be established or how it should function (though it does contain a link to a Department resource page of interest), but it is fair to assume, given its source and wide distribution, that it would be cited in support of an argument that having a properly functioning campus TAM team is currently a best and expected practice.[20]

Further, as more institutions create TAM teams, the presence of such teams on campus becomes a part of the custom in the industry, which can itself be used as evidence of the standard of care. While the "reasonable care under the circumstances" standard usually remains the technical standard in most cases, evidence of customs to help inform what that means can be persuasive.[21] These

theories would go a long way toward establishing that the applicable standard of care requires colleges and universities to have TAM teams.

Such a case would be supported further by the publication, "A Risk Analysis Standard for Natural and Man-Made Hazards to Higher Education Institutions," published by the ASME Innovative Technologies Institute, LLC (ASME-ITI), and approved by the American National Standards Institute (ANSI) in 2010 (ASME-ITI Risk Analysis Standard). URMIA members are likely familiar with this document, as it outlines a "methodology to identify, analyze, quantify, and communicate asset characteristics, vulnerabilities to natural and man-made hazards, and consequences of these hazards on the campuses of colleges and universities."[22] On the topic of TAM teams, the Standard recommends "that Threat Assessment Teams be put into place on campus to help identify potential persons of concern and gather and analyze information regarding the potential threat posed by an individual(s)."[23]

In light of this ASME-ITI/ANSI recommendation, risk managers should recognize that courts have often allowed expert witnesses to testify to the effect that standards prepared by voluntary standards organizations such as ANSI represent the standard of care on a topic and/or have otherwise allowed such standards into evidence.[24] While voluntary standards do not have the force of law like statutes do, they can be persuasive evidence of the standard of care, given the deliberative, consensus driven process by which many are created. There is ample case law to this effect,[25] so it is fair to assume that some courts would similarly permit reference to the ASME-ITI/ANSI TAM team recommendation in the event of TAM-related litigation.

In addition to recommending that colleges and universities have a campus TAM team, the ASME-ITI/ANSI Risk Assessment Standard "provides resources for implementing Threat Assessment Teams on campus."[26] While such resources would not, again, define the standard of care exclusively or conclusively, it is likely

> When a person or situation is reported, the team must first determine whether there is any imminent danger or an emergency situation.

that they would be cited as persuasive in the event of TAM-related litigation, because they are relied upon and recommended in the ASME-ITI/ANSI standard. Therefore, risk managers should determine whether their threat assessment teams are in fact following practices similar to those described in the cited resources. TAM teams should follow practices that are most responsive to the needs of their particular campuses, but if a team's practices differ substantially from the general approaches outlined in the resources cited in the ASME-ITI/ANSI Standard, the team should be able to articulate why its following a different approach is more appropriate given the unique needs of its campus.

The remaining sections will outline some best and promising practices in more detail, highlight common areas of concern, and offer suggestions about how risk managers can work with TAM teams to address any gaps between where the teams are right now and where they should be.

II. Best Practices in Campus Threat Assessment

The resources that are referenced in the ASME-ITI/ANSI standard provide guidance on what the authors consider to be current best practices for campus threat assessment and threat management.[27] These resources cover both the processes and procedures that TAM teams should follow in handling reports of threats or other concerning behavior, as well as the campus and community systems and resources that support and facilitate TAM team operations.

a. Threat Assessment Processes and Procedures

There are several steps to the campus threat assessment and management process, beginning from the point where the TAM team first learns about a threat or other disturbing behavior through to the closure of the case. The steps in the best practices for campus threat assessment and management are as follows.[28]

i. Screen Initial Reports

When a person or situation is reported to the TAM team, the first thing the team should do is determine whether there is any imminent danger or an emergency situation. Determining whether there is an imminent danger will generally be based solely or primarily on the information that is reported to the TAM team and any other information the team already possesses. If the TAM team feels the situation *is* an emergency, the team should call law enforcement or security to take immediate steps to contain the person, make an arrest, or possibly get the person to an emergency psychiatric evaluation if the circumstances allow. The team will eventually need to conduct a full threat assessment inquiry to take appropriate measures in the event the person in question is released and returns to campus; but in the event of an emergency or imminent situation, the team's primary course of action is to notify law enforcement to ensure the situation is contained.

If the TAM team determines that there is *not* an emergency or imminent concern, the next thing the team should do is conduct a full threat assessment inquiry to determine whether the person or situation of concern poses a threat of violence or self-harm.[29]

ii. Conduct a Full Threat Assessment Inquiry

To conduct a full threat assessment inquiry or investigation, the TAM team should seek out information from all persons and other sources that may have some information about the person or situation of concern. This information seeking mandate is an important role that distinguishes TAM teams from CARE teams and other student assistance teams, which typically respond to the information provided to them and do not seek out additional information from multiple sources.

The sources that the TAM team can contact for information should include persons who interact with the person of concern, as well as those who may be in a position to observe the person even if they typically do not interact with the person. The TAM team should gather information from people inside the institution, such as professors, resident advisors, and specialty service offices, such as disability services or veterans services. Where possible, the team should also gather information from outside the institution, such as from an employer, previous school, community league coach, Internet activity, and family members where advisable.

iii. Evaluate Whether the Person or Situation Poses a Threat

After gathering additional information in the threat assessment inquiry, the TAM team will evaluate the information to determine whether the person or situation in question poses a threat of violence or self-harm. To do this, the team can first organize the case information using a series of investigative questions, detailed in the resources recommended by the ASME-ITI/ANSI-approved risk assessment standard. The team should then use the information it has collected to determine whether the person of concern poses a threat—that is, to determine if the person has developed an idea or plan to do harm and is taking steps to carry it out.

If the TAM team determines that the person *does* pose a threat, it will then develop, implement, and monitor a case management plan to intervene and reduce the threat posed. If the team determines that the person *does not* pose a threat, the team can close the case or can opt to monitor the person or situation for a period of time and re-evaluate the case to assess whether the person still does not pose a threat.

iv. Develop, Implement, and Monitor a Threat Management Plan

If the TAM team determines that the person in question poses a threat of violence or suicide, the team should then develop, implement, monitor, and document a plan to intervene and reduce the threat.[30] The plan should be customized to best address the person of concern and situation with the resources that the team and institution have available or could access or coordinate. The goal of a threat management plan is to help move the person of concern away from thoughts and plans of violence or suicide and get assistance to address problems.

Threat management/case management plans can include any of the following as the situation and resources dictate:

- Monitor the situation for further developments
- Engage with the person of concern to de-escalate the situation
- Involve an ally or trusted person to monitor the person of concern
- Family/parental notification
- Law enforcement intervention
- Disciplinary review and action
- Implement a behavioral contract
- Voluntary referral for mental health evaluation and/or treatment
- Mandated psychological assessment
- Involuntary hospitalization for evaluation and/or treatment
- Leave or separation from the institution
  - Voluntary leave
  - Interim suspension
  - Involuntary leave
- Modification of the environment to mitigate impact of contributory factors
- Collaborate with identified target/victim to decrease vulnerability
- Monitor and prepare for impact of likely precipitating events

Once the TAM team has created a threat management plan, it is just as important that the team document the plan, implement the plan, and then monitor how well the plan is working to make sure it is having the intended effect and not inadvertently making the situation worse.

It is important to note that a person can continue to pose a threat even after he/she is no longer a member of the campus community. The TAM team should continue to monitor the plan and modify it as needed for as long as the person/situation may still reasonably pose a threat. It may be necessary for the TAM team to continue to refer the person of concern to necessary resources or take other follow-up steps as the situation and level of concern dictate. As the TAM team considers what may affect the person's behavior in the short-, mid-, and long-term, the team should anticipate the impact of future precipitating events—including important dates or events such as anniversaries, failing a course, termination of benefits, the ending of a relationship, or the occurrence of mass attacks elsewhere—that could prompt the person to become an increased threat. The team should develop contingency plans and take necessary steps to reduce or mitigate the anticipated threats.

v. Close and Document the Case

Cases handled by a TAM team generally remain open until the person of concern no longer appears to pose a threat. This may be well beyond when criminal cases are closed or mental health services are completed. Whether the case remains open or is closed, the TAM team should document how they handled the case, including the report that first came to the team's attention, the information the team gathered, the evaluation it made, the case management plan it developed and implemented (if necessary), and any re-evaluations or monitoring that the team conducted after the initial evaluation and case management efforts where relevant.

The level of detail in the case documentation—as well as where and how case records are maintained and stored—are critical issues for an institution's legal counsel to help a TAM team determine. The case documentation can also include the team's appraisal of whether there was sufficient concern regarding public safety that the Family Educational Rights and Privacy Act (FERPA)[31] health and safety exception would apply, in the event information sharing in the case is ever questioned or challenged. Legal counsel should be consulted on documentation issues, which are discussed further below.

b. Resources and Activities that Support TAM Team Operations

While there is a tendency to think of the TAM team as involving only those individuals directly involved in staffing cases, we view the TAM team differently. Certainly, the identified members of the official team are critical to the process. However, just as important are all the members of the community that support and facilitate the work of the TAM team. Just as a sports team has first

string players on the field, the effective team also has back-ups to those players: specialty units, coaches, managers, scouts, marketing agents, fans, and, yes, even critics. So, too, does an effective TAM team. Furthermore, an effective TAM team recognizes and maximizes the value and contribution of all those elements to achieve the desired goal—the improved safety and well-being of the campus community.

TAM teams handle day to day reports submitted to the team, conduct full inquiries, and implement and monitor case management activities. To be more fully effective, though, a TAM team needs support from key resources and activities on campus and in the community. These resources and activities[32] include:

- Support/backing from the institution's leadership
- Administrative support
- Access to mental health services
- Involvement of law enforcement and security services
- Active outreach and training to the community
- Engagement with gatekeepers of all types, at all levels
- Clear policies and procedures for TAM team authority and operations

Risk managers can play an important role in making sure these resources are available to the TAM team, and that the activities are conducted, so that the team can focus its time on investigating and managing cases.

III. Common Challenges and Recommended Solutions

Many institutions and TAM teams face common challenges that can hinder their effectiveness.[33] Some of the more common challenges and obstacles that TAM teams encounter include misconceptions on campus about threat assessment and threat management; misunderstandings regarding FERPA, Health Insurance Portability and Accountability Act (HIPAA), state

privacy laws, and information sharing; misconceptions about how disabilities laws apply to the TAM context; problems related to institutional policies and procedures that are not integrated optimally with TAM team operations; problems with documentation; moving directly to case management efforts without evaluating the person or situation of concern; and failing to implement part or all of a case management plan.

a. Misconceptions About Threat Assessment and Management

When launching a threat assessment and management capacity of some sort, TAM team members may well encounter misconceptions and misunderstandings about what behavioral threat assessment is and what it is not. Some of these misconceptions include that threat assessment is the same thing as profiling (not true); that "reporting" someone to the TAM team is the same thing as tattling (not true, unless the person reporting is doing so maliciously); and that anyone reported to the TAM team is immediately or eventually suspended, expelled, punished, or fired (not true unless the institution has inappropriately conjoined its disciplinary process and threat assessment process).

One way that risk managers can help address these misconceptions is by working with their TAM team to develop and publicize frequently asked questions about campus threat assessment and management. Another way is for risk managers to advocate for periodic campus-wide awareness training, such as orientation meetings for students and residential advisors and academic and operational department meetings, that would encourage reporting of concerns and promote familiarity with the TAM concept. The thrust of such training should be that the TAM team is focused on promoting campus safety and helping individuals who need it, not on punishment for disciplinary offenses. The more transparent the threat assessment process is for the

> **One way risk managers can help address misconceptions is by working with their TAM team to develop and publicize frequently asked questions and advocate for periodic campus-wide awareness training.**

campus community—with respect to how the TAM team operates, not with respect to the particulars of a specific case—the easier it will be for the TAM team to build credibility and inspire confidence and the more likely people will be to submit reports to the team. In sum, simply having a TAM team on campus is not enough. For the team to be effective at reducing risk, the community must know about the team and be willing to report concerns when appropriate.

b. Misunderstandings about FERPA, HIPAA, and State Privacy Laws

When seeking information about a particular student in the course of its investigative work, TAM teams often encounter misunderstandings about FERPA and the extent to which it is perceived as interfering with TAM team members, professors, and others in regard to sharing information about a student of concern. Many people still believe that student records and information may not be shared under any circumstances. It is clear from the work of the Virginia Tech Review Panel and other entities that these misunderstandings are widespread and often difficult to counter.[34]

One way that risk managers can help enhance the overall effectiveness of their TAM team is by developing resources and strategies or supporting training programs to better educate the campus community about FERPA, the exceptions under which information can be shared, and the limited remedies for inappropriate disclosure of FERPA-protected information (campus personnel are often surprised to discover, for example, that neither individuals nor institutions can be sued for violating FERPA). TAM teams and campus police and security officers should be within the institution's definition of "school officials" with whom education records and information therefrom may be shared freely,[35] and institutions should take steps to assure that faculty and staff members know that. Most importantly, faculty and staff must understand that a long standing "health and safety" exception that was broadened in response to the Virginia Tech shootings permits disclosure of education records to any appropriate parties (on or off campus) where necessary to protect the health or safety of the student or others.[36] Through resources such as periodic training, web page information, and one-page fact sheets,

risk managers can help TAM teams to educate the campus community about the truth—and correct any misconceptions—regarding FERPA.

While not as prevalent, similar issues can be presented by campus community members' misplaced concerns about the privacy provisions of HIPAA. The HIPAA Privacy Rule prohibits the disclosure of personal health information by health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. While HIPAA does apply to certain medical information on some campuses, many colleges and universities do not have operations that are covered by HIPAA, and student health records are generally covered by FERPA, not HIPAA.[37] Further, even if HIPAA does apply to certain records on some campuses, it permits disclosure of protected health information if a covered entity believes in good faith that disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and such disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.[38] In sum, risk managers and TAM teams should take steps to determine whether HIPAA privacy rule restrictions actually apply to campus operations and to educate the campus community about the rule and the health and safety exception if applicable to ensure that undue concerns about HIPAA do not restrict the provision of important information to a TAM team.

As for state law privacy rules, the most commonly applicable state law rules are those pertaining to the relationship between health care providers and their patients. Those rules, and the circumstances in which disclosure of otherwise privileged information might be allowed or required, are discussed in Section I.a.ii. above. The most important thing that risk managers can do with respect to such rules is to assure that TAM teams and providers who routinely see campus community members, such as student counseling center providers or employee assistance program (EAP) providers, have a *shared* understanding of the thresholds for disclosure that the providers will apply. TAM teams should understand when they can rely upon providers to breach privileges due to a specific threat level, and when, on the other hand, they should assume that they will have to assess and

manage threats based on other information sources. Risk managers should encourage TAM teams to have frank conversations with providers about such issues.

TAM teams cannot function without information from the campus community, so it is crucial that campus community members have an accurate understanding of privacy rules and, just as importantly, the exceptions to those rules. That way, TAM teams can do their important work without being restricted unduly by concerns about privacy rules.

c. Misconceptions about Disabilities Laws

Colleges and universities are covered by the Americans with Disabilities Act of 1990 (as amended in 2008) (ADA) and Section 504 of the Rehabilitation Act, and many are covered by parallel state laws. The requirements of these laws are similar in most respects, so this article will refer to the ADA, because it is the broadest and the most broadly applicable. Undue deference to the potential ADA-related rights of persons of concern could lead a TAM team or institution to fail to take necessary threat management steps, while a failure to respect ADA-required procedures could result in liability under the ADA. TAM teams must, therefore, coordinate threat management efforts with counsel to assure that ADA-related issues are handled optimally.

A detailed treatment of these issues is beyond the scope of this article, but TAM teams should at least understand that while the coverage of the ADA is very broad,[39] it does not require that institutions tolerate threatening behavior that poses a "direct threat" to others[40] or that renders a student or employee not qualified to participate in the academic, residential, or work environment.[41] This is true in most states and federal circuits even if the threatening behavior is caused by a disability.[42] With this general information in mind, TAM teams can focus on inappropriate behavior instead of worrying about ADA issues specifically and work with legal counsel to take threat management actions that they deem necessary (e.g., mandatory counseling, suspension,

> **TAM teams must coordinate threat management efforts with counsel to assure that ADA-related issues are handled optimally.**

conditional re-entry to campus) without undue concern over the possibility that the person of concern might be covered by the ADA.

TAM teams do need to understand, though, that there are ADA-related due process considerations they need to respect. The US Department of Education's Office of Civil Rights (OCR) has been clear in emphasizing that if an institution proposes to affect the status of a student covered by the ADA or Rehabilitation Act, it must provide "minimal due process" for temporary status changes, and "full due process" for longer term or permanent status changes. This means that in emergent situations, such as those that might require temporary suspensions, students should be provided with some notice of the institution's concerns and some opportunity for the student to explain his or her side of the story. After the emergent issue has passed, if the institution decides to pursue longer term curtailment of a student's rights, the student should receive a hearing and an opportunity for an appeal. At most institutions, a TAM team will not be responsible for administering disciplinary, involuntary withdrawal, or similar processes, but it should at least understand the due process requirements that will apply to the institution. This will allow the team's threat management recommendations or actions to dovetail effectively with campus procedures, and student rights can be respected without unduly compromising campus safety considerations.

d. Problems with Institutional Policies and Procedures

Risk managers should work with TAM teams and counsel to assess whether institutional policies relevant to TAM operations, such as policies regarding student misconduct, weapons, workplace violence, threatening behavior and statements, and trespassing, are phrased in such a way as to allow TAM teams to take or advocate for disciplinary or protective action as appropriate. Universities should change policies, which in many

states are enforceable as contracts, so that they can serve essential institutional prerogatives, while also optimally supporting TAM operations. Further, where teams and counsel discern through a review that there are gaps in institutional policies that could make it more difficult to address threatening behavior, universities should create policies to fill those gaps.

Similarly, institutional procedures that are likely to be implicated by TAM operations should also be reviewed by TAM teams and counsel. Teams need to become familiar with how the institution's procedures function, so that they will understand any related limitations. For example, if an institution's student disciplinary procedure or involuntary withdrawal procedure places practical limitations on what the TAM team can do or recommend in a given situation, the team needs to understand that in advance, rather than getting an unpleasant surprise in the midst of an emergent situation. Advance review will also provide an opportunity for the team and counsel to advocate for the revision of any procedures that will obviously and unnecessarily limit the options available for the management of threat situations.

In sum, while colleges and universities must comply with statutes as they are written, they have some flexibility in defining the rules that they impose on themselves through institutional policies and procedures. Optimized policies and procedures can facilitate the work of TAM teams, while those that universities craft without TAM issues in mind can impair that work and complicate already risky situations. A thorough TAM-related policy and procedure review should, therefore, be on every risk manager's agenda.

e. Documentation Challenges

Risk managers know well that accurate documentation is helpful—unless it's not. Obviously, an institution would like good decision making processes to be documented well, but would regret the creation of documentation that,

> **Documentation that states the rationale for the team's decisions and summarizes the factual bases for those decisions can memorialize the team's thinking if its decisions are ever questioned.**

if taken out of context, could shed an unflattering light on the work of a TAM team. TAM teams must understand that unless a privilege against disclosure applies, most of the documents they create, including e-mails, personal notes, and other relatively informal documentation, would be subject to disclosure in the event of litigation. Further, unless an exemption applies, public institutions may have to disclose documents in response to public record act requests, and colleges and universities may also have to turn over TAM team documents if a student of concern demands them under FERPA.[43] While teams may be able to resist disclosure in specific cases if exemptions apply, teams should still be cautious and create all drafts, notes, e-mails, and final summary documents with these realities in mind.

Documentation that states the rationale for the team's decisions at various points in an assessment and management process and summarizes the factual basis for those decisions can serve to memorialize the team's thought process if its decisions are ever questioned. In final form, the documentation regarding a case should demonstrate that the team's work and decision making process was, to borrow Dr. Gene Deisinger's acronym, Fair, Objective, Reasonable, and Timely, in order to FORTify the institution's position.

Documentation should not, on the other hand, contain off-handed comments, speculation without basis in fact, ill-considered observations about sensitive mental health or disability issues, or partially formed thoughts and deliberations. While teams must "think out loud" when weighing options in a particular case, they do not need to document every passing thought and preliminary deliberation. It is very helpful to have a skilled scribe for the group who has worked with counsel to determine how to optimally document the team's deliberations and decision making.

Of course, because legal issues are often presented by the deliberations of TAM teams, those deliberations and related documentation could fall within the scope of

the attorney-client privilege, if legal counsel is involved. As discussed above, TAM-related discussions often involve balancing the privacy and/or disability law rights of persons of concern against the institution's legal duty to provide a safe campus community. Involving counsel in a TAM team's deliberations is therefore natural and appropriate. Counsel may be particularly helpful in reviewing draft documentation and minutes. If deliberations and related documents are within the scope of the attorney-client privilege under state law, they should be protected from disclosure in the event of litigation, from a FERPA request made by a student of concern, and, in some states, from a public record request.

The bottom line for risk managers is that they should assure that their campus TAM teams have consulted with counsel about the application of the attorney-client privilege to their communications and documents and about optimal documentation practices. That way, if disclosure of documents is ever necessary, the university can disclose them with confidence rather than trepidation.

f. Case Management Without Evaluation

When cases first come to the attention of a TAM team, they can be accompanied by significant fear and other emotion that leads to an action imperative, or a strong pull to do something in response to the fear expressed. Certainly in those limited cases where there is an imminent threat to the community or an individual, such as a report of a person walking into an administrative building with a weapon, then institutions must understandably act quickly, even if the report turns out to misrepresent the situation. However, most reports do not involve such exigent circumstances and instead allow for time and opportunity to gather additional information, assess the situation, and develop a reasonable and meaningful approach based on the degree of danger that the TAM team perceives there to be. Having a consensus among the team members regarding whether the person or situation poses a threat—and the corresponding priority level the team believes the case merits[44]—can help guide clear, fact-based decisions regarding the most appropriate case management strategies to employ. This decreases the likelihood of reactionary interventions that may not improve the situation and can, at times, inadvertently escalate a situation unnecessarily. It also

decreases the impulse to craft case management plans based on partial or incomplete information, allowing the team to develop a full picture of the situation and corroborate the information in hand before deciding how best to intervene.

A well-developed threat assessment and management process allows for informed, assessment-led interventions that can best:

- De-escalate, control, or contain the person of concern
- Decrease the vulnerability of likely victims
- Mitigate effects of negative environmental or systemic influences
- Anticipate the effect of precipitating events that may develop

Risk managers can assist TAM teams in monitoring and reviewing team processes, challenging reactionary interventions (in the absence of exigent situations), and supporting assessment-based interventions that are proportional and responsive to the situation at hand.

g. Failing to Implement a Case Management Plan

The last common challenge facing TAM teams is that they do solid work in conducting a full inquiry, making the assessment, and developing a case management plan—but then fail to implement and monitor part or all of the case management plan. Failing to implement a case management plan can come about because an individual TAM team member fails to do what he or she was tasked with doing, someone outside the team fails to do what he or she was asked to do to assist the team, or the team as a whole fails to put into action the plan that it crafted. There are various reasons, excuses, and rationales for these occurrences, but regardless of the perceived validity of the rationale, from a legal perspective, this could result in a significant safety risk and related legal exposure in the event that a person of concern causes harm. It is fair to say that TAM teams will be accorded discretion to decide on a reasonable course of action when assessing and managing threats, within the bounds of the duties described above. However, if a team fails to follow through on a commitment it makes to itself, it will have a more difficult time justifying its approach. If the answer to the question, "Why didn't you follow through?," is that

changing circumstances required a change of course, that would be subject to the same reasonableness standard. If, however, the answer is, "I forgot or didn't get around to it," that would sound very hollow in the context of litigation over a violent incident, whether the failure to follow through would actually have prevented the harm or not.

Risk managers can help their TAM teams to become more fully effective by ensuring that the team engages in the complete threat assessment and management process to include implementing and monitoring case management plans they develop to intervene and reduce any threats posed. If a TAM team is overloaded with incoming reports and new cases to investigate, the institution's risk manager can help the team to offload implementation of case management plans or specific components to various campus personnel who would fulfill these duties responsibly. Risk managers can also advocate for the hiring of a dedicated case manager position (or two or three dedicated case managers, as needs dictate), whose primary job would be to implement, monitor, and report on case management plans developed by the TAM team.[45] Finally, risk managers can conduct or request outside assistance in conducting a review or audit of the TAM team's work to identify areas where the team's procedures may fall short of best practices and to find remedies to bridge those gaps.

Conclusion

There is no question that engaging with individuals who may pose a threat to others on campus is a risky business. In practical terms, though, some risk in this area cannot be avoided, because the current standard of care dictates that colleges and universities must have a campus threat assessment team. Given this reality, risk managers should assure that their campus communities know about and feel comfortable reporting concerns to their TAM teams, their teams follow best and promising practices, misconceptions about privacy and disability laws will not impede their teams' work, institutional policies and procedures support rather than impede the work of their teams, their teams follow optimal documentation practices, and their institutions are positioned to balance appropriately the statutory rights of persons of concern against campus safety needs. If risk managers can address

these issues, they will have gone a long way toward minimizing legal liability in this sensitive area and, most importantly, toward reducing the risk of harm on their campuses.

About the Authors

Jeffrey J. Nolan is an attorney with Dinse, Knapp & McAndrew, P.C., where he focuses his practice on training, policy development, advising, and litigation on behalf of colleges and universities and other employers. He also serves as a senior consultant to Sigma Threat Management Associates, P.A.

Marisa R. Randazzo, PhD, is a managing partner of Sigma Threat Management Associates, P.A. She previously served as chief research psychologist for the US Secret Service.

Gene Deisinger, PhD, is deputy chief of police and director, threat management services at Virginia Tech and is also a managing partner at Sigma Threat Management Associates, P.A.

Endnotes

1 The authors worked as subject matter experts with the team that developed the US Department of Justice Community Oriented Policing Services (COPS) Office's national curriculum, *Campus Threat Assessment Training—A Multidisciplinary Approach for Institutions of Higher Education* (see www.campusthreatassessment.org). They also served as faculty for that program, which was presented at 10 locations throughout the United States in 2009, 2010, and 2011.

2 *Restatement (Third) of Torts: Liability for Physical and Emotional Harm* (Restatement (Third) of Torts), § 7 (American Law Institute, 2011).

3 This discussion will focus on duties owed to students and campus visitors, but not faculty and staff because, in most situations, workers' compensation statutes provide the exclusive remedy for employees who are injured or killed within the scope of their employment. Some sections

of the Restatement (see, e.g., Restatement (Third) of Torts, § 40(b)(4)(a) and § 40, cmt. k) and some exceptional provisions of state law do contemplate institutional liability to employees notwithstanding workers' compensation exclusivity, but such issues are limited, state-specific, and complicated enough that they are beyond the scope of this article. It should suffice to say that institutions will of course want to do what they can reasonably to keep employees safe from physical attacks on campus, even in the absence of a general legal duty to do so.

4   Restatement (Third) of Torts, § 37. For those risk managers and attorneys who have followed the development of case law in this area over the years, section 37 of the Third Restatement replaces sections 314 and 315 of the Restatement (Second) of Torts, upon which many courts have relied in deciding whether and/or what duties colleges and universities owe to their students.

5   Restatement (Third) of Torts, § 40(a), § 40(b)(5).

6   Restatement (Third) of Torts, § 40, cmt. l. Comment l listed and annotated as follows various cases in which courts imposed a duty of reasonable care to protect students on college or university property: "Schieszler v. Ferrum Coll., 236 F. Supp. 2d 602 (W.D.Va.2002) (concluding that, on specific facts alleged by plaintiff, college owed affirmative duty to student who committed suicide); Peterson v. S.F. Cmty. Coll. Dist., 685 P.2d 1193 (Cal.1984) (duty owed to student raped in college parking ramp); Furek v. Univ. of Del., 594 A.2d 506 (Del.1991) (finding university had special relationship with student who was a fraternity pledge but also relying on its undertaking to regulate hazing and its status as possessor of land and student's status of invitee); Nova Southeastern Univ., Inc. v. Gross, 758 So. 2d 86 (Fla.2000) (duty owed to graduate student placed by university in mandatory internship); Niles v. Bd. of Regents of Univ. Sys. of Ga., 473 S.E.2d 173 (Ga.Ct.App.1996) (stating in dicta that a "university student is an invitee to whom the university owes a duty of reasonable care"); Stanton v. Univ. of Me. Sys., 773 A.2d 1045 (Me.2001) (university owed duty to student-athlete as business invitee who was residing in dormitory to provide information about appropriate precautions for personal safety); Mullins v. Pine Manor Coll., 449 N.E.2d 331 (Mass.1983); Knoll v. Bd. of Regents of Univ. of Neb., 601 N.W.2d 757 (Neb.1999) (victim of fraternity hazing episode owed duty by university based on its role as landowner with student as its invitee); cf. Mintz v. State, 362 N.Y.S.2d 619 (App.Div.1975) (impliedly assuming that duty existed in deciding that university had not acted unreasonably as a matter of law in supervising overnight canoe outing by students); Davidson v. Univ. of N.C. at Chapel Hill, 543 S.E.2d 920 (N.C.Ct.App.2001) (holding that university has special relationship with cheerleader based on mutual benefit to each from the activity and control exerted by the university over the activity, but denying, in dicta, that university has special relationship generally with students)." Restatement (Third) of Torts, § 40, cmt. l.

On the other hand, the ALI cited and annotated as follows cases in which courts found no duty: "Bradshaw v. Rawlings, 612 F.2d 135 (3d Cir.1979) (applying Pennsylvania law) (college owed no duty to student injured while being transported by another underage student who had become drunk at off-campus class picnic); Booker v. Lehigh Univ., 800 F. Supp. 234 (E.D.Pa.1992) (university owed no duty to student who was injured after becoming inebriated at on-campus fraternity party); Baldwin v. Zoradi, 176 Cal. Rptr. 809 (Ct.App.1981) (university owed no duty to student by virtue of dormitory license where risks created by excessive drinking and drag racing were not foreseeable to university); Univ. of Denver v. Whitlock, 744 P.2d 54 (Colo.1987) (concluding that university

owed no duty to student injured while on trampoline at fraternity; to impose duty could result in imposing regulations on student activity that would be counterproductive to appropriate environment for student development); Coghlan v. Beta Theta Pi Fraternity, 987 P.2d 300, 311–312 (Idaho 1999) (college does not have special relationship with student that imposes a duty to protect student from risks involved in voluntary intoxication); Rabel v. Ill. Wesleyan Univ., 514 N.E.2d 552 (Ill.App. Ct.1987) (university owed no duty to student based on its landlord-tenant relationship with her for harm that resulted from prank by intoxicated fraternity member); Nero v. Kan. State Univ., 861 P.2d 768 (Kan.1993) (declining to impose duty on university solely because of its role as school but concluding university had duty of care as landlord for student living in dormitory); Boyd v. Tex. Christian Univ., Inc., 8 S.W.3d 758 (Tex.App.1999) (university had no duty to student injured while at off-campus bar); Beach v. Univ. of Utah, 726 P.2d 413 (Utah 1986) (university had no duty to protect student from consequences of voluntary intoxication while on university-sponsored field trip)." Restatement (Third) of Torts, § 40, cmt. l.

Finally, the ALI cited two general resources as follows: "Peter F. Lake, *The Rise of Duty and the Fall of* In Loco Parentis *and Other Protective Tort Doctrines in Higher Education Law*, 64 Mo. L. Rev. 1 (1999) (identifying a trend in tort law toward holding institutions of higher education to a tort duty with respect to the safety of students); Jane A. Dall, Note, *Determining Duty in Collegiate Tort Litigation: Shifting Paradigms of the College–Student Relationship*, 29 J.C. & U.L. 485 (2003) (advocating recognition of a special relationship between colleges and their students)." Restatement (Third) of Torts, § 40, cmt. l.

7   Restatement (Third) of Torts, § 40(b)(3).

8   Restatement (Third) of Torts, § 40(b)(6).

9   See cases cited in endnote 6 above. In addition to those cases, other cases in which institutions have been held to have a "business invitee" or "landlord-tenant"-based duty to protect on-campus visitors against acts by third parties include Bearman v. Univ. of Notre Dame, 453 N.E.2d 1196 (Ind. 1983) (university had duty to protect bystander injured due to fight between two drunken tailgaters), Peterson v. San Francisco Comm. College Dist., 36 Cal.3d 799, 205 Cal.Rptr. 842, 685 P.2d 1193 (1984) (college owed duty to protect student from reasonably foreseeable criminal attack on campus), and Miller v. State, 62 N.Y.2d 506, 467 N.E.2d 493 (N.Y. 1984) (state university had duty, as landlord, to use reasonable security precautions to protect student from foreseeable rape in an on-campus dormitory).

10   See Restatement (Third) of Agency, § 2.04 (American Law Institute, 2006).

11   See Restatement (Third) of Agency, § 7.07, cmt. c.

12   Restatement (Third) of Torts, § 41(b)(3).

13   Restatement (Third) of Torts, § 41, cmt. e.

14   Ibid.

15   Restatement (Third) of Torts, § 41(b)(4).

16   The scope of the patient-mental health professional privilege varies from state to state. One national resource often looked to for general guidance is the American Psychological Association's code, which provides in pertinent part that the privilege may be breached with patient consent "where permitted by law for a valid purpose such as to . . . protect the client/patient, psychologist, or others from harm . . . ." *APA Ethics Code 2002*, Sec. 4.05(b).

17 See <u>Mullins v. Pine Manor College,</u> 449 N.E.2d 331 (Mass.1983) (finding that student on-campus rape victim relied upon college's providing security services, based on generalized interest by college applicants in campus security and the student victim's having visited several campuses before selecting Pine Manor); <u>Furek v. Univ. of Del.</u>, 594 A.2d 506 (Del.1991) (holding university subject to duty to student with regard to risks of fraternity hazing based on its undertaking to prohibit and regulate hazing activities); <u>Davidson v. Univ. of N.C. at Chapel Hill</u>, 543 S.E.2d 920 (N.C.Ct. App.2001) (finding that university owed duty to cheerleader based on its undertaking to advise cheerleading squad on safety matters).

18 See 110 ILCS 12/20(b) (2009) (Illinois statute, enacted after the February, 2008 shootings at Northern Illinois University, which requires each Illinois institution of higher education to develop a campus threat assessment team); Va. Code Ann. § 23-9.2:10 (2008) (Virginia statute enacted after the April, 2007 shootings at Virginia Tech which requires public higher education institutions in Virginia to establish a threat assessment team that includes members from law enforcement, mental health professionals, representatives of student affairs and human resources, and, if available, college or university counsel, and which charges such team to provide guidance to students, faculty, and staff regarding recognition of behavior that may represent a threat to the community, to identify members of the campus community to whom threatening behavior should be reported, and to implement policies and procedures for the assessment of individuals whose behavior may present a threat, and for "appropriate means of intervention with such individuals, and sufficient means of action, including interim suspension or medical separation to resolve potential threats.").

19 The Blueprint is available at: http://www.iaclea.org/visitors/PDFs/VT-taskforce-report_Virginia-Tech.pdf. In preparing the Blueprint, the authors (Raymond H. Thrower, Steven J. Healy, Dr. Gary J. Margolis, Michael Lynch, Dolores Stafford and William Taylor) consulted and referenced the following documents: Mass Shootings at Virginia Tech, April 16, 2007, Report of Review Panel, Presented to Governor Kaine, Commonwealth of Virginia, August 2007; Investigation of April 16, 2007, Critical Incident At Virginia Tech Prepared by Office of the Inspector General For Mental Health, Mental Retardation & Substance Abuse Services, James W. Stewart, III. Report: # 140-07; Presidential Internal Review, Working Group Report on the Interface Between Virginia Tech Counseling Services, Academic Affairs, Judicial Affairs and Legal Systems, Submitted to President Charles Steger, August 12, 2007; Oklahoma Campus Life and Safety and Security Task Force (CLASS) Final Report, January 15, 2008; New Jersey Campus Security Task Force Report, Submitted to Governor Jon S. Corzine, October 2007; Expecting the Unexpected - Lessons from the Virginia Tech Tragedy, by American Association of State Colleges & Universities; The Report of the University of California Campus Security Task Force, University of California Office of the President, January 2008; Gubernatorial Task Force for University Campus Safety, Report on Findings and Recommendations, State of Florida, May 24, 2007; Governor's Task Force on Campus Safety, State of Wisconsin, November 15, 2007; International Association of Campus Law Enforcement Administrators Special Review Task Force on Virginia Tech; Missouri Campus Security Task Force, Report on Findings and Recommendations, August 21, 2007; Association of American Universities, August 2007; Survey on Safety on AAU Campuses after the Virginia Tech Shootings; Report of the Campus Safety Task Force Presented to North Carolina Attorney General Roy Cooper; National Association of Attorneys General, Task Force on School and Campus Safety, Report &

Recommendations, September 2007; Report to the President of the United States on Issues Raised by the Virginia Tech Tragedy, June 13, 2007; The Report of the Virginia Tech Review Panel Synopsis prepared by Charles F. Carletta, JD, Secretary of the Institute and General Counsel, Rensselaer Polytechnic Institute, October 2007.

20 *Addressing Emergencies on Campus*, US Department of Education, Family Policy Compliance Office, at 11 (June 2011). Available at: http://www2.ed.gov/policy/gen/guid/fpco/pdf/emergency-guidance.pdf.

21 See Dobbs, The Law of Torts, § 164 (West Group, 2001) ("On the issue of negligence, a safety custom is often relevant because it reflects the judgment and experience of many people and thus directly suggests how a reasonable person might behave under the circumstances, on the theory that customary behavior is usually not negligent, or on the more specific ground that, under some circumstances, customary behavior tends to prove the proper balance of risks and utilities. . . . . [A] safety custom in a negligence case is relevant evidence tending to show what does or does not count as reasonable care."

22 ASME-ITI Risk Analysis Standard at 1.

23 Ibid., 10.

24 See Dobbs, The Law of Torts, § 164 ("As a sword, the plaintiff can show the defendant's violation of a safety custom as some evidence that defendant failed to act as a reasonable person under the circumstances. In some cases, evidence of the custom is presented by an expert, but the rule is no less applicable if the custom is institutionalized in advisory standards of the relevant industrial association." (citing, e.g., <u>Hansen v. Abrasive Eng'g & Manufacturing, Inc.</u>, 317 Or. 378, 856 P.2d 625 (1993) (ANSI advisory standard deemed admissible but not conclusive)).

25 The court in <u>Getty Petroleum Marketing, Inc. v. Capital Terminal Co.</u>, 391 F.3d 312 (1st Cir. 2004), provided a fair, balanced summary of the law in this area, as follows:

Many cases involve voluntary industry standards that do not have the force of law in the relevant jurisdiction. The overwhelming majority of such cases are negligence actions where the industry standard is offered as evidence of the appropriate standard of care. See, e.g., <u>Miller v. Yazoo Mfg. Co.</u>, 26 F.3d 81, 83 (8th Cir.1994) (in personal injury action, American National Standards Institute lawnmower safety standards were offered to establish standard of care); <u>Matthews v. Ashland Chem., Inc.</u>, 770 F.2d 1303, 1310-11 (5th Cir.1985) (in personal injury action, NFPA, National Electric Code, and the American National Standard Specifications for Accident Prevention Signs were offered to establish standard of care); <u>Boston & Me. R.R. v. Talbert</u>, 360 F.2d 286, 290 (1st Cir.1966) ("certain nationally recognized standards concerning the design of highway and railroad crossings" were offered to establish standard of care, with trial judge's warning that they were "not completely authoritative"); <u>Dickie v. Shockman</u>, No. A3-98-137, 2000 WL 33339623, *3 (D.N.D. July 17, 2000) (in personal injury action, NFPA standards "and other codes applicable within the propane industry" were offered to establish standard of care).

These voluntary standards do not irrefutably establish the standard of care in a negligence case. Rather, they constitute "one more piece of evidence upon which the jury could decide whether the defendant acted as a reasonably prudent person in the circumstances of th[e] case." <u>Boston & Me. R.R.</u>, 360 F.2d at 290. The defendant is free to argue that the standard is unduly demanding, either in general or in the particular instance, and that it does not reflect industry practice or the standard that a reasonably prudent person would employ. After all, voluntary standards are not law; in essence, they are simply recommendations written by

experts who may not themselves be available for cross-examination. In short, the merits of the standard are "for the jury's consideration like any other evidence in the case." Ibid.

Consequently, courts have generally treated such standards as factual evidence that the court may admit or exclude based on ordinary evidentiary principles. See, e.g., Miller, 26 F.3d at 83-84 (voluntary standard was properly admitted); Matthews, 770 F.2d at 1310-11 (voluntary standards were properly excluded); Boston & Me. R.R., 360 F.2d at 290 (voluntary standards were properly admitted); Dickie, 2000 WL 33339623, at *3 (admitting expert testimony regarding voluntary standards).

Getty Petroleum, 391 F.3d at 326-27. See also Kent Village Assocs. Joint Venture v. Smith, 657 A.2d 330, 337 (Md.Ct.Spec.App. 1995) ("[S]afety standards ... may be admitted to show an accepted standard of care, the violation of which may be regarded as evidence of negligence." See also generally Feld, Annotation, Admissibility in Evidence, On Issue of Negligence, of Codes or Standards of Safety Issued or Sponsored by Governmental Body or by Voluntary Association, 58 A.L.R.3d 148 (1974 & 2010 Supp.).

26   ASME-ITI Risk Assessment Standard at 10. The ASME-ITI/ANSI Standard states that "the following resources or equivalent may be helpful in conducting a risk assessment": Randazzo and Plummer, *Implementing Behavioral Threat Assessment on Campus: A Virginia Tech Demonstration Project* (Virginia Polytechnic Institute and State University, 2009), http://www.threatassessment.vt.edu/Implementing_Behavioral_Threat_Assessment.pdf); Deisinger, Randazzo, O'Neill, and Savage, *The Handbook for Campus Threat Assessment & Management Teams* (Applied Risk Management, 2008); *The Virginia Tech Review Panel Report*, August 2007, http://www.vtreviewpanel.org/report/index.html.

27   See *Implementing Behavioral Threat Assessment on Campus* (2009); *The Handbook for Campus TAM Teams* (2008).

28   These steps are summarized from *The Handbook for Campus TAM Teams* (2008).

29   TAM teams that are handling multiple cases can triage the initial reports received to determine which reports merit a full inquiry, and/or which reports should be handled first if all reports are to be investigated. *The Handbook for Campus TAM Teams* (2008) outlines sample screening and triage procedures for this purpose.

30   At institutions where a separate CARE or similar team works with students who may be at risk of suicide, and/or where an EAP or outside resource works with employees who may be at such risk, proper referrals should be made if a TAM team determines that a person of concern poses a risk to him or herself, but not to others. Legal duties to prevent suicide vary substantially based on particular circumstances and state law (discussion of which is beyond the scope of this article), but TAM teams will of course recognize at least some moral duty to attempt to make a referral if that appears necessary.

31   20 U.S.C. § 1232g et seq.

32   A full discussion of these resources and their usefulness for enhancing TAM team operations and effectiveness is beyond the scope of this article. More information can be found in *The Handbook for Campus TAM Teams* (2008).

33   *Implementing Behavioral Threat Assessment on Campus* (2009), another resource recommended in the ASME-ITI/ANSI-approved risk assessment standard, details the specific challenges that Virginia Tech encountered in establishing its threat assessment team following its campus shooting in 2007, and the solutions that it implemented to address those challenges.

34   See *The Virginia Tech Review Panel Report*, August 2007, http://www.vtreviewpanel.org/report/index.html. See also several of the resources consulted by the Blueprint for Safer Campuses (listed in endnote 19, *supra*).

35   See 34 C.F.R. § 99.34(a)(1). See also *Addressing Emergencies on Campus*, at 11 ("schools can respond to student behavior that raises concerns about a student's mental health and the safety of the student and others that is chronic or escalating, by using a threat assessment team, and then may make other disclosures under the health or safety emergency exception, as appropriate, when an 'articulable and significant threat' exists.").

36   See 34 C.F.R. § 99.31(a)(10) and 34 C.F.R. § 99.36.

37   See HHS-DOE, *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Information Portability and Accountability Act of 1996 (HIPAA) to Student Health Records*, http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf.

38   See 45 C.F.R. § 164.512(j).

39   The ADA requires that reasonable accommodations be provided to individuals with a disability, which includes individuals who have a physical or mental impairment that substantially limits a major life activity, conditions that substantially limit the operation of a major bodily function, and mental health conditions that substantially limit an individual's ability to learn, concentrate, think and communicate. The ADA also prohibits discrimination against individuals who have a record of a disability, or who are regarded as having a disability. See generally 42 U.S.C. § 12102.

40   A "direct threat" means a significant risk to the health or safety of others that cannot be eliminated by reasonable accommodation (in the employment context), and/or the elimination or modification of policies, practices or procedures or the provision of auxiliary services (in the student/member of the public context). In assessing whether a direct threat is present, institutions must assess the duration of the risk, the nature and severity of the potential harm, the likelihood that the potential harm will occur, and the imminence of the potential harm. See 42 U.S.C. § 12111(3) (employment context); 42 U.S.C. § 12182(b)(3); 28 C.F.R. §§ 35.104, 35.159, 28 C.F.R §§ 36.104, 36.208 (student/member of the public context).

41   See, e.g., Ascani v. Hofstra University, 173 F.3d 843 (2nd Cir. 1999) (unpublished disposition) (holding that a student who threatened and frightened her professor, and in fact pled guilty to harassment and trespass, was not "otherwise qualified" to continue as a graduate student, even if the behavior was precipitated by her mental illness (citing Palmer v. Circuit Court of Cook County, 117 F.3d 351, 352 (7th Cir.1997) (reaching this conclusion in the work setting), cert. denied, 522 U.S. 1096, 118 S.Ct. 893, 139 L.Ed.2d 879 (1998); Husowitz v. Runyon, 942 F.Supp. 822, 834 (E.D.N.Y.1996) (same)); Bhatt v. University of Vermont, 184 Vt. 195, 958 A.2d 637, 2008 VT 76 (2008) (holding, under state public accommodations law patterned after the ADA, that institution could dismiss a medical student for misconduct allegedly caused by a mental disability, where the misconduct demonstrated that he was not qualified to remain in the program); Williams v. Widnall, 79 F.3d 1003 (10th Cir. 1996) (holding that the Rehabilitation Act did not prohibit termination of employee for threatening his co-workers, even if that behavior was caused by a mental disability; Little v. FBI, 1 F.3d 255, 259 (4th Cir.1993) (same).

42   See cases cited in endnote 41, *supra*. Even in federal circuits where courts have ruled that disciplining an individual for misconduct caused by a disability is the same thing as disciplining the individual for having a disability, see, e.g., Hartog v. Wasatch Academy, 129 F.3d 1076 (10th Cir.

1997) (the 10th Circuit encompasses Oklahoma, Kansas, New Mexico, Colorado, Wyoming and Utah) and <u>Humphrey v. Memorial Hospitals Ass'n</u>, 239 F3d 1128 (9th Cir. 2001) (the Ninth Circuit encompasses California, Washington, Montana, Idaho, Oregon, Nevada, Arizona, Hawaii and Alaska), institutions and employers still do not have to continue to matriculate or employee individuals who are not qualified even with reasonable accommodations, or who pose a "direct threat". See, e.g., <u>Hartog</u>, 129 F.3d at 1087. As noted above, risk managers and TAM teams should work with legal counsel to determine how to best navigate the disability law principles that will be applied to TAM work in their jurisdiction.

43   FERPA regulations provide that students generally have a right to review their "education records," which are defined broadly as personally-identifiable information recorded in any format (subject to various qualifications and exceptions), within 45 days of making a review request. 34 C.F.R. § 99.10. Thus, unless an exception applies, a student of concern could request access to a TAM team's records in the midst of a threat management process, which could be problematic. However, law enforcement unit records are not "education records" subject to disclosure if maintained under the strict mandates of the applicable definition, see 34 C.F.R. § 99.8, and some TAM teams maintain their records with this exemption in mind. Of course, even if documents were not subject to disclosure under FERPA, they might still be subject to disclosure in the context of litigation, a civil rights agency investigation, or under public record laws, if applicable.

44   See *The Handbook for Campus TAM Teams* (2008) for a full discussion of case prioritization and sample priority levels.

45   See *Implementing Behavioral Threat Assessment on Campus* (2009) for a discussion of Virginia Tech's experience hiring several case managers and for a sample case manager position description in the Appendix.

I could not tread these perilous paths in safety,

if I did not keep a saving sense of humor.

—Horatio Nelson (1758–1805),

Soldier in the Royal Navy, particularly during the Napoleonic Wars

URMIA

UNIVERSITY RISK MANAGEMENT &
INSURANCE ASSOCIATION

URMIA National Office
P.O. Box 1027
Bloomington, Indiana 47402
www.urmia.org

PREVENTATIVE MEASURES

BUILDING THREAT ASSESSMENT TEAMS IN SCHOOLS:

THE NaBITA RISK RUBRIC

THE 2019 NATIONAL BEHAVIORAL INTERVENTION TEAM ASSOCIATION (NaBITA) WHITEPAPER

The NaBITA Risk Rubric

THE NaBITA 2019 WHITEPAPER

Authored by
Brett A. Sokolow, J.D.
Brian Van Brunt, Ed.D.
W. Scott Lewis, J.D.
Makenzie Schiemann, M.S.
Amy Murphy, Ph.D.
Jamie Molnar, LMHC

NaBITA
.org
the National Behavioral Intervention Team Association

The NaBITA Risk Rubric
College and University Edition

Authored by

Brett A. Sokolow, J.D.

Brian Van Brunt, Ed.D.

W. Scott Lewis, J.D.

Makenzie Schiemann, M.S.

Amy Murphy, Ph.D.

Jamie Molnar, LMHC

Editorial Consultation and Contributions by:

The NaBITA Advisory Board

CONTENTS

Introduction

Since its introduction in 2009, the NaBITA Threat Assessment Tool has become the most widely used risk rubric by behavioral intervention teams in the United States (Schiemann & Van Brunt, 2018). It is currently used by 92% of Behavioral Intervention Teams (BITs) and is quickly gaining similar traction in PreK-12 school environments and corporate/workplace settings (Schiemann & Van Brunt, 2018).

No matter what other risk assessment inventory or proprietary tools your team uses or accesses, the results of those measures should be funneled back into the NaBITA Risk Rubric to guide team action.

To continue improving the efficacy of the tool and to facilitate its continued adoption and use, NaBITA has completed the second major revision, as detailed in this 2019 Whitepaper.

The first revision of this tool in 2014 focused on more intentional research support and underpinnings of the tool and to cross-validate the tool with other empirically validated threat assessment tools including the Structured Interview for Violence Risk Assessment-35 (SIVRA-35) (Sokolow, Lewis, Schuster, Swinton & Van Brunt, 2014). In this 2019 revision, our primary goal is to build on the ease-of-use inherent within the original tool design, to improve the application of the tool to low-level, early intervention cases. Changes were made to promote precision, clarity and consistency. Teams should find that this revised tool makes their jobs clearer and increases team confidence in decision-making on cases. A second resource will be released to explore the topic of baseline and risk rubric application with case studies.

What has Changed?

- The name of the NaBITA Threat Assessment Tool has changed to the NaBITA Risk Rubric to better reflect the application to all BIT situations, including initial triage, and not only those situations with a threat present. With a more general name, the function of the Risk Rubric as the overarching directional tool for teams should be clearer. No matter what other risk assessment inventory or proprietary tools your team uses or accesses, the results of those measures should be funneled back into the NaBITA Risk Rubric to guide team action. NaBITA has devised four other specific/precise assessment tools for teams or providers to deploy that are intended to feed into the accuracy of the NaBITA Risk Rubric, but the Rubric will work in concert with any validated tool or inventory. For low-level or generalized risks, the NaBITA Risk Rubric should be all you need. Where more specific violence risk assessment is necessary, the SIVRA-35, DD-12, ERIS, and VRAW[2] scales empower teams to laser in to more precise measures, but those measures still inform the overall risk scale of the NaBITA Rubric.
- The revised NaBITA Risk Rubric will be presented in four versions: 1) College and University, 2) PreK-12 Schools, 3) Corporate/Workplace, and Community/ Municipality.
- The risk scales were refined to eliminate overlap among levels and simplify decision-making about risk levels for teams. Previous versions had three levels on the D-Scale, five on the Generalized Risk and nine on the Hostility and Violence Scale. In this revision, they have each been streamlined to four corresponding levels.
- The D-Scale now more overtly incorporates affective (emotionally driven) violence.

- The Hostility and Harm to Others scale on the right flank of the Rubric, now called the E-Scale, has four levels and aligns with the D-Scale on the left flank. Teams will find the four level E-Scale is easier to use and simpler to navigate, increasing consistency of risk ratings. The more poetic and somewhat dramatic language of Glasl (1999) used in the previous version was also streamlined to better reflect the research in the threat assessment community since he published in 1999.
- Elements of the Generalized Risk Rubric, previously in the center of the tool, have been incorporated into both the D-Scale and E-Scale so teams do not have to complete a third rating via the middle scale; instead, the middle scale is simply the resulting determination of the level of risk from the two sides, now called Overall Summary. Users work from the sides to the middle to obtain an overall risk level.
- The interventions on the back of the tool have been enhanced to incorporate various school and workplace settings and to better reflect the emerging intervention and case management practices in the field.

What Hasn't Changed?

- The NaBITA Risk Rubric is still the foundational risk rubric to be used on **_all_** BIT cases and provides a behavioral and risk evaluation for teams. It is our hope that these updates will help teams better learn and apply the rubric to each case that comes to the team.
- The prime learning outcome from NaBITA Whitepapers and our trainings is unchanged as well. It is the industry standard, best practice, and intention of NaBITA in designing the Rubric for teams to enter an overall risk level into a recordkeeping mechanism – preferably a database – EACH AND EVERY time the team considers a subject or there is a situation/incident of significance with that subject. The trend line, tracking, and trajectory identification that this diligence by teams will empower is the key to why NaBITA's approaches have been so effective at preventing violence and empowering interventions within school environments for the last ten years. It takes discipline to record a risk level each time you discuss a subject, but the student-facing teams (to give the most common team example) that have mastered this discipline can show the greatest efficacy, most empowered management of risk, and highest retention, completion, and success rates as a result of their efforts.

> *The NaBITA Risk Rubric is still the foundational risk rubric to be used on all BIT cases and provides a behavioral and risk evaluation for teams.*

- The NaBITA Risk Rubric remains built upon a multidisciplinary field of research related to violence and threat assessment and provides an objective, evidence-based risk rating for cases.
- The NaBITA Risk Rubric is most effective when used in coordination with other BIT Standards of Practice (Van Brunt, Schiemann, Pescara-Kovach, Murphy & Halligan-Avery, 2018) and paired with other assessment tools and resources such as the SIVRA-35, VRAW[2], ERIS, etc.

Importance of Assessing Risk

Since NaBITA's inception, the creation and use of an objective risk assessment has been a crucial component of the BIT process. BITs should engage in three key phases as they work through a case: 1) data gathering, 2) assessment, and 3) intervention (Federal Commission on School Safety, 2018; Fein, Vossekuil & Holden, 1995; Sokolow, Schuster, Lewis & Swinton, 2014). To objectively assess risk, teams must apply a standardized tool to every case – regardless of how serious or how trivial the case may seem. Assessing the level of risk is critical to identifying the safety concerns and deploying the appropriate intervention measures needed to address these concerns (Cornell, Maeng, Burnette, Jia, Huang, Konold, Datta, Malone & Meyer, 2018; National Threat Assessment Center, 2018; Federal Commission on School Safety, 2018; Sokolow, Schuster, Lewis & Swinton, 2014; JED Foundation, 2013; Delworth, 1989). When bias, tradition, culture, or subjective opinions drive the assessment phase, teams run the risk of either over- or under-reacting or missing key indicators of risk (Eells & Rockland-Miller, 2011; Cornell, 2010).

The NaBITA Risk Rubric is designed to be the initial assessment applied to every case. Following this triage assessment, teams should deploy additional assessments and gather additional data to most effectively assess risk. The NaBITA Risk Rubric gives teams a framework for understanding the risk present in a case and offers possible interventions to reduce the risk. Once the rubric is applied, it will often be useful to apply additional assessments measuring unique risk and protective factors. Such risks include, but are not limited to, the potential for suicide or self-harm, violence to others, or other disruptive behaviors in the community. When the NaBITA Risk Rubric is used in tandem with other measures, knowledge, and expertise, the team can assess risk comprehensively and build a successful intervention strategy.

NaBITA Risk Rubric

D-SCALE
Life Stress and Emotional Health

DECOMPENSATING

- Behavior is severely disruptive, directly impacts others, and is actively dangerous. This may include life-threatening, self-injurious behaviors such as:
  - Suicidal ideations or attempts, an expressed lethal plan, and/or hospitalization
  - Extreme self-injury, life-threatening disordered eating, repeated DUIs
  - Repeated acute alcohol intoxication with medical or law enforcement involvement, chronic substance abuse
  - Profoundly disturbed, detached view of reality and at risk of grievous injury or death and/or inability to care for themselves (self-care/protection/judgment)
  - Actual affective, impulsive violence or serious threats of violence such as:
    - Repeated, severe attacks while intoxicated; brandishing a weapon
    - Making threats that are concrete, consistent, and plausible
    - Impulsive stalking behaviors that present a physical danger

DETERIORATING

- Destructive actions, screaming or aggressive/harassing communications, rapid/odd speech, extreme isolation, stark decrease in self-care
  - Responding to voices, extremely odd dress, high risk substance abuse; troubling thoughts with paranoid/delusional themes; increasingly medically dangerous binging/purging
  - Suicidal thoughts that are not lethal/imminent or non-life threatening self-injury
- Threats of affective, impulsive, poorly planned, and/or economically driven violence
  - Vague but direct threats or specific but indirect threat; explosive language
  - Stalking behaviors that do not harm, but are disruptive and concerning

DISTRESSED

- Distressed individuals engage in behavior that concerns others, and have an impaired ability to manage their emotions and actions. Possible presence of stressors such as:
  - Managing chronic mental illness, mild substance abuse/misuse, disordered eating
  - Situational stressors that cause disruption in mood, social, or academic areas
  - Difficulty coping/adapting to stressors/trauma; behavior may subside when stressor is removed, or trauma is addressed/processed
- If a threat is present, the threat is vague, indirect, implausible, and lacks detail or focus

DEVELOPING

- Experiencing situational stressors but demonstrating appropriate coping skills
- Often first contact or referral to the BIT/CARE team, etc.
- Behavior is appropriate given the circumstances and context
- No threat made or present

TRAJECTORY?

OVERALL SUMMARY

CRITICAL

4 — In this stage, there is a serious risk of suicide, life-threatening self-injury, dangerous risk taking (e.g. driving a motorcycle at top speed at night with the lights off) and/or inability to care for oneself. They may display racing thoughts, high risk substance dependence, intense anger, and/or perceived unfair treatment or grievance that has a major impact on the students' academic, social, and peer interactions. The individual has clear target for their threats and ultimatums, access to lethal means, and an attack plan to punish those they see as responsible for perceived wrongs. Without immediate intervention (such as law enforcement or psychiatric hospitalization), it is likely violence will occur. There may be leakage about the attack plan (social media posts that say "I'm going to be the next school shooter" or telling a friend to avoid coming to campus on a particular day). There may be stalking behavior and escalating predatory actions prior to violence such as intimidation, telegraphing, and "test-runs" such as causing a disruption to better understand reaction time of emergency response.

ELEVATED

3 — Behavior at the elevated stage is increasingly disruptive (with multiple incidents) and involves multiple offices such as student conduct, law enforcement, and counseling. The individual may engage in suicidal talk, self-injury, substance intoxication. Threats of violence and ultimatums may be vague but direct or specific but indirect. A fixation and focus on a target often emerge (person, place, or system) and the individual continues to attack the target's self-esteem, public image, and/or access to safety and support. Others may feel threatened around this individual, but any threat lacks depth, follow-through, or a narrowing against an individual, office, or community. More serious social, mental health, academic, and adjustment concerns occur, and the individual is in need of more timely support and resources to avoid further escalation. Conditional ultimatums such as "do this or else" may be made to instructors, peers, faculty, and staff.

MODERATE

2 — Prior to this stage, conflict with others has been fairly limited. The hallmark of moderate is an increase in conflict with others through aggressive speech, actions, and mannerisms. They may become frustrated and engage in non-verbal behaviors or begin to post things on social media, put up posters around campus, or storm away from conversations. Stress, illness, lack of friends, and support are now becoming an increasing concern. The individual may be tearful, sad, hopeless, anxious, or frustrated. This may be caused by difficulty adjusting, dating stress, failure in class assignments, and/or increasing social isolation. If there is a threat or physical violence such as carelessly pushing someone out of their way while storming off, the violence is typically limited and driven by adrenaline and impulsiveness, rather than any deeper plan to hurt others.

MILD

0/1 — The individual here may be struggling and not doing well. The impact of their difficulty is limited around others, with the occasional report being made to the BIT/CARE team out of an abundance of caution and concern rather than any direct behavior or threats. They may be having trouble fitting in, adjusting to college, making friends, or may rub people the wrong way. They alienate others with their thoughts or mannerisms, and there may be minor bullying and conflict. With support and resources, it is likely the individual will be successful adapting and overcoming obstacles. Without support, it is possible they will continue to escalate on the rubric.

BASELINE

E-SCALE
Hostility and Violence to Others

EMERGENCE OF VIOLENCE

- Behavior is moving towards a plan of targeted violence, sense of hopelessness, and/or desperation in the attack plan; locked into an all or nothing mentality
- Increasing use of military and tactical language; acquisition of costume for attack
- Clear fixation and focus on an individual target or group; feels justified in actions
- Attack plan is credible, repeated, and specific; may be shared, may be hidden
- Increased research on target and attack plan, employing counter-surveillance measures, access to lethal means; there is a sense of imminence to the plan
- Leakage of attack plan on social media or telling friends and others to avoid locations

ELABORATION OF THREAT

- Fixation and focus on a singular individual, group, or department; depersonalization of target, intimidating target to lessen their ability to advocate for safety
- Seeking others to support and empower future threatening action; may find extremists looking to exploit vulnerability; encouraging violence
- Threats and ultimatums may be vague or direct and are motivated by a hardened viewpoint; potential leakage around what should happen to fix grievances and injustices
- There is rarely physical violence here, but rather an escalation in the dangerousness and lethality in the threats; they are more specific, targeted, and repeated

ESCALATING BEHAVIORS

- Driven by hardened thoughts or a grievance concerning past wrongs or perceived past wrongs; increasingly adopts a singular, limited perspective
- When frustrated, storms off, disengaged, may create signs or troll on social media
- Argues with others with intent to embarrass, shame, or shut down
- Physical violence, if present, is impulsive, non-lethal, and brief; may seem similar to affective violence, but driven here by a hardened perspective rather than mental health or environmental stress

EMPOWERING THOUGHTS

- Passionate and hardened thoughts; typically related to religion, politics, academic status, money/power, social justice, or relationships
- Rejection of alternative perspectives, critical thinking, empathy, or perspective-taking
- Narrowing on consumption of news, social media, or friendships; seeking only those who share the same perspective
- No threats of violence

TRAJECTORY?

Overview of the NaBITA Risk Rubric

The NaBITA Risk Rubric is designed to assign a specific level of risk to each case discussed by the BIT, each time they are discussed. NaBITA offers a number of resources and guidance that can help new teams move through the analysis and discussion as they apply the risk rubric (www.nabita.org) Let's begin by first revisiting the primary parts of the NaBITA Risk Rubric and how a BIT should use it.

The D-Scale: This scale assesses issues of life stress and emotional health through a series of four progressive levels: *1) Developing, 2) Declining, 3) Deteriorating,* and *4) Decompensating*. As the levels increase, there are more concerning and serious emotional and behavioral health related risks including the potential for affective violence and aggression. The trajectory of this scale is more likely to result in self-harm than in harm to others.

The E-Scale: This scale assesses issues of hostility and violence to others through a series of four progressive levels: *1) Empowering Thoughts, 2) Escalating Behaviors, 3) Elaboration of Threat,* and *4) Emergence of Violence*. The levels increase to address more concerning risk factors for targeted/instrumental violence, hostility, and threats to others. The trajectory of this scale is more likely to result in harm to others than in harm to self, though both risks are present.

> *BITs are designed to have an integrated approach to addressing disruptive and concerning behaviors, mental health risk, student conduct, drug/substance abuse, disability, life adjustment (e.g. relationship break-up, homesickness, grieving, family distress), and threat assessment cases.*

Overall Summary: After the D- and E-Scales are scored, this center section of the risk rubric provides a summation of the four overall risk levels: *1) Mild, 2) Moderate, 3) Elevated,* and *4) Critical*. The user determines the overall risk level by reviewing the D-Scale and the E-Scale. The risk level is reviewed and documented each time a case is discussed and may shift over time as interventions are deployed or the situation evolves. The risk level delineates the level of intervention and action to be considered by the team. It may also be helpful to assign each level on the overall summary a sense of trajectory by assigning a (+) when getting worse and moving up the scale, (-) for when getting better and moving down the scale, and (0) for staying static. So, a situation at level 2 that is escalating is more accurately termed a 2+, whereas a 2 that is de-escalating as the result of successful intervention would have the trajectory of 2-. A static 2 that is not changing dynamically is just a 2.

Interventions: The back of the NaBITA Risk Rubric offers a range of risk-based actions that the team should consider. These interventions are based on the level of risk determined in the Overall Summary (Mild, Moderate, Elevated, and Critical), and they are supported by a decade of successful interventions by teams that have followed their roadmap.

The D-Scale: Life Stress and Emotional Health

BITs are designed to have an integrated approach to addressing disruptive and concerning behaviors, mental health risk, student conduct, drug/substance abuse, disability, life adjustment (e.g. relationship break-up, homesickness, grieving, family distress), and threat assessment cases (Murphy & Halligan-Avery, 2018; Sokolow & Lewis, 2009; Sokolow, Schuster, Lewis & Swinton, 2014; Van Brunt, Schiemann, Pescara-Kovach, 2018). BIT and CARE teams should receive referrals concerning a broad range of issues. Concerns related to suicide, depression, or psychological issues are the most common reasons for referrals to the BIT (Schiemann & Van Brunt, 2018). Closely following are referrals for academic, financial, and social stress (Schiemann & Van Brunt, 2018). This data demonstrates that teams need to be able to assess risk, or concern, for those referrals that *do not* include a mental health crisis or a threat, as well as for those that do include these elements.

The 2019 revision of the D-Scale addresses the need for BITs to assess a wide range of presenting concerns and to ensure focus on early identification of concerning behaviors. Further, BITs are administrative and consultative bodies and not diagnostic teams. The updated D-Scale responds to this administrative function and provides BITs with better clarity and language useful for assessing life stress and emotional health – which may often overlap with mental health – without using diagnostic or clinical language. In doing this, we maintained the core elements of the 2014 D-Scale, as they remain rooted in relevant research (Delworth, 1989; Dunkle, Silverstein & Warner, 2008; 2013; Eells & Rockland-Miller, 2011; JED Foundation, 2008; Van Brunt, 2013). However, we adjusted some of the more clinical terminology to reflect the administrative function of the team and broadened the scope of risk factors in the scale to reflect the preventative nature of BITs.

In mental health diagnostics, the Global Assessment of Functioning (GAF) provides a numerical scale, ranging from 1-100, used by clinicians and physicians to rate the social, occupational, and mental health functioning of individuals (American Psychiatry Association, 2000). We used some of this framework for the categorization of risk in the revised D-Scale. Relevant to the NaBITA Risk Rubric D-Scale, the GAF scores are grouped into 10 different ranges, each indicating a different level of functioning or risk. These levels have been widely accepted in the clinical field as way of conceptualizing an individual's functioning and for developing intervention measures to enhance their functioning (Aas, 2010). The GAF was not included in the newest version of the Diagnostic Statistical Manual (DSM-V), but this decision for exclusion was based on reliability issues when the GAF was applied in clinical settings and used to determine diagnosis and treatment. Given that our application of the GAF was in providing a framework for revising the new D-Scale, the clinical reliability issues were not as relevant here, as we focused on the GAF as a model for administrative teams in categorizing risk and developing interventions.

Additionally, the D-Scale is also rooted in the concept of affective violence, an adrenaline-driven, biological reaction to aggression which leads to the production of adrenaline, increase in heart rate, and resulting body language, behavior, and communication indicators. This allows the BIT to better identify and measure these observable behaviors (Grossman, 1996; 2000; Grossman and Siddle, 2000; Howard, 1999; Hart & Logan, 2011; Hart, Sturmey, Logan & McMuran, 2011; Meloy, 2000; 2002; 2006). In the higher stages, this violence is reactive and impulsive; driven by perceived or actual threats and/or fear. An individual trying to manage and respond to this mixture of vulnerability and physiological

responses, prompted largely by the release of adrenaline, often responds with unpredictable, sponta-neous, affective violence (Howard, 1999).

The D-Scale outlines a progressive decline in the student's coping mechanisms due to a increasingly severe mental health conduction, difficulty adapting to increased stress or some combination of the two. The Developing level has been included to better capture the "pre-risk" category, which is helpful in establishing baseline and encouraging faculty and staff to engage in early, preventative sharing of information to the team.

D-SCALE
Life Stress and Emotional Health

DECOMPENSATING

▲ Behavior is severely disruptive, directly impacts others, and is actively dangerous. This may include life-threatening, self-injurious behaviors such as:
  - ▲ Suicidal ideations or attempts, an expressed lethal plan, and/or hospitalization
  - ▲ Extreme self-injury, life-threatening disordered eating, repeated DUIs
  - ▲ Repeated acute alcohol intoxication with medical or law enforcement involvement, chronic substance abuse
  - ▲ Profoundly disturbed, detached view of reality and at risk of grievous injury or death and/or inability to care for themselves (self-care/protection/judgment)
  - ▲ Actual affective, impulsive violence or serious threats of violence such as:
    - ▲ Repeated, severe attacks while intoxicated; brandishing a weapon
    - ▲ Making threats that are concrete, consistent, and plausible
    - ▲ Impulsive stalking behaviors that present a physical danger

DETERIORATING

■ Destructive actions, screaming or aggressive/harassing communications, rapid/odd speech, extreme isolation, stark decrease in self-care
  - ■ Responding to voices, extremely odd dress, high risk substance abuse; troubling thoughts with paranoid/delusional themes; increasingly medically dangerous binging/purging
  - ■ Suicidal thoughts that are not lethal/imminent or non-life threatening self-injury
■ Threats of affective, impulsive, poorly planned, and/or economically driven violence
  - ■ Vague but direct threats or specific but indirect threat; explosive language
  - ■ Stalking behaviors that do not harm, but are disruptive and concerning

DISTRESSED

● Distressed individuals engage in behavior that concerns others, and have an impaired ability to manage their emotions and actions. Possible presence of stressors such as:
  - ● Managing chronic mental illness, mild substance abuse/misuse, disordered eating
  - ● Situational stressors that cause disruption in mood, social, or academic areas
  - ● Difficulty coping/adapting to stressors/trauma; behavior may subside when stressor is removed, or trauma is addressed/processed
● If a threat is present, the threat is vague, indirect, implausible, and lacks detail or focus

DEVELOPING

◆ Experiencing situational stressors but demonstrating appropriate coping skills
◆ Often first contact or referral to the BIT/CARE team, etc.
◆ Behavior is appropriate given the circumstances and context
◆ No threat made or present

4

3

2

0/1

DEVELOPING

- Experiencing situational stressors but demonstrating appropriate coping skills
- Often first contact or referral to the BIT/CARE team, etc.
- Behavior is appropriate given the circumstances and context
- No threat made or present

DISTRESSED

- Distressed individuals often engage in behavior that concerns others, and have an impaired ability to manage their emotions and actions. Possible presence of stressors such as:
  o Managing chronic mental illness symptoms, mild substance abuse/misuse, disordered eating
  o Situational stressors that cause disruption in mood, social, or academic areas
  o Difficulty coping/adapting to stressors/trauma; behavior may subside when stressor is removed, or trauma is addressed/processed
- If a threat is present, the threat is vague, indirect, implausible, and lacks detail or focus

DETERIORATING

- Destructive actions, screaming or aggressive/harassing communications, rapid/odd speech, extreme isolation, stark decrease in self-care
  o Responding to voices, extremely odd dress, high risk substance abuse; troubling thoughts with paranoid/delusional themes; increasingly medically dangerous binging/purging
  o Suicidal thoughts that are not lethal/imminent or non-life threatening self-injury
- Threats of affective, impulsive, poorly planned, and/or economically driven violence
  o Vague but direct threats or specific but indirect threat; explosive language
  o Stalking behaviors that do not harm, but are disruptive and concerning

DECOMPENSATING

- Behavior is severely disruptive, directly impacts others, and is actively dangerous. This may include life-threatening, self-injurious behaviors such as:
  o Suicidal ideations or attempts, an expressed lethal plan, and/or hospitalization
  o Extreme self-injury, life-threatening disordered eating, repeated DUIs
  o Repeated acute alcohol intoxication with medical or law enforcement involvement, chronic substance abuse
  o Profoundly disturbed, detached view of reality, at risk of grievous injury or death, and/or an inability to care for themselves (self-care/protection/judgment)
- Actual affective, impulsive violence or serious threats of violence such as:
  o Repeated, severe attacks while intoxicated; brandishing a weapon
  o Making threats that are concrete, consistent, plausible
  o Impulsive stalking behaviors that present a physical danger

The following offers a summary of the D-Scale.

DEVELOPING (Level 0-1)

At the developing level, individuals could be described as not being at their best. Here, they are experiencing situational stressors and are demonstrating appropriate coping skills. They may be going through a difficult time, experiencing life stressors, or experiencing mild psychological symptoms, but they are behaving and responding appropriately given the circumstances and context. Individuals in the developing stage have not had prior interactions with or referrals to the team and they are experiencing limited, if any, impact on their ability to be relatively successful, personally and/or academically. Additionally, at Developing we do not see any threat present and no threats have been made. Although individuals scored on this part of the scale are performing well, they are included here to preventatively assess the trajectory of their behavior. In other words, are they likely to worsen if are not connected or supported? The difficulties experienced at this level are risk factors for escalated concern, including exacerbated mental health issues, affective violence, or suicide if they are not addressed. If the team can help those who are upset, lonely, grieving, or experiencing stress in some way, many difficulties can be addressed before they rise to higher levels of concern.

Situational stressors can impact any of us, but our ability to cope means that even if we act out or cause others concern, we return to baseline either because the situational stressors resolve or when our coping mechanisms kick in. Our trajectory is to momentarily spike on the D-Scale, but then quickly return to baseline. The BIT is keeping an eye on Developing situations to ensure that they do return to baseline. It is when the concerns remain despite resolution of the underlying situational stressors that the team would want to take note. If the trajectory moves away from baseline and up the D-Scale, the BIT has more cause for concern and will want to monitor the situation more carefully. Movement up the scale may mean that situational stressors are mounting upon each other, or that coping strategies are not effective.

It bears noting that some students or staff may come to us with a higher baseline, or history of managing these difficulties in a more chronic manner. In other words, they may operate normally in a "Distressed" fashion, but they are able to maintain relationships, progress academically, etc. The team may just want to make sure that these individuals are connected with resources and monitor them.

References: American Psychiatric Association (2013); Adams, Hazelwood & Hayden (2014); Cornell (2010); Drum, Brownson, Denmark & Smith (2009); Eells & Rockland-Miller (2011); Hollingsworth, Dunkle & Douce (2009); JED Foundation (2013); NaBITA and ACCA (2012); Van Norman (2017).

DISTRESSED (Level 2)

At Distressed, we see individuals who are experiencing mental health challenges or situational stressors that are causing difficulty in their life. The individual is not coping or adapting well. They may experience difficulty regulating their emotions (panic attacks, episodes of tearfulness at inappropriate or unexpected times, etc.) and/or difficulty performing at normative levels socially, emotionally, or academically. Individuals at the distressed level may be experiencing challenges related to common development tasks or life stressors such as relationship discord, financial difficulties, feelings of isolation, etc., and are having difficulty in other areas (social, mood, academics, etc.) as a result. This impact, however, is likely the result of the unaddressed presence of a mental health issue, unlearned coping skills, or improperly addressing the situational stressor. The resulting behavior often subsides once the stressor subsides or the mental health issue is addressed.

If the individual is disruptive to others, it is likely to a small group of people closest to them and does not exhibit repeated behaviors of disruption. Additionally, if a threat is present it is vague (not specific as to time, place, means) and indirect (no fixed target), without consistency or detail, or conditional (If X, happened, I might do Y). Often this type of threat is described as passive suicidal ideation, where a person experiences vague thoughts like, "I wish I wasn't here anymore" or "I wish it would all just end," but they do not have any intent or plan to kill themselves. Although the threat is vague, it still presents risk as those at the distressed level are likely experiencing stressors or mental health issues that make them vulnerable and in need of support.

References: American Psychiatric Association (2013); Adams, Hazelwood & Hayden (2014); Cornell (2010); Drum, Brownson, Denmark & Smith (2009); Eells & Rockland-Miller (2011); Hollingsworth, Dunkle & Douce (2009); JED Foundation (2013); NaBITA and ACCA (2012); Van Norman (2017).

DETERIORATING (Level 3)

At this level, we have individuals who are engaging in behavior that is increasingly disruptive or concerning. Their behavior is disruptive in that it is starting to impact others and affect others' ability to be successful personally or academically. This could be through *repeatedly* interrupting the academic community or by placing an *undue* burden of responsibility on others (faculty, staff, classmates) to care for them or watch over them.

The individual at the deteriorating level may also be experiencing significant impact on their emotional health, their social interactions, or their academic performance as a result of a mental health issue or other life stressor. This impact is significant and makes it so that the individual is unable to maintain social relationships and/or to perform as they normally would academically.

The threat of harm at the deteriorating level is neither imminent nor life-threatening. There is likely a threat present, but it is not concrete. For individuals experiencing threats of harm to self, or suicidal ideation, they lack a plan or have a plan which would not be lethal. If they are engaging in self-harm or risky behavior it is concerning and/or disruptive, but not life-threatening. Examples of this behavior would be intentional self-injury that results in superficial wounds or disordered eating that is not yet causing medical complications. Similarly, individuals threatening affective violence at this stage are

likely to make statements that are either vague but direct ("I'm going to make my teacher's life a living hell"), or specific but indirect ("Someone should go all postal on this place"). These threats lack realism and are not likely to be carried out as the plan is not consistent. While individuals at this level may make others feel threatened and their behavior can be aggressive and hostile, they do not pose an imminent threat of harm.

References: American Psychiatric Association (2013); Drum, Brownson, Denmark, & Smith (2009); Hollingsworth, Dunkle & Douce (2009); Grossman (1996; 2000); Howard (1999); JED Foundation (2013); Laur (2002); National Threat Assessment Center (2018).

DECOMPENSATING (Level 4)

This level includes either imminent risk of harm or harm that has already occurred. This includes both harm to self and affective violence (violence driven by emotion rather than carefully planned, intent-driven attacks). Individuals at risk for or engaging in harm to self are either acutely suicidal or are engaging in life-threatening self-harm. They may engage in other risky behavior such as significant substance abuse, extreme disordered eating, frequently driving under the influence, etc. Individuals may be acutely suicidal with a plan to kill themselves, which includes both the intent and the means to follow through on this plan. This plan likely has been communicated, may include a timeline, and it is likely that the individual is going to try to carry it out.

Individuals at this level may also be experiencing a threat to their safety resulting from a detachment from reality that is creating an inability to care for themselves. Their ability to keep themselves safe, eat, shower, etc., is seriously compromised by the disconnect from reality and/or other impairments. At the decompensating level, this self-harm, risky behavior, or lack of ability to care for themselves creates an imminent safety risk – the individual's life is at risk if the behavior is not stopped immediately.

The imminent risk of harm or harm that has already occurred also applies to individuals engaging in or threatening affective, impulsive violence. Affective, or impulsive, violence is reactive and fueled by emotion. Individuals engaging in affective violence at the decompensating level have typically already engaged in the harmful behavior. Examples of this behavior could include viciously attacking someone while intoxicated, brandishing a weapon with an intent to severely harm or kill, multiple instances of uncontrolled, poorly planned physical violence, and/or destroying property that creates a significant safety concern. This may also include impulsive stalking behaviors, intimidation, and/or intimate partner violence that presents a high risk of physical danger. At this juncture, teams are likely acting in support of the Crisis Response Team or law enforcement as opposed to leading management of the case themselves.

References: American Psychiatric Association (2013); Drum, Brownson, Denmark, & Smith (2009); Hollingsworth, Dunkle & Douce (2009); Grossman (1996; 2000); Howard (1999); JED Foundation (2013); Laur (2002); National Threat Assessment Center (2018).

The E-Scale: Hostility and Violence to Others

The E-Scale provides a framework for targeted or predatory violence. This violence is a result of a planned, intent-driven action that is more commonly exhibited by terrorists and those engaging in mission-oriented, instrumental violence such as a school shooting. Targeted violence involves a more strategic, focused attack and a desire for the individual to complete a mission (Meloy, 2000; 2006; Meloy, Hoffmann, Guldimann & James, 2011; O'Toole, 2014; Meloy & Hoffman, 2014; Van Brunt, 2015). This hostility occurs when a person becomes isolated, disconnected, lacks trust, and often feels threatened and frustrated by a perceived attack. They plot and plan their revenge and often execute plans with a militaristic, tactical precision (Meloy, 2000; 2006; Meloy, Hoffmann, Guldimann & James, 2011; Meloy & Hoffman, 2014; O'Toole, 2014).

The levels are outlined here to offer delineated points of opportunity to engage with the individual, intervene, and move them off the pathway to violence.

Such violence and hostility typically develop over time, with those planning attacks often "leaking" information about their plans to others (O'Toole, 2014). This leakage and the nature of stage-by-stage progression provide behavioral intervention and threat assessment teams the potential opportunity to prevent the harm. Targeted violence may be a bit of a misnomer in the sense that the term does not imply a specific target, but instead references threats that are pre-meditated, planned, and methodically executed, rather than those that are spontaneous and more likely to emerge without leakage and therefore without warning.

O'Toole (2014) describes those intending targeted violence as individuals who are mission-oriented. "Mission-oriented shootings are hardly impulsive crimes. They are well-planned and can involve days, weeks, months, even years of making preparations and fantasizing about the crime. The planning is strategic, complex, detailed, and sufficiently secretive to minimize the risk of being detected and maximize the chances for success. The planning does not occur in a vacuum—during this phase, mission-oriented shooters make many decisions, including the types of weapons and ammunition they will use and where to obtain it, the clothes they will wear, the location of the assault, who the victims will be, what they will do at the location, and the date and time of the shooting" (p. 9).

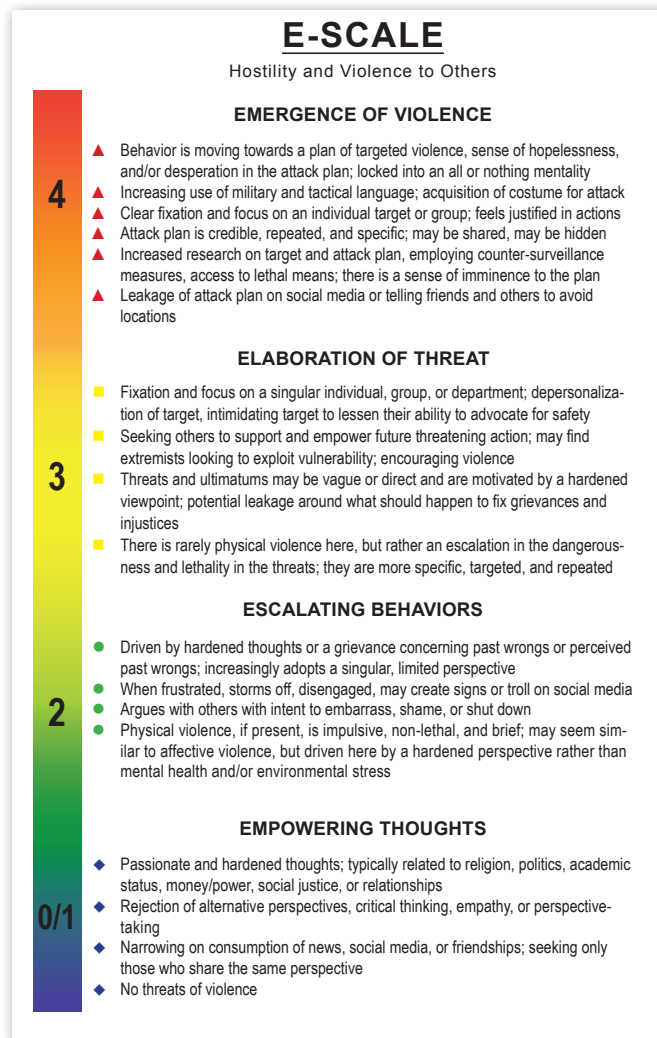The levels are outlined here to offer delineated points of opportunity to engage with the individual, intervene, and move them off the *pathway to violence*, as described by Calhoun and Weston (2003) and Fein et al. (1995). Each of the four levels can be observed and methodically engaged with all necessary resources by law enforcement, campus housing, student conduct, disability services, counseling, and others trained to identify and intervene. Engagement is intended to prevent the individual from further escalation.

Previous versions of the NaBITA Risk Rubric built upon Glasl's (1999) model of crisis escalation. This model provided a useful framework in understanding the progressive acceleration that occurs with individuals prior to such a targeted violent episode. In this update, NaBITA has simplified this model into four stages built upon the research and practical experience of training BIT, CARE, and Threat Assessment Teams from around the world. This helps improve the rubric's clarity, ease of application, and increases its research support.

E-SCALE
Hostility and Violence to Others

4

EMERGENCE OF VIOLENCE

▲ Behavior is moving towards a plan of targeted violence, sense of hopelessness, and/or desperation in the attack plan; locked into an all or nothing mentality
▲ Increasing use of military and tactical language; acquisition of costume for attack
▲ Clear fixation and focus on an individual target or group; feels justified in actions
▲ Attack plan is credible, repeated, and specific; may be shared, may be hidden
▲ Increased research on target and attack plan, employing counter-surveillance measures, access to lethal means; there is a sense of imminence to the plan
▲ Leakage of attack plan on social media or telling friends and others to avoid locations

3

ELABORATION OF THREAT

■ Fixation and focus on a singular individual, group, or department; depersonaliza-tion of target, intimidating target to lessen their ability to advocate for safety
■ Seeking others to support and empower future threatening action; may find extremists looking to exploit vulnerability; encouraging violence
■ Threats and ultimatums may be vague or direct and are motivated by a hardened viewpoint; potential leakage around what should happen to fix grievances and injustices
■ There is rarely physical violence here, but rather an escalation in the dangerous-ness and lethality in the threats; they are more specific, targeted, and repeated

2

ESCALATING BEHAVIORS

● Driven by hardened thoughts or a grievance concerning past wrongs or perceived past wrongs; increasingly adopts a singular, limited perspective
● When frustrated, storms off, disengaged, may create signs or troll on social media
● Argues with others with intent to embarrass, shame, or shut down
● Physical violence, if present, is impulsive, non-lethal, and brief; may seem sim-ilar to affective violence, but driven here by a hardened perspective rather than mental health and/or environmental stress

0/1

EMPOWERING THOUGHTS

◆ Passionate and hardened thoughts; typically related to religion, politics, academic status, money/power, social justice, or relationships
◆ Rejection of alternative perspectives, critical thinking, empathy, or perspective-taking
◆ Narrowing on consumption of news, social media, or friendships; seeking only those who share the same perspective
◆ No threats of violence

Empowering Thoughts

- Passionate and hardened thoughts; typically related to religion, politics, academic status, money/power, social justice, or relationships
- Rejection of: alternative perspectives, critical thinking, empathy, or perspective-taking
- Narrowing on consumption of news, social media, or friendships; seeking only those who share the same perspective
- No threats of violence

Escalating Behaviors

- Driven by hardened thoughts or a grievance concerning past wrongs or perceived past wrongs; increasingly adopts a singular, limited perspective
- When frustrated, storms off, disengages, may create signs or troll on social media
- Argues with others with intent to embarrass, shame, or shut-down
- Physical violence, if present, is impulsive, non-lethal, and brief; may seem similar to affec-tive violence, but driven here by a hardened perspective rather than mental health and/or environmental stress

Elaboration of Threat

- Fixation and focus on a singular individual, group, or department; depersonalization of target, intimidating target to lessen their ability to advocate for safety
- Seeking others to support and empower future threatening action; may find extremists looking to exploit vulnerability; encouraging violence
- Threats and ultimatums may be vague or direct but are motivated by a definitely hardened viewpoint; potential leakage around what should happen to fix grievances and injustices
- There is rarely physical violence here, but rather an escalation in the dangerousness and lethality in the threats; they are more specific, targeted, and repeated

Emergence of Violence

- Behavior is moving towards a plan of targeted violence, sense of hopelessness, and/or desperation in the attack plan; locked into an all or nothing mentality
- Increasing use of military and tactical language; acquisition of costume for attack
- Clear fixation and focus on an individual target or group; feels justified in actions
- Attack plan is credible, repeated, and specific; may be shared, may be hidden
- Increased research on target and attack plan, employing counter-surveillance measures, access to lethal means; there is a sense of imminence to the plan
- Leakage of attack plan on social media or telling friends and others to avoid locations

The following section offers a more detailed description of the E-Scale.

EMPOWERING THOUGHTS (Level 1)

The individual feels a strong passion about a particular belief, while filtering out information that doesn't line up with their beliefs. Common examples include religion, politics, academic expectations, social justice, or relationships. There are no threats or specific targeted individuals identified at this phase. These beliefs may be demonstrated by social media posts or wearing inflammatory articles of clothing.

It bears noting that some students or staff may come to us with a higher baseline (a history of their behavior that has a more chronic expectation) on the E-Scale. In other words, they may operate normally in a "Empowering" or "Escalating" fashion, but they are able to maintain relationships, progress academically, etc. One could argue the current political climate lends itself to encouraging these as normative behaviors. That said, the team may just want to make sure that these individuals are connected with resources and monitor them.

References: ATAP (2006); ASIS & SHRM (2011); Glasl (1999); Meloy et al. (2011); O'Toole (2002); Randazzo & Plummer (2009); Sokolow et al. (2011); Sokolow & Lewis (2009); Turner & Gelles (2003); Van Brunt, Murphy & Zedginidze (2017); Van Brunt (2012; 2015).

ESCALATING BEHAVIORS (Level 2)

The individual at this level begins to argue and confront others around them in harmful debate with an intent to polarize. Here, being right supersedes the facts, and they seek to impose their beliefs on others or encourage common cause. They frequently engage in confrontations with others as a result.

The individual finds their previous arguments and discussions unsatisfactory and begins to storm off or become aggressive when challenged. This leads to an increase in non-verbal behaviors which communicate their frustration and anger. There is a move away from debate and dialogue and a move toward further objectification and depersonalization. This may include the use of signs and posters, social media posts, and passive aggressive behavior. If there is any physical violence at this phase, it is impulsive, non-lethal, and brief. This acting out looks similar to affective violence on the D-Scale, but here it is driven by a strongly held perspective and/or belief set, rather than a mental health condition or reaction to environmental stress.

References: ATAP (2006); ASIS & SHRM (2011); Glasl (1999); Meloy & Hoffman (2014); Meloy et al. (2011); Randazzo & Plummer (2009); Sokolow et al. (2011); Sokolow & Lewis (2009); Turner & Gelles (2003); O'Toole (2002); Van Brunt (2012; 2015).

ELABORATION OF THREAT (Level 3)

Here, there is a crystalizing of a target and a fixation and focus on an individual, group, department, or organization. They find others who support their beliefs by joining groups or clubs, organizations, teams, reading books, or accessing online resources. They seek to confirm their ideas and find ways to intimidate and confront others beyond verbal arguments. There is a shaming or embarrassing of the target and a desire to *unmask* them in the community. There is further objectifying and depersonalizing of the target's feelings, thoughts, and actions. They may challenge the target with a "do this or else" conditional ultimatum. There may be a threat of punishment if the target does not comply with the threats and demands. Threats are infused with credibility, but there is rarely physical violence at this stage and only an increase in threatening language or leaked of plan details. If there is physical violence, it mirrors the affective violence on the D-Scale and it is impulsive and non-lethal, expressive, and reactive.

At this juncture, teams skilled at emerging threat detection may be acting in concert with a Crisis Response Team and/or law enforcement as opposed to solely managing the case.

References: ATAP (2006); ASIS & SHRM (2011); Drysdale et al. (2010); Glasl (1999); Meloy & Hoffman (2014); Meloy et al. (2011); Randazzo & Plummer (2009); Sokolow et al. (2011); Sokolow & Lewis (2009); Turner & Gelles (2003); O'Toole (2002); O'Toole & Bowman (2011); Turner & Gelles (2003); U.S. Postal Service (2007); Van Brunt (2012; 2015).

EMERGENCE OF VIOLENCE (Level 4)

The early stage of this phase can involve test runs at carrying out the attack plan on the target or a substitute target. These may include destroying the target's possessions, invasive monitoring of their family, friends, or social circle, or gathering information to better harm the target. Intentional leakage is rarer at this stage than in Level 3 (Elaboration of Threat) but may occur inadvertently, as the preparation behavior for the final step on the pathway to violence is observed by others despite efforts to keep it covert. As the planning moves forward, the attacker increasingly uses militaristic and tactical language, developing strategies to carry out their plan. They may desire to live after an attack to continue to spread their message or have a growing awareness they may die in the attack. They are often full of

hopelessness, desperation, and suicidal thoughts and have a sense of inevitability related to their attack

In each case that comes to the team, the NaBITA Risk Rubric should be used as an initial assessment to determine next steps for further data collection, assessment, and/or intervention. It is useful to use both the D and E scales first and then confirm the overall category by referencing the overall summary.

plan. Detaching from meaningful relationships, giving away prized possessions, extremely flat affect, or warning some people away from the target are abstracted forms of leakage that may characterize this stage. They justify their violence based on their hardened perspective.

At this juncture, teams are likely acting in support of the Crisis Response Team or law enforcement, as opposed to managing the case.

References: ATAP (2006); ASIS & SHRM (2011); Drysdale et al. (2010); Glasl (1999); Meloy & Hoffman (2014); Meloy et al. (2011); Randazzo & Plummer (2009); Sokolow et al. (2011); Sokolow & Lewis (2009); Turner & Gelles (2003); O'Toole (2014); O'Toole & Bowman (2011); Turner & Gelles (2003); U.S. Postal Service (2007); Van Brunt (2012; 2015); Vossekuil et al. (2000; 2002).

Overall Summary

In each case that comes to the team, the NaBITA Risk Rubric should be used as an initial assessment to determine next steps for further data collection, assessment, and/or intervention. It is useful to use both the D and E scales first and then confirm the overall category by referencing the overall summary. Each case is different, so every element of the summary may not apply to each case. Instead, the summary offers an overall description to help the team better evaluate the risk.

Teams should use an additional descriptor to address movement or trajectory (-, +), when assigning an individual to a Mild, Moderate, Elevated, or Critical level. Our goal is to keep the NaBITA Risk Rubric straightforward and easily understood so that it can be applied to each case. These visual descriptions of trajectory were designed to help teams better capture individuals who are getting worse (-) and moving up the scale, getting better (+) and moving down the scale, or remaining the same.

OVERALL SUMMARY

CRITICAL

In this stage, there is a serious risk of suicide, life-threatening self-injury, dangerous risk taking (e.g. driving a motorcycle at top speed at night with the lights off) and/or inability to care for oneself. They may display racing thoughts, high risk substance dependence, intense anger, and/or perceived unfair treatment or grievance that has a major impact on the students' academic, social, and peer interactions. The individual has clear target for their threats and ultimatums, access to lethal means, and an attack plan to punish those they see as responsible for perceived wrongs. Without immediate intervention (such as law enforcement or psychiatric hospitalization), it is likely violence will occur. There may be leakage about the attack plan (social media posts that say "I'm going to be the next school shooter" or telling a friend to avoid coming to campus on a particular day). There may be stalking behavior and escalating predatory actions prior to violence such as intimidation, telegraphing, and "test-runs" such as causing a disruption to better understand reaction time of emergency response.

ELEVATED

Behavior at the elevated stage is increasingly disruptive (with multiple incidents) and involves multiple offices such as student conduct, law enforcement, and counseling. The individual may engage in suicidal talk, self-injury, substance intoxication. Threats of violence and ultimatums may be vague but direct or specific but indirect. A fixation and focus on a target often emerge (person, place, or system) and the individual continues to attack the target's self-esteem, public image, and/or access to safety and support. Others may feel threatened around this individual, but any threat lacks depth, follow-through, or a narrowing against an individual, office, or community. More serious social, mental health, academic, and adjustment concerns occur, and the individual is in need of more timely support and resources to avoid further escalation. Conditional ultimatums such as "do this or else" may be made to instructors, peers, faculty, and staff.

MODERATE

Prior to this stage, conflict with others has been fairly limited. The hallmark of moderate is an increase in conflict with others through aggressive speech, actions, and mannerisms. They may become frustrated and engage in non-verbal behaviors or begin to post things on social media, put up posters around campus, or storm away from conversations. Stress, illness, lack of friends, and support are now becoming an increasing concern. The individual may be tearful, sad, hopeless, anxious, or frustrated. This may be caused by difficulty adjusting, dating stress, failure in class assignments, and/or increasing social isolation. If there is a threat or physical violence such as carelessly pushing someone out of their way while storming off, the violence is typically limited and driven by adrenaline and impulsiveness, rather than any deeper plan to hurt others.

MILD

The individual here may be struggling and not doing well. The impact of their difficulty is limited around others, with the occasional report being made to the BIT/CARE team out of an abundance of caution and concern rather than any direct behavior or threats. They may be having trouble fitting in, adjusting to college, making friends, or may rub people the wrong way. They alienate others with their thoughts or mannerisms, and there may be minor bullying and conflict. With support and resources, it is likely the individual will be successful adapting and overcoming obstacles. Without support, it is possible they will continue to escalate on the rubric.

Overall Summary Category	Descriptions
Mild (-)	Questionable if even needed to be shared with the BIT; report often made out of an abundance of caution.
Mild	Some minor concerns, typically the individual will access services on their own or with a slight nudge from BIT.
Mild (+)	Minor concerns, but likely the situation will worsen without added support and intervention.
Moderate (-)	Minor conflict exists, but is sporadic and lacks consistency. Stress and emotional disruption may exist.
Moderate	Individual in need of further outreach. Struggling with interpersonal relationships, grades, academics, etc.
Moderate (+)	Likely involvement from multiple departments (counseling, conduct, disability). Escalation likely.
Elevated (-)	Multiple conflicts, inconsistent emotional state, suicidal thoughts, disruptive conduct behavior inconsistently popping up, interpersonal conflict sporadic.
Elevated	Fairly consistent disruptive behavior, emotional concerns, suicidal thoughts, and/or substance risk. Interpersonal conflict frequent.
Elevated (+)	High level of concern over current behavior paired with likelihood of escalation to an attack or violence. Crisis response and law enforcement likely involved at this point.
Critical (-)	Actively planning violence to self or others, at the stage of considering action. Crisis response and law enforcement definitively involved at this point.
Critcal	Attack or suicide occurs or about to occur. Crisis response and law enforcement definitively involved at this point.

MILD (-, +)

The individual here may be struggling and their coping mechanisms may be failing or eroding. The impact of their difficulty is limited around others, with the occasional report being made to the BIT/CARE team out of an abundance of caution and concern rather than any direct behavior or threats. They may be having trouble fitting in, adjusting to college, making friends, or may rub people the wrong way. They alienate others with their thoughts or mannerisms and there may be minor bullying and conflict. With support and resources, it is likely the individual will be successful at adapting and overcoming obstacles. Without support, it is likely they will continue to escalate up the rubric.

MODERATE (-, +)

Prior to this stage, conflict with others has been fairly limited. The hallmark of moderate is an increase in conflict with others through aggressive speech, actions, and mannerisms. They may become frustrated and engage in non-verbal behaviors or begin to post things on social media, put up posters around campus, or storm away from conversations. Stress, illness, lack of friends, and support are now becoming an increasing concern. The individual may be tearful, sad, hopeless, anxious, irritable, or frustrated. This may be caused by difficulty adjusting, dating stress, failure in class assignments, and/or increasing social isolation and life stressors. If there is a threat or physical violence, such as impulsively pushing someone out of their way while storming off, the violence is typically limited and driven by adrenaline and impulsiveness, rather than any deeper plan to hurt others.

ELEVATED (-, +)

Behavior at the elevated stage is increasingly disruptive and often will involve multiple offices such as student conduct, law enforcement, and counseling. Disruptive behavior is frequent with multiple incidents, often surrounding certain staff, locations, or individuals. The individual may engage in suicidal talk, self-injury that is not life-threatening, or substance intoxication without a life-risk. Threats of violence and ultimatums may be vague but direct ("If I don't get my financial aid check from you today, things aren't going to go well for you") or specific but indirect ("I know people who have guns, it wouldn't be hard to do something here on campus"). A fixation and focus for the individual's frustration often emerge here, and they may try to make a person, place, or system feel more vulnerable by attacking self-esteem, image, and access to safety and support. Others may feel threatened around this individual, but any threats lack depth, follow-through, or a narrowing against an individual, office, or community. More serious social, mental health, academic, and adjustment concerns occur, and the individual is in need of more timely support and resources to avoid further escalation. Conditional ultimatums such as "do this or else" may be made to instructors, peers, faculty, and staff.

CRITICAL (-, +)

In this stage, there may be a serious risk of suicide, life-threatening self-injury, dangerous risk-taking (e.g. driving a motorcycle at top speed at night with the lights off), and/or inability to care for oneself. Racing thoughts, substance dependence, intense anger, and perceived unfair treatment or grievance may create a major impact on the indivdual's academic, social, and peer interactions. The individual may have a clear target for their threats and ultimatums, lethal means, and an attack plan to punish those they see as responsible for perceived wrongs. They seek to punish those who are responsible for their grievances and the injustices they have suffered. ***Without immediate intervention*** (such as law enforcement or psychiatric hospitalization), it is likely violence will occur. There may be leakage about the attack plan (social media posts that say "I'm going to be the next school shooter" or telling a friend to avoid coming to campus on a particular day) or the individual may go dark and become tactical. There may be stalking behavior and escalating predatory actions prior to violence such as intimidation, telegraphing, and "test-runs," such as causing a disruption to better understand reaction time of emergency response.

Once the level of risk has been assessed, it is the team's responsibility to identify the interventions appropriate to the risk present. A thoughtful intervention responds to the assessed risk level and is tailored to the individual's core issues.

Interventions

Once the level of risk has been assessed, it is the team's responsibility to identify the interventions appropriate to the risk present. A thoughtful intervention responds to the assessed risk level and is tailored to the individual's core issues (Hollingsworth, Dunkle & Douce, 2009). When the intervention is not in response to the assessed level of risk and is not tailored to the individual, teams run the risk of either over- or under-reacting to the individual, and thus not providing the individual or the community at large with the response or intervention needed for safety (Sokolow, Schuster, Lewis & Swinton, 2014). To guide the decision-making related to interventions, the NaBITA Risk Rubric identifies a pool of interventions appropriate at each risk level. The list of interventions within each risk level should be seen as a toolbelt of interventions. Not every case will require every tool to solve it – teams must be thoughtful in selecting the most appropriate tool or tools for the job at hand.

The following section offers a summary of the interventions offered in a college environment.

**INTERVENTION OPTIONS TO ADDRESS RISK
AS CLASSIFIED**

CRITICAL (4)
- Initiate wellness check/evaluation for involuntary hold or police response for arrest
- Coordinate with necessary parties (student conduct, police, etc.) to create plan for safety, suspension, or other interim measures
- Obligatory parental/guardian/emergency contact notification unless contraindicated
- Evaluate need for emergency notification to community
- Issue mandated assessment once all involved are safe
- Evaluate the need for involuntary/voluntary withdrawal
- Coordinate with university police and/or local law enforcement
- Provide guidance, support, and safety plan to referral source/stakeholders

ELEVATED (3)
- Consider a welfare/safety check
- Provide guidance, support, and safety plan to referral source/stakeholders
- Deliver follow up and ongoing case management or support services
- Required assessment such as the SIVRA-35, ERIS, HCR-20, WAVR-20 or similar; assess social media posts
- Evaluate parental/guardian/emergency contact notification
- Coordinate referrals to appropriate resources and provide follow-up
- Likely referral to student conduct or disability support services
- Coordinate with university police/campus safety, student conduct, and other departments as necessary to mitigate ongoing risk

MODERATE (2)
- Provide guidance and education to referral source
- Reach out to student to encourage a meeting
- Develop and implement case management plan or support services
- Connect with offices, support resources, faculty, etc. who interact with student to enlist as support or to gather more information
- Possible referral to student conduct or disability support services
- Offer referrals to appropriate support resources
- Assess social media and other sources to gather more information
- Consider VRAW^2 for cases that have written elements
- Skill building in social interactions, emotional balance, and empathy; reinforcement of protective factors (social support, opportunities for positive involvement)

MILD (0/1)
- No formal intervention; document and monitor over time
- Provide guidance and education to referral source
- Reach out to student to offer a meeting or resources, if needed
- Connect with offices, support resources, faculty, etc. who interact with student to enlist as support or to gather more information

Mild Interventions

- No formal intervention; document and monitor over time
- Provide guidance and education to referral source
- Reach out to student to offer a meeting or resources, if needed
- Connect with offices, support resources, faculty, etc., who interact with the individual to offer support or to gather more information

Moderate Interventions

- Provide guidance and education to referral source
- Reach out to individual to encourage a meeting
- Develop and implement case management plan or support services
- Connect with offices, support resources, faculty, etc. who interact with student to enlist as support or to gather more information
- Possible referral to student conduct or disability support services
- Offer referrals to appropriate support resources
- Assess social media and other sources to gather more information
- Consider VRAW^2 for cases that have written elements
- Skill building in social interactions, emotional balance, and empathy; reinforcement of protective factors (social support, opportunities for positive involvement)

Elevated Interventions

- Consider a welfare/safety check
- Provide guidance, support, and safety plan to referral source/stakeholders
- Deliver follow-up and ongoing case management or support services
- Required assessment such as the SIVRA-35, ERIS, HCR-20, WAVR-20, or similar; assess social media posts
- Evaluate parental/guardian/emergency contact notification
- Coordinate referrals to appropriate resources and provide follow-up
- Likely referral to student conduct or disability support services
- Coordinate with university police/campus safety, student conduct, and other departments as necessary to mitigate ongoing risk

Critical Interventions

- Initiate wellness check/evaluation for involuntary hold or police response for arrest
- Coordinate with necessary parties (student conduct, police, etc.) to create a plan for safety, suspension, or other interim measures
- Obligatory parental/guardian/emergency contact notification unless contraindicated
- Evaluate need for emergency notification to community
- Issue mandated assessment once all involved are safe
- Evaluate the need for involuntary/voluntary withdrawal
- Coordinate with university police and/or local law enforcement
- Provide guidance, support, and safety plan to referral source/stakeholders

The following section offers a more detailed description of the interventions.

MILD INTERVENTIONS

Interventions at the mild level are significantly more hands-off than at the other levels. While team members/case managers can certainly still meet with individuals at the mild level of risk, it is likely not needed. Remember, here the individual is being referred out of an abundance of caution and concern rather than from any direct behavior or threats. In many cases the team may not engage directly with them at all. If the individual of concern is already connected to the appropriate resources, the team may adopt a hands-off approach where the team notes the concerns prompting the referral and the resources the individual is connected to as part of an information gathering and monitoring process. If they are not engaged, connected, or aware of all community resources, teams might consider a soft-outreach from a case manager or other team member offering resource information the individual may find helpful.

Similar to what is suggested at the moderate level, here teams have an opportunity to partner with the referral source, or other known supports, to connect them with resources and to observe their behavior for any signs they are escalating. The team will want to get a preliminary sense of baseline and trajectory here if possible. Individuals at the mild level are likely to be successful once connected to supports. In many cases, coaching the referral source might be helpful in guiding them in responding to or supporting the individual. For example, an intervention for a student referred by their RA for experiencing homesickness might be to coach the RA on how to have a conversation with the student and to work with them on getting involved on campus. For those navigating food or housing insecurities, a conversation with a case manager to explore institutional and community resources should occur.

References: NABITA & ACCA (2012); Van Norman (2017); Adams, Hazelwood & Hayden (2014); JED Foundation (2013); Dunkle, Silverstein & Warner (2008); Hollingsworth, Dunkle & Douce (2009).

MODERATE INTERVENTIONS

The focus of the interventions at the moderate level lies in coordinating resources and supports to individuals who are struggling. At the moderate level, case management is a key strategy for teams. At this level of risk, case management is solution-focused and looks at helping individuals overcome the variety of stressors they are experiencing. Within a week or less of receiving the referral, teams should offer the individual a meeting with a case manager or with someone on the team serving in this capacity. While this meeting is voluntary, team members should be thoughtful about how they present the opportunity to meet so that it is appealing to the individual. In offering this meeting, it can be helpful to explain how the meeting can benefit them and what supports or resources there may be to relieve some of their difficulty. Removing stigma and barriers as well as establishing the helpful nature of the process is key in engaging the individual in voluntary referrals.

Referrals will be based on individual needs and could include counseling, wellness coaching, career services, student activities or clubs, financial aid, academic resources, or social service supports such as food pantries, homeless shelters, etc. At the moderate level, the case manager should

work together with the individual to identify the resources most appropriate for their needs and then assist them in connecting with the resources. Case management is not a one and done approach. Follow-up in the form of additional meetings, phone calls, or emails, can be beneficial in not only bridging the individual to the support resources and ensuring they are connected but also monitoring the effect such supports have on the individual's trajectory.

At a moderate level of risk, teams also have an opportunity to engage their outer circle members, and/or the referring faculty/staff member in providing support. Often, the referring party or another outer circle member may have a pre-existing relationship with the individual which can be leveraged in connecting the individual with resources or in reducing the behavior of concern. Teams can coach the referring party on how they can engage with the individual and can offer strategies for preventing a recurrence of the behavior.

References: NABITA & ACCA (2012); Van Norman (2017); Adams, Hazelwood & Hayden (2014); JED Foundation (2013); Dunkle, Silverstein & Warner (2008); Hollingsworth, Dunkle & Douce (2009).

ELEVATED INTERVENTIONS

These interventions are designed to mitigate the concern, provide support, and further assess the individual. Perhaps the most useful tool in your toolbelt at the elevated level is an assessment, which should be voluntary if possible, but should also be mandated if the subject is not willing to volunteer. An assessment gives teams an opportunity to seek or perform an evaluation to determine the individual's functioning, risk factors present, and ongoing interventions that may reduce the risk. The results of an assessment provide teams with the critical information they need to determine what interventions to use moving forward.

Teams must also evaluate the need to initiate a welfare/wellness check, parental/guardian/emergency contact notification, and/or a referral to student conduct, HR, or disability services. Each individual will vary. This is an opportunity for teams to tailor the approach to the specific needs of the person of concern. In cases where safety is a concern, teams may need to either call the individual and make immediate contact to establish safety or initiate a wellness check by a mental health professional, the local crisis unit, or law enforcement. Teams should also consider parental/guardian/emergency contact notification at the elevated level. Some elements to consider include the level of health and safety risk present and whether the emergency contact is a known support or a known risk factor. If the case involves disruption to others or other violations of the code of conduct, it is usually appropriate to refer the case to conduct. Teams need to find a balance between referring every policy violation present in the case to conduct and ensuring that individuals are held accountable for their behavior so as to mitigate future escalation of behavior. BIT is not meant as a diversion around student conduct, but often it's the timing of the referral that is the key.

At Elevated, it is critical that the individual receives ongoing support and case management, whether this support comes from a case manager dedicated to the team, or from individual team members serving as case managers to individuals referred to the team. In either case, someone needs to be assigned to the case who is responsible for meeting with the individual, assessing their needs, connecting them with resources, and providing follow-up support to ensure ongoing connection. This

outreach to the individual should happen quickly. At the elevated level, contact to the individual should be coordinated within hours of receiving the referral. Additionally, given the level of concern at the elevated level, case management cannot be a "one and done" approach. In many cases, the ongoing support will involve multiple meetings, facilitating referrals, and ensuring connection with resources like counseling, disability support, academic support, and/or psychiatric care. Releases of information should be secured where needed so that the case manager and/or the team can receive updates about how the individual is doing and whether they remain connected with the resource. Simply referring an individual to these resources is insufficient and ineffective case management at the elevated level.

References: Dunkle, Silverstein, & Warner (2008); JED Foundation (2008, 2013); Hollingsworth, Dunkle & Douce (2009); NaBITA & ACCA (2012); Adams, Hazelwood, & Hayden (2014); Drum, Brownson, Denmark & Smith (2009).

CRITICAL INTERVENTIONS

At this level, interventions are first and foremost directed at establishing safety. Depending on the nature of the situation, this may mean establishing the safety of the individual or of the community. In instances of harm-to-self, suicidal ideation, or inability to care for oneself, it is the team's goal to deploy interventions that keep the individual safe. At the Critical level, this is likely to require a welfare/wellness check by a mental health professional, the local crisis unit, or law enforcement to initiate an involuntary hospitalization. The welfare/wellness check should be initiated immediately, and an emergency team meeting should be called to discuss the case.

In instances of threats of harm to others, the interventions will be aimed at stopping the individual from engaging in violence and protecting the target of violence. Again, at this level, it is likely that the individual will be hospitalized and/or arrested given the severity of the behavior and the imminence of the threat present. To protect the safety of the target of the violence, teams should coordinate with university police, local law enforcement, student conduct, etc. to evaluate the need for an emergency notification to the community and/or to an individual target. Teams should also work with these departments to ensure interim measures for safety are in place such as no-contact orders, trespass or *persona non grata* orders, interim suspension, etc. Again, teams should deploy these interventions immediately and call an emergency team meeting to coordinate all of the safety measures.

While a mandated assessment for individuals at this level may eventually be necessary to understand ongoing risk and potential for future violence, it is not the focus of the interventions at the critical level. Individuals at Critical are experiencing too much distress and/or are imminently at risk of engaging in harm and therefore a mandated assessment is further down the line of interventions. In other words, the behavior or risk is too severe for a mandated assessment – safety is the first priority and the mandated assessment can come later, after the individual's release from the hospital or jail.

Given the severity of the behavior and threat at the critical level, it is likely that the individual will need to be separated from the community. Preferably, this separation occurs through the conduct process or a voluntary withdrawal or leave, but teams should have the option for an involuntary withdrawal if there is imminent concern for safety. As a result of the imminent concern for the health and safety of the individual, and the potential for removal from the institution, teams will often feel an obligation to notify the student's parent(s)/guardian(s)/emergency contact to discuss the behavior and concerns for safety, assuming this is not somehow contraindicated. Teams should use this opportunity to build alliances with the emergency contact and engage them as allies in the process of establishing safety.

Removing an individual from the institution may not eliminate the threat to the community. Partnering with the parent(s)/guardian(s)/emergency contact, as well as local law enforcement and support resources, is key in bridging the continuity of risk assessment and management.

References: Eells & Rockland-Miller (2011); Dunkle, Silverstein & Warner (2008); JED Foundation (2008, 2013); Deisinger, Randazzo, O'Neill & Savage (2008); Nolan, Randazzo & Deisinger (2011); Deisinger & Scalora (2016); Drum, Brownson, Denmark & Smith (2009); Hollingsworth, Dunkle & Douce (2009); National Threat Assessment Center (2018).

Frequently Asked Questions (FAQ)

What if a team wants to keep using the earlier version of the tool?

You certainly can keep using the tool. The new version of the Risk Rubric has improved research support and more consistent categories to help teams correct errors. One common mistake to ensure you are addressing in documentation with the previous tool is noting the D-Scale with a 1-9 score when that is reserved for the hostility and violence scale. There is also an emphasis on attending and responding to lower risk behaviors that was suggested by Homeland security and the Secret Service.

How should a team appropriately document the change to the new tool in existing cases?

Simply noting the NaBITA Risk Rubric (2019 edition) may on new cases will suffice. Note the elevated threshold remains the critical separation point for more intensive interventions.

What other versions of the tool are available?

There are currently three versions of the too. It was formalized in 2009, updated in 2014 and the current update the Risk Rubric was completed in the spring of 2019.

What resources are there to train teams on the new tool?

NaBITA is committed to providing a range of training options on the tool. These include this 2019 whitepaper, in-person training lectures, a 20-minute online summary, a detailed online video summary along with case study applications. In the summer of 2019, additional resources including the Baseline, Trajectory and Intervention guide, NaBITA 2019 Risk Rubric Update webinar, an updated 21 questions flow logic for the Risk Rubric and an online version of the Risk Rubric.

Applying the NaBITA Risk Rubric

The NaBITA Risk Rubric is designed to be applied to all cases as an initial triage tool for the team to develop an intervention strategy. The information contained in the referral, collateral, and background gathered by the team is used to determine the level of risk and the appropriate interventions based on that risk. The D-Scale assesses for life stress and emotional health, the E-Scale assesses for hostility and violence to others, and the Overall Summary conceptualizes the overall risk, indicating to the team the appropriate resources, support, and interventions to deploy.

Having the NaBITA Risk Rubric readily available during team meetings can be instrumental to keep team members on task and focus the discussion on the objective assessment of risk. One practical way of doing this is to print and laminate color copies of the rubric and have the chair bring them to each meeting.

When you apply the D-Scale and E-Scale, risk is determined based on the type of concerns present in the case. Cases involving an emotional health issue, life stressor, suicide or self-harm, affective violence, or other general well-being concern will be assessed on the D-Scale, while cases involving hostility, aggression, predatory violence, or threats of harm to others will be assessed on the E-Scale. The D-Scale and the E-Scale provide detailed and specific indicators of risk and threat, allowing teams to make an accurate assessment of where the individual falls on the Overall Summary Scale. Once this has been determined, teams select interventions from the corresponding risk level. Starting with the correct side of the rubric is critical, because it will help the team to determine the trajectory the individual may follow. While the rubric is not predictive, because a team cannot know if an individual will mitigate, remain static, or escalate, the rubric does help teams to understand what a person of concern will be facing if they mitigate or escalate.

Having the NaBITA Risk Rubric readily available during team meetings can be instrumental to keep team members on task and focus the discussion on the objective assessment of risk. One practical way of doing this is to print and laminate color copies of the rubric and have the chair bring them to each meeting. The chair can then easily direct the conversation and team members' attention to the rubric during case discussions. Once the risk level is determined by the team, it should be documented in the team's record, along with a note about the interventions the team has decided to deploy. It is important to note that risk is not stagnant. An individual's level of risk will shift over time as a result of your team deploying appropriate interventions and teams should continually gather available information, reassess the level of risk using the NaBITA Risk Rubric, and note any changes in risk in the record.

References

Ass, I.M. (2010). Global Assessment of Functioning (GAF): Properties and frontier of current knowledge. *Annals of General Psychiatry*. Retrieved from www.annals-general-psychiatry.com/content/9/1/20

Adams, S., Hazelwood, S. Hayden, B. (2014). Student affairs case management: Merging social work theory with student affairs practice. Journal of Student Affairs Research and Practice, 51(4), 446-458.

American Psychiatric Association (2013). Diagnostic and statistical manual of mental disorders (4th ed.). Washington, DC:.

ASIS International and the Society for Human Resource Management. (2011). Workplace violence prevention and intervention: American National Standard. Retrieved from www.asisonline.org/guidelines/published.htm

Association of Threat Assessment Professionals (ATAP) (2006). Risk Assessment Guideline Elements for Violence (RAGE-V): Considerations for Assessing the Risk of Future Violent Behavior. ATAP.

Calhoun, T., & Weston, S. (2003). Contemporary threat management. San Diego: Specialized Training Services.

Cornell, D. (2010). Threat assessment in college settings. Change (8–15). Retrieved from www.changemag.org.

Cornell, D., Maeng, J., Burnette, A., Jia, Y., Huang, F., Konold,T., Datta, P., Malone, M. and Meyer, P. (2018). Student threat assessment as a standard school safety practice: Results from a statewide implementation study. School Psychology Quarterly, 33(2), 213-222.

Deisinger, G., Randazzo, M., O'Neill, D. & Savage, J. (2008). The handbook of campus threat assessment and management teams. Applied Risk Management, LLC.

Deisinger, E., and Scalora, M. (2016). Threat assessment and management in higher education in the United States: A review of the 10 years since the mass casualty incident at Virginia Tech. Journal of Threat Assessment and Management, 3(3-4), 186-199.

Delworth, U. (Ed.). (1989). Dealing with the behavioral and psychological problems of students; New Directions for Student Services. San Francisco: Jossey-Bass.

Dunkle, J. H., Silverstein, Z. B., & Warner S. L. (2008). Managing violent and other troubling students: The role of threat assessment teams on campus. Journal of College and University Law, 34(3): 585–636.

Drum, D., Brownson, C., Burton Denmark, A., & Smith, S. (2009). New data on the nature of suicidal crises in college students: Shifting the paradigm. Professional Psychology: Research and Practice, 40(3), 213-222.

Drysdale, D., Modzeleski, W. & Simons, A. (2010). Campus Attacks: Targeted violence affecting institutions of higher education. Washington, DC: United States Secret Service, United States Department of Education and Federal Bureau of Investigation.

Eells, G.T. & Rockland-Miller, H.S. (2011). Assessing and responding to disturbed and disturbing students: Understanding the role of administrative teams in institutions of higher education. Journal of College Student Psychotherapy, 25:8-23.

Federal Commission on School Safety (2018). Final Report on the Federal Commission on School Safety. Retrieved on February 24, 2019 from https://www2.ed.gov/documents/school-safety/school-safety-report.pdf

Fein, R., Vossekuil, B., Holden, G. (1995). Threat assessment: An approach to prevent targeted violence (NCJ 155000). Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Glasl, F. (1999). Confronting Conflict: A First-Aid Kit for Handling Conflict. A. Stroud, UK: Hawthorn Press.

Grossman, D. (1996). On Killing: The Psychological Cost of Learning to Kill in War and Society. New York: Back Bay Books.

Grossman, D. (2000). Aggression and Violence, in Oxford Companion to American Military History. New York: Oxford University Press.

Grossman, D. & Siddle, B. (2000). Psychological effects of combat, in Encyclopedia of Violence, Peace and Conflict. Kidlington, UK: Academic Press.

Hart, S., & Logan, C. (2011). Formulation of violence risk used evidence-based assessment: The structured professional judgment approach. In P. Sturmey & M. McMurran (Eds.), Forensic case formulation (83–106). Chichester, England: Wiley-Blackwell.

Hart, S., Sturmey, P., Logan, C., & McMuran, M. (2011). Forensic case formulation. International Journal of Forensic Mental Health, 10, 118–126.

Howard, P.J. (1999). The Owner's Manual for The Brain: Everyday Applications from Mind-Brain Research (2nd Ed.). Bard Press.

Hollingsworth, K., Dunkle, J., and Douce, L. (2009). The high-risk (disturbed and disturbing) college student. New Directions for Student Services 128, 37-54.

JED Foundation (2008). Student mental health and the law: A resource for institutions of higher education. New York: JED Foundation.

JED Foundation. (2013). Balancing safety and support on campus: A guide to campus teams. NY, NY: JED Foundation.

Laur, D. (2002). The Anatomy of Fear and How it Relates to Survival Skills Training. Cleveland, OH: Integrated Street Combatives.

Meloy, J. (2000). Violence risk and threat assessment: A practical guide for mental health and criminal justice professionals. San Diego, CA: Specialized Training Services.

Meloy, J. R. (2002). "Stalking and violence," in J. Boon & L. Sheridan (Eds), Stalking and Psychosexual Obsession: Psychological Perspectives for Prevention, Policing, and Treatment West Sussex, UK: John Wiley & Sons, Ltd.

Meloy, J. R. (2006). The empirical basis and forensic application of affective and predatory violence. Australian and New Zealand Journal of Psychiatry, 40: 539–47.

Meloy, J., Hoffmann, J., Guldimann, A. and James, D. (2011). The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology. Behavioral Sciences and the Law.

Meloy, R. & Hoffman, J. (Ed.s) (2014). The International Handbook of Threat Assessment. New York, NY: Oxford University Press.

NaBITA and ACCA (2012). Case Management in Higher Education. A publication of the National Behavioral Intervention Team Association and the American College Counseling Association.

National Threat Assessment Center. (2018). Enhancing school safety using a threat assessment model: An operational guide for preventing targeted school violence. U.S. Secret Service, Department of Homeland Security.

Nolan, J., Randazzo, M. and Deisinger, G. Campus Threat Assessment and Management Teams: What Risk Managers Need to Know Now. URMIA Journal Reprint, retrieved on February 24, 2019 from http://www.sigmatma.com/wp-content/uploads/2014/02/NolanRandazzoDeisinger_Campus-ThreatAssessmentTeams_FINAL_20110802.pdf

O'Toole, M. E. (2002). The school shooter: A threat assessment perspective. FBI.

O'Toole, M. E. (2014). The Mission-Oriented Shooter: A New Type of Mass Killer. Journal of Violence and Gender, 1(1), 9-10.

O'Toole, M. E. & Bowman, A. (2011). Dangerous instincts: How gut feelings betray. New York: Hudson Street Press.

Randazzo, M. and Plummer, E. (2009). Implementing Behavioral Threat Assessment on Campus: A Virginia Tech Demonstration Project. Printed by Virginia Polytechnic Institute and State University, Blacksburg, Va.

Schiemann, M. and Van Brunt, B. (2018). Summary and analysis of 2018 NaBITA Survey data. The Journal of Behavioral Intervention Teams (J-BIT), 6, p. 42-57.

Sokolow, B., Lewis, W., Schuster, S., Swinton, D., and Van Brunt, B. (2014). Threat assessment in the campus setting: The NaBITA 2014 whitepaper. Malvern, PA: National Association of Behavioral Intervention Teams (NaBITA).

Sokolow, B. & Lewis, S. (2009). 2nd Generation Behavioral Intervention Best Practices. Malvern, PA: The National Center for Higher Education Risk Management.

Sokolow, B., Lewis, S., Manzo, L., Schuster, S., Byrnes, J. & Van Brunt, B. (2011). Book on BIT. A publication of the National Behavioral Intervention Team Association (www.nabita.org).

Turner, J. and Gelles, M. (2003). Threat Assessment: A Risk Management Approach. NY, NY: Routledge.

United States Postal Service (2007). Threat Assessment Team Guide, www.nalc.org/depart/cau/pdf/manuals/Pub%20108%20(2007-Mar).pdf

Van Brunt, B. (2012). Ending Campus Violence: New Approaches to Prevention. New York, NY: Routledge.

Van Brunt, B. (2013). A Comparative Analysis of Threat and Risk Assessment Measures in the Journal of Campus Behavioral Intervention (J-BIT), 1 (111-151). Publication of the National Behavioral Intervention Team Association (NaBITA).

Van Brunt B. (2015). Harm to Others: The Assessment and Treatment of Dangerousness. (American Counseling Association, Alexandria, VA).

Van Brunt, B., Murphy, A. and Zedginidze, A. (2017). An exploration of the risk, protective, and mobilization factors related to violent extremism in college populations. Journal of Violence and Gender, 4(3), 81-101.

Van Brunt, B., Schiemann, M., Pescara-Kovach, L., Murphy, A. Halligan-Avery, E. (2018) Standards for Behavioral Intervention Teams. Journal of Campus Behavioral Intervention (J-BIT), 6, p. 29-41.

Van Norman, J.D (2017). Case management's impact on graduation, retention, and suicide at Colorado State University. Journal of Campus Behavioral Intervention (J-BIT), 5, 75-83.

Vossekuil, B., Fein, R., Reddy, M., Borum, R. & Modzeleski, W. (2002). The Final Report and Findings of the Safe School Initiative: Implications for the prevention of school attacks in the United States. Retrieved from www.secretservice.gov/ntac/ssi_fi nal_report.pdf

Vossekuil, B., Reddy, M., Fein, R., Borum, R. & Modzeleski, M. (2000). USSS Safe School Initiative: An Interim Report on the Prevention of Targeted Violence in Schools. Washington, DC: U.S. Secret Service, National Threat Assessment Center.

NaBITA

www.nabita.org

NaBITA Risk Rubric

E-SCALE
Hostility and Violence to Others

OVERALL SUMMARY

D-SCALE
Life Stress and Emotional Health

E-SCALE

4 — EMERGENCE OF VIOLENCE

▲ Behavior is moving towards a plan of targeted violence, sense of hopelessness, and/or desperation in the attack plan; locked into an all or nothing mentality
▲ Increasing use of military and tactical language; acquisition of costume for attack
▲ Clear fixation and focus on an individual target or group; feels justified in actions
▲ Attack plan is credible, repeated, and specific; may be shared, may be hidden
▲ Increased research on target and attack plan, employing counter-surveillance measures, access to lethal means; there is a sense of imminence to the plan
▲ Leakage of attack plan on social media or telling friends and others to avoid locations

3 — ELABORATION OF THREAT

■ Fixation and focus on a singular individual, group, or department; depersonalization of target, intimidating target to lessen their ability to advocate for safety
■ Seeking others to support and empower future threatening action; may find extremists looking to exploit vulnerability; encouraging violence
■ Threats and ultimatums may be vague or direct and are motivated by a hardened viewpoint; potential leakage around what should happen to fix grievances and injustices
■ There is rarely physical violence here, but rather an escalation in the dangerousness and lethality in the threats; they are more specific, targeted, and repeated

2 — ESCALATING BEHAVIORS

● Driven by hardened thoughts or a grievance concerning past wrongs or perceived past wrongs; increasingly adopts a singular, limited perspective
● When frustrated, storms off, disengaged, may create signs or troll on social media
● Argues with others with intent to embarrass, shame, or shut down
● Physical violence, if present, is impulsive, non-lethal, and brief; may seem similar to affective violence, but driven here by a hardened perspective rather than mental health and/or environmental stress

0/1 — EMPOWERING THOUGHTS

◆ Passionate and hardened thoughts; typically related to religion, politics, academic status, money/power, social justice, or relationships
◆ Rejection of alternative perspectives, critical thinking, empathy, or perspective-taking
◆ Narrowing on consumption of news, social media, or friendships; seeking only those who share the same perspective
◆ No threats of violence

OVERALL SUMMARY

4 — CRITICAL

In this stage, there is a serious risk of suicide, life-threatening self-injury, dangerous risk taking (e.g. driving a motorcycle at top speed at night with the lights off) and/or inability to care for oneself. They may display racing thoughts, high risk substance dependence, intense anger, and/or perceived unfair treatment or grievance that has a major impact on the students' academic, social, and peer interactions. The individual has clear target for their threats and ultimatums, access to lethal means, and an attack plan to punish those they see as responsible for perceived wrongs. Without immediate intervention (such as law enforcement or psychiatric hospitalization), it is likely violence will occur. There may be leakage about the attack plan (social media posts that say "I'm going to be the next school shooter" or telling a friend to avoid coming to campus on a particular day). There may be stalking behavior and escalating predatory actions prior to violence such as intimidation, telegraphing, and "test-runs" such as causing a disruption to better understand reaction time of emergency response.

3 — ELEVATED

Behavior at the elevated stage is increasingly disruptive (with multiple incidents) and involves multiple offices such as student conduct, law enforcement, and counseling. The individual may engage in suicidal talk, self-injury, substance intoxication. Threats of violence and ultimatums may be vague but direct or specific but indirect. A fixation and focus on a target often emerge (person, place, or system) and the individual continues to attack the target's self-esteem, public image, and/or access to safety and support. Others may feel threatened around this individual, but any threat lacks depth, follow-through, or a narrowing against an individual, office, or community. More serious social, mental health, academic, and adjustment concerns occur, and the individual is in need of more timely support and resources to avoid further escalation. Conditional ultimatums such as "do this or else" may be made to instructors, peers, faculty, and staff.

2 — MODERATE

Prior to this stage, conflict with others has been fairly limited. The hallmark of moderate is an increase in conflict with others through aggressive speech, actions, and mannerisms. They may become frustrated and engage in non-verbal behaviors or begin to post things on social media, put up posters around campus, or storm away from conversations. Stress, illness, lack of friends, and support are now becoming an increasing concern. The individual may be tearful, sad, hopeless, anxious, or frustrated. This may be caused by difficulty adjusting, dating stress, failure in class assignments, and/or increasing social isolation. If there is a threat or physical violence such as carelessly pushing someone out of their way while storming off, the violence is typically limited and driven by adrenaline and impulsiveness, rather than any deeper plan to hurt others.

0/1 — MILD

The individual here may be struggling and not doing well. The impact of their difficulty is limited around others, with the occasional report being made to the BIT/CARE team or threats. They may be having trouble fitting in, adjusting to college, making friends, or may rub people the wrong way. They alienate others with their thoughts or mannerisms, and there may be minor bullying and conflict. With support and resources, it is likely the individual will be successful adapting and overcoming obstacles. Without support, it is possible they will continue to escalate on the rubric.

BASELINE

D-SCALE

4 — DECOMPENSATING

▲ Behavior is severely disruptive, directly impacts others, and is actively dangerous. This may include life-threatening, self-injurious behaviors such as:
▲ Suicidal ideations or attempts, an expressed lethal plan, and/or hospitalization
▲ Extreme self-injury, life-threatening disordered eating, repeated DUIs
▲ Repeated acute alcohol intoxication with medical or law enforcement involvement, chronic substance abuse
▲ Profoundly disturbed, detached view of reality and at risk of grievous injury or death and/or inability to care for themselves (self-care/protection/judgment)
▲ Actual affective, impulsive violence or serious threats of violence such as:
   ▲ Repeated, severe attacks while intoxicated; brandishing a weapon
   ▲ Making threat that are concrete, consistent, and plausible
   ▲ Impulsive stalking behaviors that present a physical danger

3 — DETERIORATING

■ Destructive actions, screaming or aggressive/harassing communications, rapid/odd speech, extreme isolation, stark decrease in self-care
■ Responding to voices, extremely odd dress, high risk substance abuse; troubling thoughts with paranoid/delusional themes; increasingly medically dangerous binging/purging
■ Suicidal thoughts that are not lethal/imminent or non-life threatening self-injury
■ Threats of affective, impulsive, poorly planned, and/or economically driven violence
   ■ Vague but direct threats or specific but indirect threat; explosive language
   ■ Stalking behaviors that do not harm, but are disruptive and concerning

2 — DISTRESSED

● Distressed individuals engage in behavior that concerns others, and have an impaired ability to manage their emotions and actions. Possible presence of stressors such as:
   ● Managing chronic mental illness, mild substance abuse/misuse, disordered eating
   ● Situational stressors that cause disruption in mood, social, or academic areas
   ● Difficulty coping/adapting to stressors/trauma; behavior may subside when stressor is removed, or trauma is addressed/processed
● If a threat is present, the threat is vague, indirect, implausible, and lacks detail or focus

0/1 — DEVELOPING

◆ Experiencing situational stressors but demonstrating appropriate coping skills
◆ Often first contact or referral to the BIT/CARE team, etc.
◆ Behavior is appropriate given the circumstances and context
◆ No threat made or present

TRAJECTORY?   TRAJECTORY?

INTERVENTION OPTIONS TO ADDRESS RISK AS CLASSIFIED

CRITICAL (4)
- Initiate wellness check/evaluation for involuntary hold or police response for arrest
- Coordinate with necessary parties (student conduct, police, etc.) to create plan for safety, suspension, or other interim measures
- Obligatory parental/guardian/emergency contact notification unless contraindicated
- Evaluate need for emergency notification to community
- Issue mandated assessment once all involved are safe
- Evaluate the need for involuntary/voluntary withdrawal
- Coordinate with university police and/or local law enforcement
- Provide guidance, support, and safety plan to referral source/stakeholders

ELEVATED (3)
- Consider a welfare/safety check
- Provide guidance, support, and safety plan to referral source/stakeholders
- Deliver follow up and ongoing case management or support services
- Required assessment such as the SIVRA-35, ERIS, HCR-20, WAVR-20 or similar; assess social media posts
- Evaluate parental/guardian/emergency contact notification
- Coordinate referrals to appropriate resources and provide follow-up
- Likely referral to student conduct or disability support services
- Coordinate with university police/campus safety, student conduct, and other departments as necessary to mitigate ongoing risk

MODERATE (2)
- Provide guidance and education to referral source
- Reach out to student to encourage a meeting
- Develop and implement case management plan or support services
- Connect with offices, support resources, faculty, etc. who interact with student to enlist as support or to gather more information
- Possible referral to student conduct or disability support services
- Offer referrals to appropriate support resources
- Assess social media and other sources to gather more information
- Consider VRAW[2] for cases that have written elements
- Skill building in social interactions, emotional balance, and empathy; reinforcement of protective factors (social support, opportunities for positive involvement)

MILD (0/1)
- No formal intervention; document and monitor over time
- Provide guidance and education to referral source
- Reach out to student to offer a meeting or resources, if needed
- Connect with offices, support resources, faculty, etc. who interact with student to enlist as support or to gather more information

CRITICAL

ELEVATED

MODERATE

MILD

NaBITA.org

LEGAL CONSIDERATIONS:

BALANCING STUDENT PRIVACY AND SCHOOL SAFETY: A GUIDE TO FERPA FOR COLLEGES AND UNIVERSITIES

Balancing Student Privacy and School Safety: A Guide to the *Family Educational Rights and Privacy Act* for Colleges and Universities

make a reasonable attempt to notify the student about the disclosure, unless the student initiates the disclosure. Additionally, upon request, the institution must provide a copy of the information disclosed and an opportunity for a hearing. *See* 34 CFR § 99.31(a)(2) and § 99.34(a).
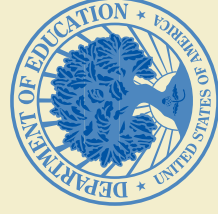
Contact Information

For further information about *FERPA*, please contact the Family Policy Compliance Office or visit its Web site.

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Ave. S.W.
Washington, DC 20202-5920
202-260-3887

For quick, informal responses to routine questions about *FERPA*, school officials may e-mail the Family Policy Compliance Office at FERPA@ED.Gov.

For inquiries about *FERPA* compliance training, contact FERPA.Client@ED.Gov.

Additional information and guidance may be found at FPCO's Web site at: http://www.ed.gov/policy/gen/guid/fpco/index.html.

• A school official may generally share with a parent information that is based on that official's personal knowledge or observation of the student.

FERPA and Student Health Information

Postsecondary institutions that provide health or medical services to students may share student medical treatment records with parents under the circumstances described above. While these records may otherwise be governed by the *Health Insurance Portability and Accountability Act of 1996* (*HIPAA*), the *HIPAA* Privacy Rule excludes student medical treatment records and other records protected by *FERPA*. The Department plans to issue further guidance on the interplay between *FERPA* and *HIPAA*.

FERPA and Student and Exchange Visitor Information System (SEVIS)

FERPA permits institutions to comply with information requests from the Department of Homeland Security (DHS) and its Immigration and Customs Enforcement Bureau (ICE) in order to comply with the requirements of SEVIS. Officials who have specific questions about this and other matters involving international students should contact the U.S. Department of Education's Family Policy Compliance Office.

Transfer of Education Records

Finally, *FERPA* permits school officials to disclose any and all education records, including disciplinary records, to another institution at which the student seeks or intends to enroll. While student consent is not required for transferring education records, the institution's annual *FERPA* notification should indicate that such disclosures are made. In the absence of information about disclosures in the annual *FERPA* notification, school officials must

Postsecondary officials are regularly asked to balance the interests of safety and privacy for individual students. While the *Family Educational Rights and Privacy Act* (*FERPA*) generally requires institutions to ask for written consent before disclosing a student's personally identifiable information, it also allows colleges and universities to take key steps to maintain campus safety. Understanding the law empowers school officials to act decisively and quickly when issues arise.

Health or Safety Emergency

In an emergency, *FERPA* permits school officials to disclose without student consent education records, including personally identifiable information from those records, to protect the health or safety of students or other individuals. At such times, records and information may be released to appropriate parties such as law enforcement officials, public health officials, and trained medical personnel. *See* 34 CFR § 99.31(a)(10) and § 99.36. This exception to *FERPA*'s general consent rule is limited to the period of the emergency and generally does not allow for a blanket release of personally identifiable information from a student's education records. In addition, the Department interprets *FERPA* to permit institutions to disclose information from education records to parents if a health or safety emergency involves their son or daughter.

Disciplinary Records

While student disciplinary records are protected as education records under *FERPA*, there are certain circumstances in which disciplinary records may be disclosed without the student's consent. A postsecondary institution may disclose to an alleged victim of any crime of violence or non-forcible sex offense the final results of a disciplinary proceeding conducted by the institution against the alleged perpetrator of that crime, regardless of whether the institution concluded a violation was committed. An institution may disclose to anyone—not just the victim—the final results of a disciplinary proceeding, if it determines that the student is an alleged

perpetrator of a crime of violence or non-forcible sex offense, and with respect to the allegation made against him or her, the student has committed a violation of the institution's rules or policies. *See* 34 CFR §§ 99.31(a)(13) and (14).

The Clery Act

The *Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act* requires postsecondary institutions to provide timely warnings of crimes that represent a threat to the safety of students or employees and to make public their campus security policies. It also requires that crime data be collected, reported, and disseminated to the campus community and to the Department annually. The *Clery Act* is intended to provide students and their families with accurate, complete, and timely information about safety on campuses so that they can make informed decisions. Such disclosures are permitted under *FERPA*. The following Web site provides more information about these and other provisions about campus safety: http://www.ed.gov/admins/lead /safety/campus. html.

Law Enforcement Unit Records

Many colleges and universities have their own law enforcement units to monitor safety and security in and around campus. Institutions that do not have a specific law enforcement units may designate a particular office or school official to be responsible for referring potential or alleged violations of law to local police authorities. Investigative reports and other records created and maintained by these law enforcement units are not considered education records subject to *FERPA*. Accordingly, institutions may disclose information from law enforcement unit records to anyone, including outside law enforcement authorities, without student consent. *See* 34 CFR § 99.8.

While an institution has flexibility in deciding how to carry out safety functions, it must also indicate in its policy or in information provided to students which office or school official serves as the college or university's "law enforcement unit." (The institution's notification to students of their rights under *FERPA* can include this designation. As an example, the Department has posted a model notification on its Web site at http://www.ed.gov/policy/gen/guid /fpco/ferpa/ps-officials.html.)

Law enforcement unit officials who are employed by the college or university should be designated in the institution's *FERPA* notification as "school officials" with a "legitimate educational interest." As such, they may be given access to personally identifiable information from students' education records. The institution's law enforcement unit officials must protect the privacy of education records it receives and may disclose them only in compliance with *FERPA*. For that reason, it is advisable that law enforcement unit records be maintained separately from education records.

Disclosure to Parents

When a student turns 18 years old or enters a postsecondary institution at any age, all rights afforded to parents under *FERPA* transfer to the student. However, *FERPA* also provides ways in which schools may share information with parents without the student's consent. For example:

- Schools may disclose education records to parents if the student is a dependent for income tax purposes.

- Schools may disclose education records to parents if a health or safety emergency involves their son or daughter.

- Schools may inform parents if the student who is under age 21 has violated any law or its policy concerning the use or possession of alcohol or a controlled substance.

LEGAL CONSIDERATIONS:
THE APPLICATION OF FERPA AND HIPAA TO STUDENT HEALTH RECORDS

U.S. Department of Health
and Human Services

U.S. Department of Education

Joint Guidance on the Application of the
Family Educational Rights and Privacy Act (*FERPA*)
And the *Health Insurance Portability and*
Accountability Act of 1996 (*HIPAA*)
To Student Health Records

November 2008

Contents

1. Does the HIPAA Privacy Rule apply to an elementary or secondary school?

2. How does FERPA apply to health records on students maintained by elementary or secondary schools?

3. Does FERPA or HIPAA apply to elementary or secondary school student health records maintained by a health care provider that is not employed by a school?

4. Are there circumstances in which the HIPAA Privacy Rule might apply to an elementary or secondary school?

5. Where the HIPAA Privacy Rule applies, does it allow a health care provider to disclose protected health information (PHI) about a troubled teen to the parents of the teen?

6. Where the HIPAA Privacy Rule applies, does it allow a health care provider to disclose protected health information (PHI) about a student to a school nurse or physician?

7. Does FERPA or HIPAA apply to records on students at health clinics run by postsecondary institutions?

8. Under FERPA, may an eligible student inspect and review his or her "treatment records"?

9. Under FERPA, may an eligible student's treatment records be shared with parties other than treating professionals?

10. Under what circumstances does FERPA permit an eligible student's treatment records to be disclosed to a third-party health care provider for treatment?

11. Are all student records maintained by a health clinic run by a postsecondary institution considered "treatment records" under FERPA?

12. Does FERPA or HIPAA apply to records on students who are patients at a university hospital?

13. Where the HIPAA Privacy Rule applies, does it permit a health care provider to disclose protected health information (PHI) about a patient to law enforcement, family members, or others if the provider believes the patient presents a serious danger to self or others?

14. Does FERPA permit a postsecondary institution to disclose a student's treatment records or education records to law enforcement, the student's parents, or others if the institution believes the student presents a serious danger to self or others?

15. Are the health records of an individual who is both a student and an employee of a university at which the person receives health care subject to the privacy provisions of FERPA or those of HIPAA?

16. Can a postsecondary institution be a "hybrid entity" under the HIPAA Privacy Rule?

I.   Introduction

The purpose of this guidance is to explain the relationship between the *Family Educational Rights and Privacy Act* (*FERPA*) and the *Health Insurance Portability and Accountability Act of 1996* (*HIPAA*) Privacy Rule, and to address apparent confusion on the part of school administrators, health care professionals, and others as to how these two laws apply to records maintained on students. It also addresses certain disclosures that are allowed without consent or authorization under both laws, especially those related to health and safety emergency situations. While this guidance seeks to answer many questions that school officials and others have had about the intersection of these federal laws, ongoing discussions may cause more issues to emerge. Contact information for submitting additional questions or suggestions for purposes of informing future guidance is provided at the end of this document. The Departments of Education and Health and Human Services are committed to a continuing dialogue with school officials and other professionals on these important matters affecting the safety and security of our nation's schools.

II.   Overview of *FERPA*

FERPA is a Federal law that protects the privacy of students' "education records." (See 20 *U.S.C.* § 1232g; 34 *CFR* Part 99). *FERPA* applies to educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education. This includes virtually all public schools and school districts and most private and public postsecondary institutions, including medical and other professional schools. If an educational agency or institution receives funds under one or more of these programs, *FERPA* applies to the recipient as a whole, including each of its components, such as a department within a university. See 34 *CFR* § 99.1(d).

Private and religious schools at the elementary and secondary level generally do not receive funds from the Department of Education and are, therefore, not subject to *FERPA*. Note that a private school is not made subject to *FERPA* just because its students and teachers receive services from a local school district or State educational agency that receives funds from the Department. The school itself must receive funds from a program administered by the Department to be subject to *FERPA*. For example, if a school district places a student with a disability in a private school that is acting on behalf of the school district with regard to providing services to that student, the records of that student are subject to *FERPA*, but not the records of the other students in the private school. In such cases, the school district remains responsible for complying with *FERPA* with respect to the education records of the student placed at the private school.

An educational agency or institution subject to *FERPA* may not have a policy or practice of disclosing the education records of students, or personally identifiable information from education records, without a parent or eligible student's written consent. See 34 *CFR* § 99.30. *FERPA* contains several exceptions to this general consent rule. See 34 *CFR* § 99.31. An "eligible student" is a student who is at least 18 years of age or who attends a postsecondary institution at any age. See 34 *CFR* §§ 99.3 and 99.5(a). Under *FERPA*, parents and eligible students have the right to inspect and review the student's education records and to seek to have them amended in certain circumstances. See 34 *CFR* §§ 99.10 – 99.12 and §§ 99.20 – 99.22.

The term "education records" is broadly defined to mean those records that are: (1) directly related to a student, and (2) maintained by an educational agency or institution or by a party acting for the

agency or institution. See 34 *CFR* § 99.3. At the elementary or secondary level, a student's health records, including immunization records, maintained by an educational agency or institution subject to *FERPA*, as well as records maintained by a school nurse, are "education records" subject to *FERPA*. In addition, records that schools maintain on special education students, including records on services provided to students under the *Individuals with Disabilities Education Act (IDEA),* are "education records" under *FERPA*. This is because these records are (1) directly related to a student, (2) maintained by the school or a party acting for the school, and (3) not excluded from the definition of "education records."

At postsecondary institutions, medical and psychological treatment records of eligible students are excluded from the definition of "education records" if they are made, maintained, and used only in connection with treatment of the student and disclosed only to individuals providing the treatment. See 34 *CFR* § 99.3 "Education records." These records are commonly called "treatment records." An eligible student's treatment records may be disclosed for purposes other than the student's treatment, provided the records are disclosed under one of the exceptions to written consent under 34 *CFR* § 99.31(a) or with the student's written consent under 34 *CFR* § 99.30. If a school discloses an eligible student's treatment records for purposes other than treatment, the records are no longer excluded from the definition of "education records" and are subject to all other *FERPA* requirements.

The *FERPA* regulations and other helpful information can be found at:
http://www.ed.gov/policy/gen/guid/fpco/index.html.

III.   Overview of *HIPAA*

Congress enacted *HIPAA* in 1996 to, among other things, improve the efficiency and effectiveness of the health care system through the establishment of national standards and requirements for electronic health care transactions and to protect the privacy and security of individually identifiable health information. Collectively, these are known as *HIPAA*'s Administrative Simplification provisions, and the U.S. Department of Health and Human Services has issued a suite of rules, including a privacy rule, to implement these provisions. Entities subject to the *HIPAA* Administrative Simplification Rules (see 45 *CFR* Parts 160, 162, and 164), known as "covered entities," are health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with covered transactions. See 45 *CFR* § 160.103. "Health care providers" include institutional providers of health or medical services, such as hospitals, as well as non-institutional providers, such as physicians, dentists, and other practitioners, along with any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. Covered transactions are those for which the U.S. Department of Health and Human Services has adopted a standard, such as health care claims submitted to a health plan. See 45 *CFR* § 160.103 (definitions of "health care provider" and "transaction") and 45 *CFR* Part 162, Subparts K–R.

The *HIPAA* Privacy Rule requires covered entities to protect individuals' health records and other identifiable health information by requiring appropriate safeguards to protect privacy, and setting limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

IV.   Where *FERPA* and *HIPAA* May Intersect

When a school provides health care to students in the normal course of business, such as through its health clinic, it is also a "health care provider" as defined by *HIPAA*. If a school also conducts any covered transactions electronically in connection with that health care, it is then a covered entity under *HIPAA*. As a covered entity, the school must comply with the *HIPAA* Administrative Simplification Rules for Transactions and Code Sets and Identifiers with respect to its transactions. However, many schools, even those that are *HIPAA* covered entities, are not required to comply with the *HIPAA* Privacy Rule because the only health records maintained by the school are "education records" or "treatment records" of eligible students under FERPA, both of which are excluded from coverage under the *HIPAA* Privacy Rule. See the exception at paragraph (2)(i) and (2)(ii) to what is considered "protected health information" (PHI) at 45 *CFR* § 160.103. In addition, the exception for records covered by *FERPA* applies both to the *HIPAA* Privacy Rule, as well as to the *HIPAA* Security Rule, because the Security Rule applies to a subset of information covered by the Privacy Rule (i.e., electronic PHI). Information on the *HIPAA* Privacy Rule is available at: http://www.hhs.gov/ocr/hipaa/. Information on the other *HIPAA* Administrative Simplification Rules is available at: http://www.cms.hhs.gov/HIPAAGenInfo/.

V.   Frequently Asked Questions and Answers

1.   Does the *HIPAA* Privacy Rule apply to an elementary or secondary school?

Generally, no. In most cases, the *HIPAA* Privacy Rule does not apply to an elementary or secondary school because the school either: (1) is not a *HIPAA* covered entity or (2) is a *HIPAA* covered entity but maintains health information only on students in records that are by definition "education records" under *FERPA* and, therefore, is not subject to the *HIPAA* Privacy Rule.

- *The school is not a HIPAA covered entity.* The *HIPAA* Privacy Rule only applies to health plans, health care clearinghouses, and those health care providers that transmit health information electronically in connection with certain administrative and financial transactions ("covered transactions"). See 45 *CFR* § 160.102. Covered transactions are those for which the U.S. Department of Health and Human Services has adopted a standard, such as health care claims submitted to a health plan. See the definition of "transaction" at 45 *CFR* § 160.103 and 45 *CFR* Part 162, Subparts K–R. Thus, even though a school employs school nurses, physicians, psychologists, or other health care providers, the school is not generally a *HIPAA* covered entity because the providers do not engage in any of the covered transactions, such as billing a health plan electronically for their services. It is expected that most elementary and secondary schools fall into this category.

- *The school is a HIPAA covered entity but does not have "protected health information."* Where a school does employ a health care provider that conducts one or more covered transactions electronically, such as electronically transmitting health care claims to a health plan for payment, the school is a *HIPAA* covered entity and must comply with the *HIPAA* Transactions and Code Sets and Identifier Rules with respect to such transactions. However, even in this case, many schools would not be required to comply with the *HIPAA* Privacy Rule because the school maintains health information only in student health records that are "education records" under *FERPA* and, thus, not "protected health information" under

HIPAA. Because student health information in education records is protected by *FERPA*, the *HIPAA* Privacy Rule excludes such information from its coverage. See the exception at paragraph (2)(i) to the definition of "protected health information" in the *HIPAA* Privacy Rule at 45 *CFR* § 160.103. For example, if a public high school employs a health care provider that bills Medicaid electronically for services provided to a student under the *IDEA*, the school is a *HIPAA* covered entity and would be subject to the *HIPAA* requirements concerning transactions. However, if the school's provider maintains health information only in what are education records under *FERPA*, the school is not required to comply with the *HIPAA* Privacy Rule. Rather, the school would have to comply with *FERPA's* privacy requirements with respect to its education records, including the requirement to obtain parental consent (34 *CFR* § 99.30) in order to disclose to Medicaid billing information about a service provided to a student.

2. **How does *FERPA* apply to health records on students maintained by elementary or secondary schools?**

At the elementary or secondary school level, students' immunization and other health records that are maintained by a school district or individual school, including a school-operated health clinic, that receives funds under any program administered by the U.S. Department of Education are "education records" subject to *FERPA*, including health and medical records maintained by a school nurse who is employed by or under contract with a school or school district. Some schools may receive a grant from a foundation or government agency to hire a nurse. Notwithstanding the source of the funding, if the nurse is hired as a school official (or contractor), the records maintained by the nurse or clinic are "education records" subject to *FERPA*.

Parents have a right under *FERPA* to inspect and review these health and medical records because they are "education records" under *FERPA*. See 34 *CFR* §§ 99.10 – 99.12. In addition, these records may not be shared with third parties without written parental consent unless the disclosure meets one of the exceptions to *FERPA*'s general consent requirement. For instance, one of these exceptions allows schools to disclose a student's health and medical information and other "education records" to teachers and other school officials, without written consent, if these school officials have "legitimate educational interests" in accordance with school policy. See 34 *CFR* § 99.31(a)(1). Another exception permits the disclosure of education records, without consent, to appropriate parties in connection with an emergency, if knowledge of the information is necessary to protect the health or safety of the student or other individuals. See 34 *CFR* §§ 99.31(a)(10) and 99.36.

3. **Does *FERPA* or *HIPAA* apply to elementary or secondary school student health records maintained by a health care provider that is not employed by a school?**

If a person or entity acting on behalf of a school subject to *FERPA*, such as a school nurse that provides services to students under contract with or otherwise under the direct control of the school, maintains student health records, these records are education records under *FERPA*, just as they would be if the school maintained the records directly. This is the case regardless of whether the health care is provided to students on school grounds or off-site. As education records, the information is protected under *FERPA* and not *HIPAA*.

Some outside parties provide services directly to students and are not employed by, under contract to, or otherwise acting on behalf of the school. In these circumstances, these records are not "education records" subject to *FERPA*, even if the services are provided on school grounds, because the party creating and maintaining the records is not acting on behalf of the school. For example, the records created by a public health nurse who provides immunization or other health services to students on school grounds or otherwise in connection with school activities but who is not acting on behalf of the school would not be "education records" under *FERPA*. In such situations, a school that wishes to disclose to this outside party health care provider any personally identifiable information from education records would have to comply with *FERPA* and obtain parental consent. See 34 *CFR* § 99.30.

With respect to *HIPAA*, even where student health records maintained by a health care provider are not education records protected by *FERPA*, the *HIPAA* Privacy Rule would apply to such records only if the provider conducts one or more of the *HIPAA* transactions electronically, e.g., billing a health plan electronically for his or her services, making the provider a *HIPAA* covered entity.

4.   Are there circumstances in which the *HIPAA* Privacy Rule might apply to an elementary or secondary school?

There are some circumstances in which an elementary or secondary school would be subject to the *HIPAA* Privacy Rule, such as where the school is a *HIPAA* covered entity and is not subject to *FERPA*. As explained previously, most private schools at the elementary and secondary school levels typically do not receive funding from the U.S. Department of Education and, therefore, are not subject to *FERPA*.

A school that is not subject to *FERPA* and is a *HIPAA* covered entity must comply with the *HIPAA* Privacy Rule with respect to any individually identifiable health information it has about students and others to whom it provides health care. For example, if a private elementary school that is not subject to *FERPA* employs a physician who bills a health plan electronically for the care provided to students (making the school a *HIPAA* covered entity), the school is required to comply with the *HIPAA* Privacy Rule with respect to the individually identifiable health information of its patients. The only exception would be where the school, despite not being subject to *FERPA*, has education records on one or more students to whom it provides services on behalf of a school or school district that is subject to *FERPA*. In this exceptional case, the education records of only those publicly-placed students held by the private school would be subject to *FERPA*, while the remaining student health records would be subject to the *HIPAA* Privacy Rule.

5.   Where the *HIPAA* Privacy Rule applies, does it allow a health care provider to disclose protected health information (PHI) about a troubled teen to the parents of the teen?

In most cases, yes. If the teen is a minor, the *HIPAA* Privacy Rule generally allows a covered entity to disclose PHI about the child to the child's parent, as the minor child's personal representative, when the disclosure is not inconsistent with state or other law. For more detailed information, see 45 *CFR* § 164.502(g) and the fact sheet regarding personal representatives at: http://www.hhs.gov/ocr/hipaa/guidelines/personalrepresentatives.pdf. In some cases, such as when a minor may receive treatment without a parent's consent under applicable law, the parents are not treated as the minor's personal representative. See 45 *CFR* § 164.502(g)(3). In such cases where

the parent is not the personal representative of the teen, other *HIPAA* Privacy Rule provisions may allow the disclosure of PHI about the teen to the parent. For example, if a provider believes the teen presents a serious danger to self or others, the *HIPAA* Privacy Rule permits a covered entity to disclose PHI to a parent or other person(s) if the covered entity has a good faith belief that: (1) the disclosure is necessary to prevent or lessen the threat and (2) the parent or other person(s) is reasonably able to prevent or lessen the threat. The disclosure also must be consistent with applicable law and standards of ethical conduct. See 45 *CFR* § 164.512(j)(1)(i).

In addition, the Privacy Rule permits covered entities to share information that is directly relevant to the involvement of a family member in the patient's health care or payment for care if, when given the opportunity, the patient does not object to the disclosure. Even when the patient is not present or it is impracticable, because of emergency circumstances or the patient's incapacity, for the covered entity to ask the patient about discussing his or her care or payment with a family member, a covered entity may share this information with the family member when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 *CFR* § 164.510(b).

6.   Where the *HIPAA* Privacy Rule applies, does it allow a health care provider to disclose protected health information (PHI) about a student to a school nurse or physician?

Yes. The *HIPAA* Privacy Rule allows covered health care providers to disclose PHI about students to school nurses, physicians, or other health care providers for treatment purposes, without the authorization of the student or student's parent. For example, a student's primary care physician may discuss the student's medication and other health care needs with a school nurse who will administer the student's medication and provide care to the student while the student is at school.

7.   Does *FERPA* or *HIPAA* apply to records on students at health clinics run by postsecondary institutions?

FERPA applies to most public and private postsecondary institutions and, thus, to the records on students at the campus health clinics of such institutions. These records will be either education records or treatment records under *FERPA*, both of which are excluded from coverage under the *HIPAA* Privacy Rule, even if the school is a *HIPAA* covered entity. See the exceptions at paragraphs (2)(i) and (2)(ii) to the definition of "protected health information" at 45 *CFR* § 160.103.

The term "education records" is broadly defined under *FERPA* to mean those records that are: (1) directly related to a student and (2) maintained by an educational agency or institution or by a party acting for the agency or institution. See 34 *CFR* § 99.3, "Education records."

"Treatment records" under *FERPA*, as they are commonly called, are:

> records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records

can be personally reviewed by a physician or other appropriate professional of the student's choice.

See 20 *U.S.C.* § 1232g(a)(4)(B)(iv); 34 *CFR* § 99.3, "Education records." For example, treatment records would include health or medical records that a university psychologist maintains only in connection with the provision of treatment to an eligible student, and health or medical records that the campus health center or clinic maintains only in connection with the provision of treatment to an eligible student. (Treatment records also would include health or medical records on an eligible student in high school if the records otherwise meet the above definition.)

"Treatment records" are excluded from the definition of "education records" under *FERPA*. However, it is important to note, that a school may disclose an eligible student's treatment records for purposes other than the student's treatment provided that the records are disclosed under one of the exceptions to written consent under 34 *CFR* § 99.31(a) or with the student's written consent under 34 *CFR* § 99.30. If a school discloses an eligible student's treatment records for purposes other than treatment, the treatment records are no longer excluded from the definition of "education records" and are subject to all other *FERPA* requirements, including the right of the eligible student to inspect and review the records.

While the health records of students at postsecondary institutions may be subject to *FERPA*, if the institution is a *HIPAA* covered entity and provides health care to *non*students, the individually identifiable health information of the clinic's *non*student patients is subject to the *HIPAA* Privacy Rule. Thus, for example, postsecondary institutions that are subject to both *HIPAA* and *FERPA* and that operate clinics open to staff, or the public, or both (including family members of students) are required to comply with *FERPA* with respect to the health records of their student patients, and with the *HIPAA* Privacy Rule with respect to the health records of their *non*student patients.

8.   Under *FERPA*, may an eligible student inspect and review his or her "treatment records"?

Under *FERPA*, treatment records, by definition, are not available to anyone other than professionals providing treatment to the student, or to physicians or other appropriate professionals of the student's choice. However, this does not prevent an educational institution from allowing a student to inspect and review such records. If the institution chooses to do so, though, such records are no longer excluded from the definition of "education records" and are subject to all other *FERPA* requirements.

9.   Under *FERPA*, may an eligible student's treatment records be shared with parties other than treating professionals?

As explained previously, treatment records, by definition, are not available to anyone other than professionals providing treatment to the student, or to physicians or other appropriate professionals of the student's choice. However, this does not prevent an educational institution from using or disclosing these records for other purposes or with other parties. If the institution chooses to do so, a disclosure may be made to any party with a prior written consent from the eligible student (see 34 *CFR* § 99.30) or under any of the disclosures permitted without consent in 34 *CFR* § 99.31 of *FERPA*.

For example, a university physician treating an eligible student might determine that treatment records should be disclosed to the student's parents. This disclosure may be made if the eligible student is claimed as a dependent for federal income tax purposes (see 34 *CFR* § 99.31(a)(8)). If the eligible student is not claimed as a dependent, the disclosure may be made to parents, as well as other appropriate parties, if the disclosure is in connection with a health or safety emergency. See 34 *CFR* §§ 99.31(a)(10) and 99.36. Once the records are disclosed under one of the exceptions to *FERPA's* general consent requirement, the treatment records are no longer excluded from the definition of "education records" and are subject to all other *FERPA* requirements as "education records" under *FERPA*.

10. Under what circumstances does *FERPA* permit an eligible student's treatment records to be disclosed to a third-party health care provider for treatment?

An eligible student's treatment records may be shared with health care professionals who are providing treatment to the student, including health care professionals who are not part of or not acting on behalf of the educational institution (i.e., third-party health care provider), as long as the information is being disclosed only for the purpose of providing treatment to the student. In addition, an eligible student's treatment records may be disclosed to a third-party health care provider when the student has requested that his or her records be "reviewed by a physician or other appropriate professional of the student's choice." See 20 *U.S.C.* § 1232g(a)(4)(B)(iv). In either of these situations, if the treatment records are disclosed to a third-party health care provider that is a *HIPAA* covered entity, the records would become subject to the *HIPAA* Privacy Rule. The records at the educational institution continue to be treatment records under *FERPA*, so long as the records are only disclosed by the institution for treatment purposes to a health care provider or to the student's physician or other appropriate professional requested by the student.

If the disclosure is for purposes other than treatment, an eligible student's treatment record only may be disclosed to a third party as an "education record," that is, with the prior written consent of the eligible student or if one of the exceptions to *FERPA*'s general consent requirement is met. See 34 *CFR* § 99.31. For example, if a university is served with a court order requiring the disclosure of the mental health records of a student maintained as treatment records at the campus clinic, the university may disclose the records to comply with the court order in accordance with the provisions of § 99.31(a)(9) of the *FERPA* regulations. However, the mental health records that the university disclosed for non-treatment purposes are no longer excluded from the definition of "education records" and are subject to all other *FERPA* requirements as "education records" under *FERPA*.

11. Are all student records maintained by a health clinic run by a postsecondary institution considered "treatment records" under *FERPA*?

Not all records on eligible students that are maintained by a college- or university-run health clinic are treatment records under *FERPA* because many such records are not made, maintained, or used only in connection with the treatment of a student. For example, billing records that a college- or university-run health clinic maintains on a student are "education records" under *FERPA*, the disclosure of which would require prior written consent from the eligible student unless an exception applies. See 34 *CFR* § 99.30. In addition, records relating to treatment that are shared with persons other than professionals providing treatment to the student are "education records" under *FERPA*. Thus, to the extent a health clinic has shared a student's treatment information with

persons and for purposes other than for treatment, such information is an "education record," not a treatment record under *FERPA*.

12. **Does *FERPA* or *HIPAA* apply to records on students who are patients at a university hospital?**

Patient records maintained by a hospital affiliated with a university that is subject to *FERPA* are not typically "education records" or "treatment records" under *FERPA* because university hospitals generally do not provide health care services to students on behalf of the educational institution. Rather, these hospitals provide such services without regard to the person's status as a student and not on behalf of a university. Thus, assuming the hospital is a *HIPAA* covered entity, these records are subject to all of the *HIPAA* rules, including the *HIPAA* Privacy Rule. However, in a situation where a hospital does run the student health clinic on behalf of a university, the clinic records on students would be subject to *FERPA,* either as "education records" or "treatment records," and not subject to the *HIPAA* Privacy Rule.

13. **Where the *HIPAA* Privacy Rule applies, does it permit a health care provider to disclose protected health information (PHI) about a patient to law enforcement, family members, or others if the provider believes the patient presents a serious danger to self or others?**

The *HIPAA* Privacy Rule permits a covered entity to disclose PHI, including psychotherapy notes, when the covered entity has a good faith belief that the disclosure: (1) is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others and (2) is to a person(s) reasonably able to prevent or lessen the threat. This may include, depending on the circumstances, disclosure to law enforcement, family members, the target of the threat, or others who the covered entity has a good faith belief can mitigate the threat. The disclosure also must be consistent with applicable law and standards of ethical conduct. See 45 *CFR* § 164.512(j)(1)(i). For example, consistent with other law and ethical standards, a mental health provider whose teenage patient has made a credible threat to inflict serious and imminent bodily harm on one or more fellow students may alert law enforcement, a parent or other family member, school administrators or campus police, or others the provider believes may be able to prevent or lessen the chance of harm. In such cases, the covered entity is presumed to have acted in good faith where its belief is based upon the covered entity's actual knowledge (i.e., based on the covered entity's own interaction with the patient) or in reliance on a credible representation by a person with apparent knowledge or authority (i.e., based on a credible report from a family member or other person). See 45 *CFR* § 164.512(j)(4).

For threats or concerns that do not rise to the level of "serious and imminent," other *HIPAA* Privacy Rule provisions may apply to permit the disclosure of PHI. For example, covered entities generally may disclose PHI about a minor child to the minor's personal representative (e.g., a parent or legal guardian), consistent with state or other laws. See 45 *CFR* § 164.502(b).

14. **Does *FERPA* permit a postsecondary institution to disclose a student's treatment records or education records to law enforcement, the student's parents, or others if the institution believes the student presents a serious danger to self or others?**

An eligible student's education records and treatment records (which are considered education records if used or made available for any purpose other than the eligible student's treatment) may be disclosed, without consent, if the disclosure meets one of the exceptions to *FERPA*'s general consent rule. See 34 *CFR* § 99.31. One of the permitted disclosures is to appropriate parties, which may include law enforcement or parents of a student, in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals. See 34 *CFR* §§ 99.31(a)(10) and 99.36.

There are other exceptions that apply to disclosing information to parents of eligible students that are discussed on the "Safe Schools & FERPA" Web page, as well as other information that should be helpful to school officials, at:
http://www.ed.gov/policy/gen/guid/fpco/ferpa/safeschools/index.html/.

15.   Are the health records of an individual who is both a student and an employee of a university at which the person receives health care subject to the privacy provisions of *FERPA* or those of *HIPAA*?

The individual's health records would be considered "education records" protected under *FERPA* and, thus, excluded from coverage under the *HIPAA* Privacy Rule. *FERPA* defines "education records" as records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution. 34 *CFR* § 99.3 ("education records"). While *FERPA* excludes from this definition certain records relating to employees of the educational institution, to fall within this exclusion, such records must, among other things, relate exclusively to the individual in his or her capacity as an employee, such as records that were created in connection with health services that are available only to employees. Thus, the health or medical records that are maintained by a university as part of its provision of health care to a student who is also an employee of a university are covered by *FERPA* and not the *HIPAA* Privacy Rule.

16.   Can a postsecondary institution be a "hybrid entity" under the *HIPAA* Privacy Rule?

Yes. A postsecondary institution that is a *HIPAA* covered entity may have health information to which the Privacy Rule may apply not only in the health records of nonstudents in the health clinic, but also in records maintained by other components of the institution that are not education records or treatment records under *FERPA*, such as in a law enforcement unit or research department. In such cases, the institution, as a *HIPAA* covered entity, has the option of becoming a "hybrid entity" and, thus, having the *HIPAA* Privacy Rule apply only to its health care unit. The school can achieve hybrid entity status by designating the health unit as its "health care component." As a hybrid entity, any individually identifiable health information maintained by other components of the university (i.e., outside of the health care component), such as a law enforcement unit, or a research department, would not be subject to the *HIPAA* Privacy Rule, notwithstanding that these components of the institution might maintain records that are not "education records" or treatment records under *FERPA*.

To become a hybrid entity, the covered entity must designate and include in its health care component all components that would meet the definition of a covered entity if those components were separate legal entities. (A covered entity may have more than one health care component.) However, the hybrid entity is not permitted to include in its health care component other types of components that do not perform the covered functions of the covered entity or components that do

not perform support activities for the components performing covered functions. That is, components that do not perform health plan, health care provider, or health care clearinghouse functions and components that do not perform activities in support of these functions (as would a business associate of a separate legal entity) may not be included in a health care component. Within the hybrid entity, most of the *HIPAA* Privacy Rule requirements apply only to the health care component, although the hybrid entity retains certain oversight, compliance, and enforcement obligations. See 45 *CFR* § 164.105 of the Privacy Rule for more information.

VI.   Conclusion

The *HIPAA* Privacy Rule specifically excludes from its coverage those records that are protected by *FERPA*. When making determinations as to whether personally identifiable information from student health records maintained by the educational agency or institution may be disclosed, school officials at institutions subject to *FERPA* should refer to *FERPA* and its requirements. While the educational agency or institution has the responsibility to make the initial, case-by-case determination of whether a disclosure meets the requirements of *FERPA*, the Department of Education's Family Policy Compliance Office is available to offer technical assistance to school officials in making such determinations.

For quick, informal responses to routine questions about *FERPA*, school officials may e-mail the Department at FERPA@ed.gov. For more formal technical assistance on the information provided in this guidance in particular or *FERPA* in general, please contact the Family Policy Compliance Office at the following address:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Ave. S.W.
Washington, D.C. 20202-8520

You may also find additional information and guidance on the Department's Web site at: http://www.ed.gov/policy/gen/guid/fpco/index.html.

For more information on the *HIPAA* Privacy Rule, please visit the Department of Health and Human Services' *HIPAA* Privacy Rule Web site at: http://www.hhs.gov/ocr/hipaa/. The Web site offers a wide range of helpful information about the *HIPAA* Privacy Rule, including the full text of the Privacy Rule, a *HIPAA* Privacy Rule summary, over 200 frequently asked questions, and both consumer and covered entity fact sheets.

In addition, if you would like to submit additional questions not covered by this guidance document or suggestions for purposes of informing future guidance, please send an e-mail to OCRPrivacy@hhs.gov and FERPA@ed.gov.

ADDITIONAL RESOURCES TO EXPLORE

PUBLICATIONS, RESEARCH & REPORTS

National Behavioral Intervention Team Association (NaBITA): Training, Assessment Tools, Consultation, Community, and Support
The National Behavioral Intervention Team Association is committed to providing education, development, and support to school professionals who endeavor every day to make their campuses safer through caring prevention and intervention.
https://www.nabita.org/

Best Practices in Campus Threat Assessment: Training, Consultation, Evaluation, and Support
SIGMA Threat Management Associates
www.sigmatma.com

College Student Death: Guidance for a Caring Campus by Rosa Citron, Erin Taylor Weathers and Katherine Garlough, (2007; University Press of America)

Ending Campus Violence: New Approaches to Prevention by Brian Van Brunt (2012 Routledge Publishing)

The Handbook for Campus Threat Assessment & Management Teams
by Gene Deisinger, Ph.D.; Marisa Randazzo, Ph.D.; Dan O'Neill, and Jenna Savage, (2008; Applied Risk Management)

United States Secret Service
NTAC-National Threat Assessment Center

- The Final Report And Findings Of The Safe School Initiative: Implications For The Prevention Of School Attacks In The United States; United States Secret Service And United States Department Of Education; May 2002; https://www.secretservice.gov/data/protection/ntac/ssi_final_report.pdf
- Threat Assessment In Schools: A Guide To Managing Threatening Situations And To Creating Safe School Climates; United States Secret Service And United States Department Of Education; May 2002; https://www.secretservice.gov/data/protection/ntac/ssi_guide.pdf
- Evaluating Risk For Targeted Violence In Schools: Comparing Risk Assessment, Threat Assessment, And Other Approaches; United States Secret Service, University Of South Florida And United States Department

Of Education; January 2001;
https://www.secretservice.gov/data/protection/ntac/ssitarget.pdf

- Making Schools Safer: Quick Reference Guide, United States Secret Service; February 2018;
https://www.secretservice.gov/data/protection/ntac/Making_Schools_Safer_Quick_Reference_Guide_2018_Update.pdf
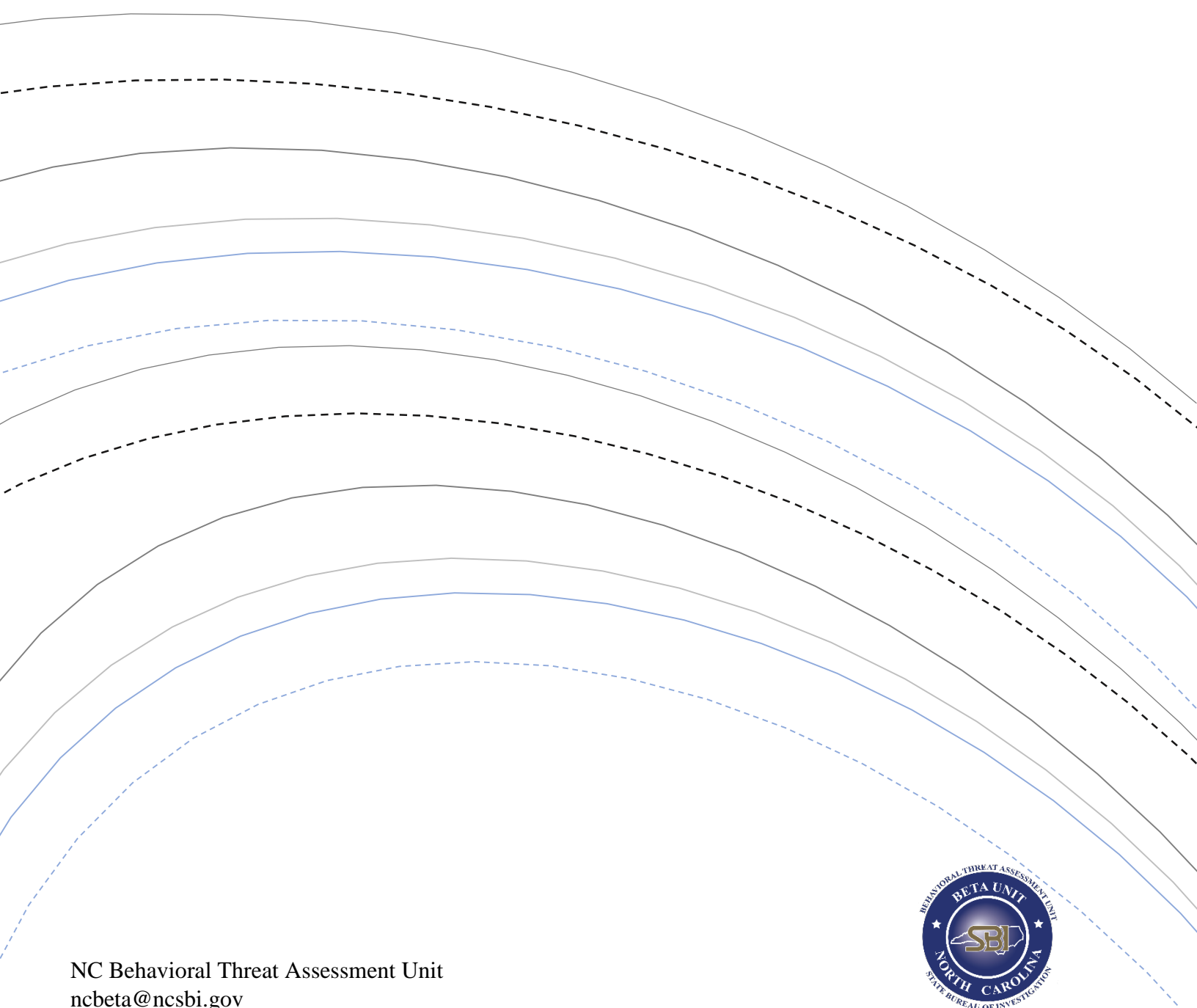
NC Behavioral Threat Assessment Unit
ncbeta@ncsbi.gov
888-624-7222

Connecting. The. Dots.