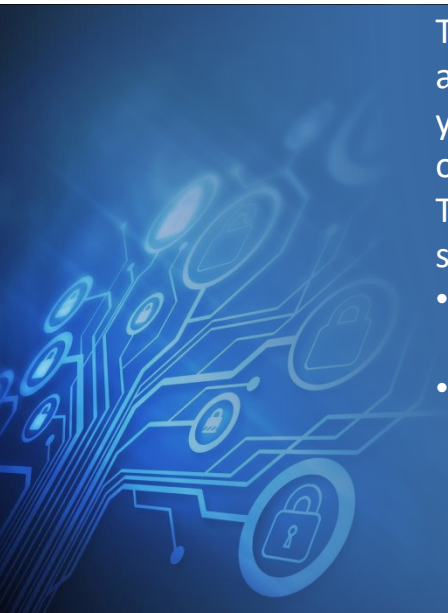
FBI Cyber Investigative Response
KEY CONSIDERATIONS

The FBI deploys personnel to conduct an investigation, which differs slightly from incidence response. The FBI:

- Cannot directly assist with remediation.
- Cannot provide comprehensive advice for network configuration or validate an organization's configuration/practices or perform vulnerability assessments.
- Can sometimes provide specific advice on mitigating particular vulnerabilities or intrusion vectors if we find evidence they have been exploited and have specific knowledge of how to mitigate.
- May share information we locate during the course of our investigation. This information could help the victim with remediation.



The FBI tries to keep information unclassified so we can share as much information as possible. We may not be able to tell you who did it, but we can tell you how, when, and where it occurred.

The FBI is a law enforcement agency, anything we do on your system(s)/network is a search under the 4th Amendment.

- This limits what the FBI can and should do on your network.
- The FBI will not be looking for evidence of criminal activity outside of the intrusion but cannot ignore evidence of other criminal activity if discovered while investigating the initial intrusion.

- The FBI will work within the parameters of what the victim is willing and able to consent to.

- The FBI tries to have minimum possible impact and are not going to disrupt victim's operations any more than necessary.

- The FBI is not a regulatory agency and is not there to evaluate or criticize victim's IT security practices.

- During an investigative response, the FBI will work alongside the company's own IT security staff, rely on them for knowledge of their systems and procedures, and share our forensic findings with them in near real time whenever possible.

- The FBI will not share victim's identity outside of the US Government, except for situations where we are legally obligated to do so (court orders, criminal prosecution, etc.)

- The FBI does not sign non-disclosure or confidentiality agreements, but all data we collect is considered criminal evidence and protected in accordance with the Federal Rules of Criminal Procedure and all applicable laws.