Security Incidents

A security incident can be defined as any physical or logical security breach that negatively affects an agency's devices, systems, and/or networks that connect to, store, or handle information traffic with criminal justice information (CJI), CJIS data (obtained from TIME/NCIC), and/or any confidential information used for the administration of criminal justice or law enforcement.

Some examples of security incidents are hackers gaining access to your network, someone clicking on a phishing email, allowing an unauthorized person into your facility who gains access to information on your network, getting a virus on your computer, etc. If a security incident occurs at your agency and Criminal Justice Information (CJI) on your network is potentially compromised, action must be taken.

Your agency can prepare for potential cyber security incidents by ensuring all personnel are aware of your agency's security incident plan, conducting regular cyber security incident training, and implementing advanced monitoring tools to detect unusual activity and potential threats.

If your agency has an incident, you should immediately notify your Local Agency Security Officer (LASO) and IT support. Notify the Crime Information Bureau (CIB) and WI Statewide Intelligence Center (WSIC) / Division of Criminal Investigation (DCI) within 24 hours of the discovery of a security incident. The sooner that CIB is notified, the quicker CIB can act to ensure that the effect to the TIME System is mitigated and service to the affected agency is restored.

CIB can be notified by calling the TIME System Control Center (TSCC) at 608-266-7633. TSCC is available 24 hours a day and 7 days per week, 365 days a year. During normal business hours, agencies can email cibtrain@doj.state.wi.us. In order to reach DCI/WI Statewide Intelligence Center, the agency should call 888-324-9742 or email wsic@doj.state.wi.us. There is also an online reporting form available: https://wifusion.widoj.gov/form/cyber-incident-reporting.

After the initial report to CIB, DOJ's firewalls are adjusted to block the agency's inbound BadgerNet traffic, the agency's main terminal traffic is re-routed to another agency, TIME system interface access is disabled, and all DOJ issued TIME System credentials are completely reset to include issuance of new usernames.

To regain TIME System access, the agency shall provide details of the incident in a detailed report to CIB. Agencies should document and retain evidence from the security incident. This information is pertinent during the investigation and helps prevent future incidents. The initial report of the incident shall include:

1. The specific type of malware/virus or hostile application
2. When the hostile actor was first observed on the network
3. Who was initially contacted and for what purpose
4. What initial steps were performed to isolate or prevent extension
5. Was any extension known or found prior to contacting higher agencies?
6. What caused delays in notification to logically connected agencies?
7. Was there any information found to have been harvested by hostile actors?
8. Was there any credential harvesting found?