Law Enforcement Cyber Incident Reporting

A Unified Message for State, Local, Tribal, and Territorial Law Enforcement

Cyber threats from malicious actors are a growing concern across the United States. Voluntary sharing of incident information between state, local, tribal, and territorial (SLTT) law enforcement and the federal government is important to ensuring a safe and secure cyberspace. This document details different ways SLTT law enforcement partners can report suspected or confirmed cyber incidents to the federal government. No matter which "door" SLTT law enforcement uses, information is shared within the federal government to provide an appropriate response while protecting citizens' privacy and civil liberties under the law.

When to Report to the Federal Government

A cyber incident is a past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the confidentiality, integrity, or availability of electronic information, information systems, services, or networks. SLTT partners are encouraged to voluntarily report suspected or confirmed cyber incidents to a federal entity. In particular, a cyber incident should be reported if it:

- May impact national security, economic security, or public health and safety.
- Affects core government or critical infrastructure functions.
- Results in a significant loss of data, system availability, or control of systems.
- Involves a large number of victims.
- Indicates unauthorized access to, or malicious software present on, critical information technology systems.
- Violates federal or SLTT law.

What to Report

Cyber incidents may be reported at various stages, including when complete information is not available. Gathering as much information as possible will help expedite assistance to your agency and your community.

- Your name, organization, address, and phone number.
- What entity experienced the incident? Who owns the affected systems? Who is the appropriate point of contact?
- What type of incident occurred?
- What was the initial entry vector or vulnerability exploited (if known)?
- How was the incident initially detected or discovered?
- What specific assets appear to be impacted (e.g., systems, networks, data)?
- Provide a synopsis of impacts (business, mission, and operational), including prioritization factors:
  - Did the incident impact critical infrastructure essential functions?
  - Was a control system compromised or manipulated?
- What response actions have already been performed by the affected entity?
  - Are they requesting federal technical assistance?
  - Have they contacted or retained a managed security service provider for mitigation/investigation?
  - Has your agency opened a law enforcement investigation? Have other law enforcement agencies been asked to investigate? Can you share the other agency's point of contact information?
- If you have them, please share:
  - Logs, including destination IP and port and destination URL
  - Operating software of the affected system(s)
  - Source ports involved in the attack
  - Indications (current or historical) of sophisticated tactics, techniques, and procedures (TTPs)
  - Indications (current or historical) that the attack specifically targeted the asset owner
  - Status change data and time stamps (including time zone)

How to Report

The federal government has several different ways for individuals, businesses, law enforcement partners, and others to report cyber incidents. SLTT law enforcement can report to the federal government in person, by e-mail, by phone, or via online tools. Reports are appropriately shared among relevant federal stakeholders in order to help mitigate the consequences of the incident, evaluate the impact on critical infrastructure, and investigate any potential criminal violations. The table on the next page summarizes these resources.

Law Enforcement Cyber Incident Reporting

A Unified Message for State, Local, Tribal, and Territorial Law Enforcement

Key Contacts for SLTT Law Enforcement Cyber Incident Reporting

Organization and Key Points of Contact	What to Report?
U.S. Department of Homeland Security (DHS)	
National Protection and Programs Directorate (NPPD)	
National Cybersecurity and Communications Integration Center (NCCIC) (http://www.dhs.gov/about-national-cybersecurity-communications-integration-center) NCCIC@hq.dhs.gov or (888) 282-0870	Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response and mitigation assistance
United States Secret Service	
Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml) Electronic Crimes Task Forces (ECTFs) (http://www.secretservice.gov/ectf.shtml)	Cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information
Immigration and Customs Enforcement Homeland Security Investigations (ICE HSI)	
ICE HSI Field Offices (http://www.ice.gov/contact/inv/) ICE HSI Cyber Crimes Center (http://www.ice.gov/cyber-crimes/)	Cyber-based domestic or international cross-border crime, including child exploitation, money laundering, smuggling, and violations of intellectual property rights
U.S. Department of Justice (DOJ)	
Federal Bureau of Investigation (FBI)	
FBI Field Offices (http://www.fbi.gov/contact-us/field) Cyber Task Forces (http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1) Law Enforcement Online Portal (https://www.cjis.gov/CJISEAI/EAIController) or (888) 334-4536	Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity

Cyber Training and Other Resources for Law Enforcement Personnel

- The FBI's Cyber Shield Alliance (https://www.cjis.gov/CJISEAI/EAIController) provides extensive resources for SLTT partners, including eGuardian (https://www.cjis.gov/CJISEAI/EAIController) access, intelligence sharing, federally sponsored training, and fellowships at the National Cyber Investigative Joint Task Force (http://www.fbi.gov/about-us/investigate/cyber/ncijtf). The FBI also supports the InfraGard (https://www.infragard.org/) partnership with the private sector.
- The U.S. Secret Service operates the National Computer Forensics Institute (https://www.ncfi.usss.gov) to provide federally sponsored training for SLTT partners, including law enforcement, prosecutors, and judges.
- The ICE HSI Cyber Crimes Center offers a variety of technical training courses related to cyber investigations and digital forensics on a request basis.
- The Computer Crime and Intellectual Property Section (CCIPS) manuals *Searching and Seizing Computers* and *Electronic Evidence* and *Prosecuting Computer Crimes* are available online at http://www.justice.gov/criminal/cybercrime/documents.html.
- SLTT partners can also advise the public to file a complaint online (http://www.ic3.gov/default.aspx) with the Internet Crime Complaint Center (http://www.ic3.gov/default.aspx).

If there is an immediate threat to public health or safety, the public should always call 9-1-1.