

* * * *

ATTENTION: AGENCY TAC/POC

* * * *

REVIEW AND DISTRIBUTE THIS NOTICE ACCORDINGLY

Reporting of Security Incidents

To ensure the protection of Criminal Justice Information the FBI's CJIS Security Policy requires the reporting of Security Incidents to appropriate authorities: In our case, they're reported to the SBI's CJIS Information Security Officer as well as the CJIS Systems Officer - we then take the information and forward it to the FBI CJIS Division as required by the Security Policy.

To make this easier, we have created a web-based reporting form that can be found at:

<http://ncsbi.gov/cjis-incident>

Recent examples of things that have been reported are malware infections, ransomware attacks, phishing, etc. Pretty much anything that impacts information technology assets that have access to CJIS should be reported.

We recently have had several agencies report ransomware attacks, ransomware is rather insidious so letting us know helps protect the entire State.

As always, if you have an attack in progress, feel free to call us at (919) 773-7900 so we can assist in any way we can.

CJIS Security Policy:

5.3.1 Reporting Security Events - The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

Get

CONNECTED

North Carolina State Bureau of Investigation