CYBER INCIDENT NOTIFICATION PROTOCOL

When to Report a Cyber Incident to the Federal Government

A cyber incident is the outcome of an action taken by an adversary targeting computers and networks to impair the confidentiality, integrity, or availability of data or networked services resulting in a threat to public health or safety, undermining of public confidence, harm to the economy, or reduction of the nation's security standpoint. In recent years, the threat posed by terrorist, nation-states, and criminal groups conducting computer network operations against the United States has evolved into a top national security threat. InfraGard members have integral role in assisting the FBI strengthen the ability to combat cyber threats as technology continues to evolve. Therefore, InfraGard members are encouraged to voluntarily report suspected or confirmed cyber incidents to a federal entity such as the FBI. 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 in a Cyber 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 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 A Cyber Incident

The federal government has several different ways for individuals, businesses, law enforcement partners, and others to report cyber incidents. Law enforcement can report to the federal government in person, by e-mail, by phone, or via online tools. Louisiana critical Infrastructure personnel can contact either **Louisiana InfraGard President Lester Millet, InfraGard Coordinator Special Agent Corey G. Harris or they can report online through www.ic3.gov**. 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.

Contact Information:

Corey Harris (504)816-3145 corey.harris@ic.fbi.gov

Lester Millet III (985) 210-7518 lmillet@portsl.com