United States Secret Service
Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

Reporting Cyber Incidents to the Federal Government:

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. The Federal Government is particularly concerned with cyber incidents resulting in significant damage. Such incidents should be reported, especially if they:

- Result in a significant loss of data, system availability, or control of systems
- Impact a large number of potential victims
- Indicate unauthorized access to, or malicious software present on, critical information technology systems
- Affect critical infrastructure or core government functions
- Impact national security, economic security, or public health and safety

Roles and Responsibilities of Federal Law Enforcement Agencies:

By design, U.S. law enforcement contains overlapping jurisdictions. This is true at the federal, state, and local levels. This structure allows for collaboration and sharing of information between law enforcement agencies. The Secret Service is just one among several federal law enforcement agencies with the authority to investigate cybercrimes. Each agency has a unique cybercrime specialization and focus.

The various agencies of the Federal Government work in tandem to leverage their collective 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. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident.

Where to Report Cyber Incidents

If there is suspicion that the cyber incident is a result of criminal activity, contact law enforcement as soon as possible and as defined within your Incident Response (IR) Plan. A preexisting relationship with law enforcement will streamline this step by clarifying what entities your organization should contact and when. For more information on IR planning, see the *U.S. Secret Service Preparing for a Cyber Incident - Introductory Guide*.

United States Secret Service | Report cybercrime and cyber incidents, including network intrusions, malware attacks, account data compromises, theft, sale, and illicit use of personally identifiable information (PII) and Payment Card Industry (PCI) data, illicit financing and money laundering, digital currency scams, payment card terminal attacks, and other cyber-enabled financial crimes to *Secret Service Field Office Cyber Fraud Task Forces*.

Federal Bureau of Investigation | 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 *Internet Crime Complaint Center (IC3)*, which accepts Internet crime complaints from both victim and third parties.

Homeland Security Investigations (HSI) | Report cybercrime, 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 to *HSI Field Offices* and the *HSI Tip Line*.

Technical Assistance from the Federal Government:

In addition to law enforcement, the Cybersecurity and Infrastructure Security Agency (CISA) provides technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery.

CISA | Report suspected or confirmed cyber incidents, particularly when interested in government assistance in removing the adversary, restoring operations, and recommending ways to improve cybersecurity, to *CISA Central*.