Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to

systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact

Threat Response

Federal Bureau of Investigation (FBI)

FBI Field Office Cyber Task Forces:
http://www.fbi.gov/contact-us/field

Internet Crime Complaint Center (IC3):
http://www.ic3.gov

Report 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 to FBI Field Office Cyber Task Forces.

Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.

National Cyber Investigative Joint Task Force

NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov

Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.

United States Secret Service

Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):
http://www.secretservice.gov/contact/field-offices

Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information

United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)

HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or https://www.ice.gov/webform/hsi-tip-form

HSI Field Offices: https://www.ice.gov/contact/hsi

HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes

Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.

Asset Response

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov

United States Computer Emergency Readiness Team:
http://www.us-cert.gov

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

U.S. Customs and Border Protection

CTPAT Program - Supply Chain Security Specialist
Phone Number:
E-Mail: _____@cbp.dhs.gov

Minimum Security Criterion - 4.4 - Cyber security policies should address how a Member shares information on cyber security threats with the government and other business partners.

Other Related CTPAT Requirements:

Minimum Security Criterion - 7.23 - CTPAT Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process.

Minimum Security Criterion - 7.23 - Members must initiate their own internal investigations of any security-related incidents (terrorism, narcotics, stowaways, absconders, etc.) immediately after becoming aware of the incident.

Minimum Security Criterion - 12.10 - Personnel must be trained on how to report security incidents and suspicious activities.

If there is an immediate threat to public health or safety, the public should always call 911.