

Local Agency Security Officer

August - September
2021



North Carolina State Bureau of Investigation - CIIS

1

Discussion Topics

- CJIS Security Policy
- Key Rolls
- LASO
- LASO Training
- LASO Requirements
- Technical Security Audit
- LASO and Compliance
- Key Areas
- Incident Response



LASO



Criminal Justice Information Security Policy

Criminal Justice
Information Security
Policy (CJIS) 5.9

Minimum level of
Information
Technology (IT)
requirements

Guidelines for
security requirements,
processing and
storage of CJIS data

Outlines roles and
responsibilities for,

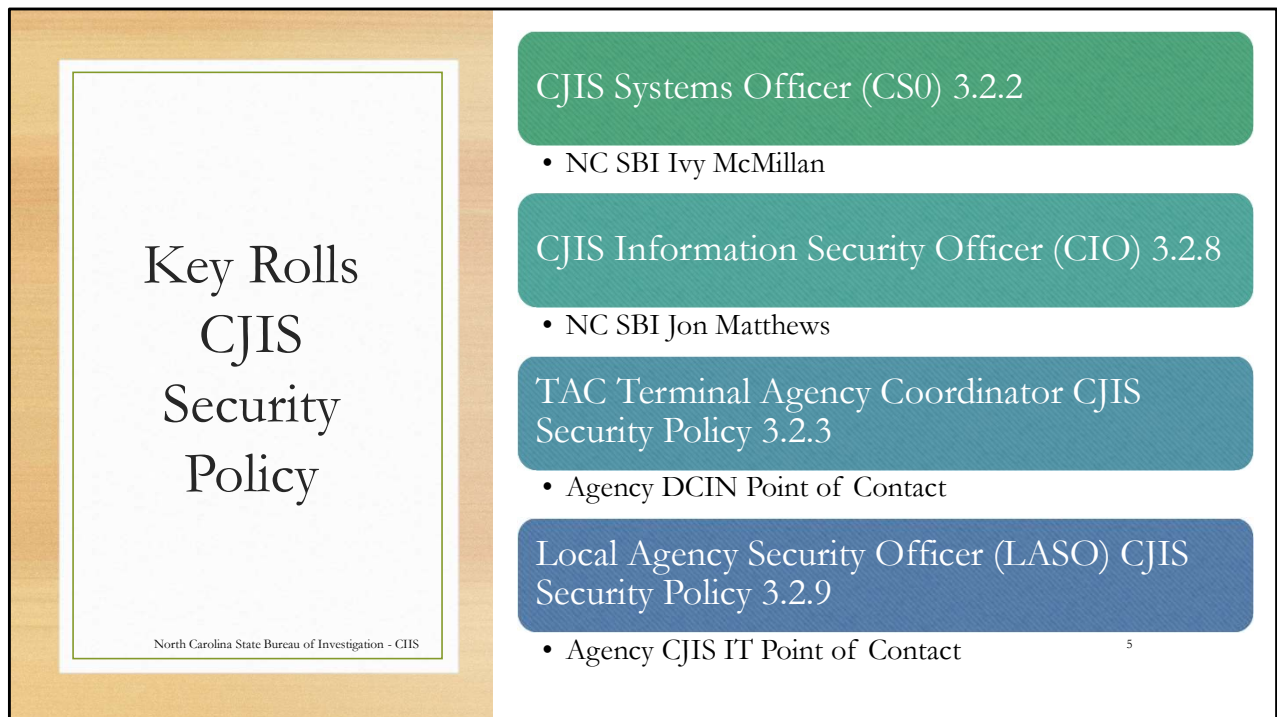
CJIS Systems Officer
(CSO)

CJIS Information
Security Officer (ISO)

Terminal Agency
Coordinator (TAC)

Local Agency Security
Officer (LAS)

Criminal Justice
Information Services
(CJIS) Security Policy
— FBI



3.2.2 (2e) - CSO – CJIS Systems Officer

E. CJIS Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).

F. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2)

Local Agency Security Officer

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

LASO



**Ability to work
with technical
people and take
direction from
technical people**



**Familiar with
security
requirements**



**Be able to
navigate the web
for appropriate
security updates**



**Stay current with
security trends**



**Does not have to
be a technical
professional**

LASO

5.2 Policy Area 2: Security Awareness Training

- Requires enhanced training for LASO / Level 4 Security Awareness
- **At a minimum:**
 - 1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
 - 2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
 - 3. Summary of audit findings from previous state audits of local agencies.
 - 4. Findings from the last FBI CJIS Division audit of the CSA.
 - 5. Most recent changes to the CJIS Security Policy

CJIS Online / NexTest

- Level 4 Security Awareness Training
- Annual requirement
- NC SBI Compliance Unit
 - No user ID already
 - Input new user profiles in CJIS Online
- User ID Agency TAC ensures LASO has appropriate level training

Technical Security Audit

- LASO audit requirement starting 1 January 2022
- Bi-Annual Audit
- Network diagram must include agency name, date and “For Official Use Only”
- LASO is responsible to complete Technical Security Audit (TSA)
- NC SBI Compliance Unit receives completed TSA during agency audit

LASO and Agency TAC

- LASO works with agency TAC and IT contact to ensure compliance
- Does not have to be agency TAC
- LASO and TAC should be different people if possible

LASO: Threat for security breach is 24 hours a day, considerations LASO alternate for vacations or off hours

LASO and Agency TAC

- LASO appointed and completes LASO Notification
- Notification will be sent to DCIN Compliance Unit
- Confirmation email will be sent to LASO and Agency TAC
- If LASO changes, submit new LASO Notification
- LASO Notification found in Omnixx Force & Trainer Links/IT Assistance/LASO Notification or by utilizing this link:

<https://forms.office.com/Pages/ResponsePage.aspx?id=0E3JiW9DEi2hLl7NP1R1rsYfSawxkFLjVxkuG-qE0NUNk5GSEIEVlc4WTNZSjNFM0JJT1VQOFQxNi4u>

LASO: Threat for security breach is 24 hours a day, considerations LASO alternate for vacations or off hours

Key Areas of Focus

- CJIS Security Policy:
- Physical Security 5.9
- Personnel Security 5.5
- Security Awareness Training 5.2
- Disposal of Media 5.8

Physical Security 5.9: Greatest threat to security is the belief there is no threat

Personnel Security 5.5:

Security Awareness Training 5.2

Disposal of Media 5.8: How to correctly dispose of media

Key Areas of Focus

- CJIS Security Policy:
- Keep systems updated 5.10.4
- Passwords 5.6
- Use anti-virus software 5.10.4
- Encryption 5.10.1.2

Keep systems updated 5.10.4: Hardware and software, updated with most recent security release

Passwords 5.6:

Use anti-virus software 5.10.4: Must be updated, always running

Encryption 5.10.1.2:

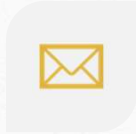
User Access

- Agency personnel and vendors are properly fingerprinted and background competed per CJIS Security Policy 5.12
- Agency personnel and vendors have received appropriate level of CJIS Security Awareness Training per CJIS Security Policy 5.2
- Vendors with remote access utilize advanced authentication to access CJIS computers

Incident Response



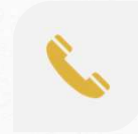
NCSBI - CJIS SECURITY
INCIDENT



JON MATTHEWS
JMATTHEWS@NCSBI.GOV



DEPARTMENT OF PUBLIC
SAFETY INFORMATION
TECHNOLOGY



919-773-7900

Incident response: Electronic breach can affect multiple systems. Downloaded virus to computer can be transferred to cell phones, watches, blue tooth devices. Incident response should be immediate to mitigate exposure

In Review

- CJIS Security Policy
- Key Rolls
- LASO
- LASO Training
- LASO Requirements
- Technical Security Audit
- LASO and Compliance
- Key Areas
- Incident Response





Questions

SBI DCIN Compliance Unit

- arahelp@ncsbi.gov
- (919) 582-8640

