



# REPORTING GUIDELINES



## Call your local police department or 9-1-1 (as appropriate):

- If you have a life-threatening situation, or an emergency
- If it is a local police matter

## Call or email your local FBI Private Sector Coordinator (InfraGard):

- If you are unsure if something should be reported
- Within 48 hours of a wire-transfer transaction associated with a business email compromise

## Call your local FBI field office or email the FBI to report an incident:

The FBI investigates a variety of criminal and national security incidents. Our website, <http://www.fbi.gov>, shares more information on what we investigate.

- If the incident or situation involves a sophisticated scam, unusual situation, concerning incident, or time-sensitive matter

## File an online report with the FBI:

- To report information on criminal activity and suspected terrorist threats
- You can complete the Online Tips and Public Leads form available at <https://tips.fbi.gov>

## File an online report to the FBI's Internet Crime Complaint Center (IC3) at <http://www.IC3.gov> for:

*Cyber scams, crimes, and frauds committed by telephone, email or Internet. These may include (not all inclusive):*

- |                              |                             |                        |
|------------------------------|-----------------------------|------------------------|
| ○ International fraud        | ○ Counterfeit check fraud   | ○ Internet extortion   |
| ○ Computer help desk fraud   | ○ Investment fraud          | ○ Identity theft       |
| ○ Romance scams              | ○ Fraudulent wire transfers | ○ Phishing attacks     |
| ○ Fraudulent vendor invoices | ○ Real Estate/Rental Fraud  | ○ Work-at-home schemes |

- Financial Fraud Kill Chain/IC3's Recovery Asset Team (RAT) - Once a complaint is submitted and analyzed by an IC3 RAT analyst, the complaint details may be forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of account. Once response is received from the recipient bank, RAT contacts the appropriate field office(s). The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.
- All incidents should be reported as quickly as possible with as many transaction details as possible, including victim and recipient account information and transaction amounts/dates, etc.
- *Note: Provide as much detail as possible about Who, What, When, Where, How, and Why (if known). This includes providing full email headers, if appropriate. Attachments are not possible.*
- *Keep a record of your complaint. You will only have one opportunity to save or print a copy of your submitted complaint.*

## InfraGard members can file an online report through Guardian

(Accessed through <https://www.infragard.org>):

- Incidents associated with a company
- Cyber incidents/intrusion activities, to include:
  - Distributed Denial of Service (DDoS)
  - Unusual port scanning
  - Malware infections
  - Phishing attacks
- Note: Provide as much detail as possible about Who, What, When, Where, How, and Why (if known). This includes providing full email headers, logs, and PCap data, if appropriate.
- Bonus: Within Guardian you can upload attachments. Once submitted, your FBI InfraGard Private Sector Coordinator is notified of the submission and it is immediately sent to the FBI's 24/7 CYWATCH for review and assignment.

**Your FBI point of contact can look at any complaint. Please understand they may direct you to report it using the appropriate reporting mechanism. If you send information that is not an FBI matter, they will attempt to direct you to the right place. Furthermore, InfraGard has access to Malware Investigator for malware samples to be analyzed anonymously.**



# REPORTING GUIDELINES



Cyber threats from malicious actors are a growing concern across the United States. No matter which method of reporting, information is shared within the federal government to provide an appropriate response while protecting citizens' privacy and civil liberties under the law.

## Descriptions of Types of Incidents

**Distributed Denial of Service Attack:** An attempt to prevent or impair the normal authorized functionality of a network, system, or application by exhausting resources.

**Economic Espionage:** (1) Whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent.

**Identity Theft:** When someone assumes your identity to perform a fraud or other criminal act.

**Malicious Code:** Successful installation of malicious software (virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.

**Phishing Attacks:** An attempt to acquire sensitive information such as usernames, passwords, credit card details, or other information, or orchestrate an action such as wire-transfer by masquerading as a trustworthy entity in an electronic communication.

**SQL Injection:** A code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g., to exfiltrate the database contents to the attacker).

**Unauthorized Access:** An individual gains logical or physical access without permission to a company's network, system, application, data, or other resource.

**Website Defacement:** An attack on a website that changes the visual appearance of the site or a webpage.

## 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. Partners are encouraged to voluntarily report suspected or confirmed cyber incidents to law enforcement. In particular, a cyber incident should be reported to the Federal Government 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 law

## Possible Types of Evidence to Preserve After an Incident

If you have them, please preserve and 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)

## Questions to be Prepared for When Reporting an Incident

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 company.

- 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 (e.g., through US-CERT)?
- Have they contacted or retained a managed security service provider for mitigation/investigation?
- If you also reported it to a state, local, tribal or territorial law enforcement agency, which agency was it reported to? Are they opening a law enforcement investigation? Have other law enforcement agencies been asked to investigate? Can you share the other agency's point of contact information?