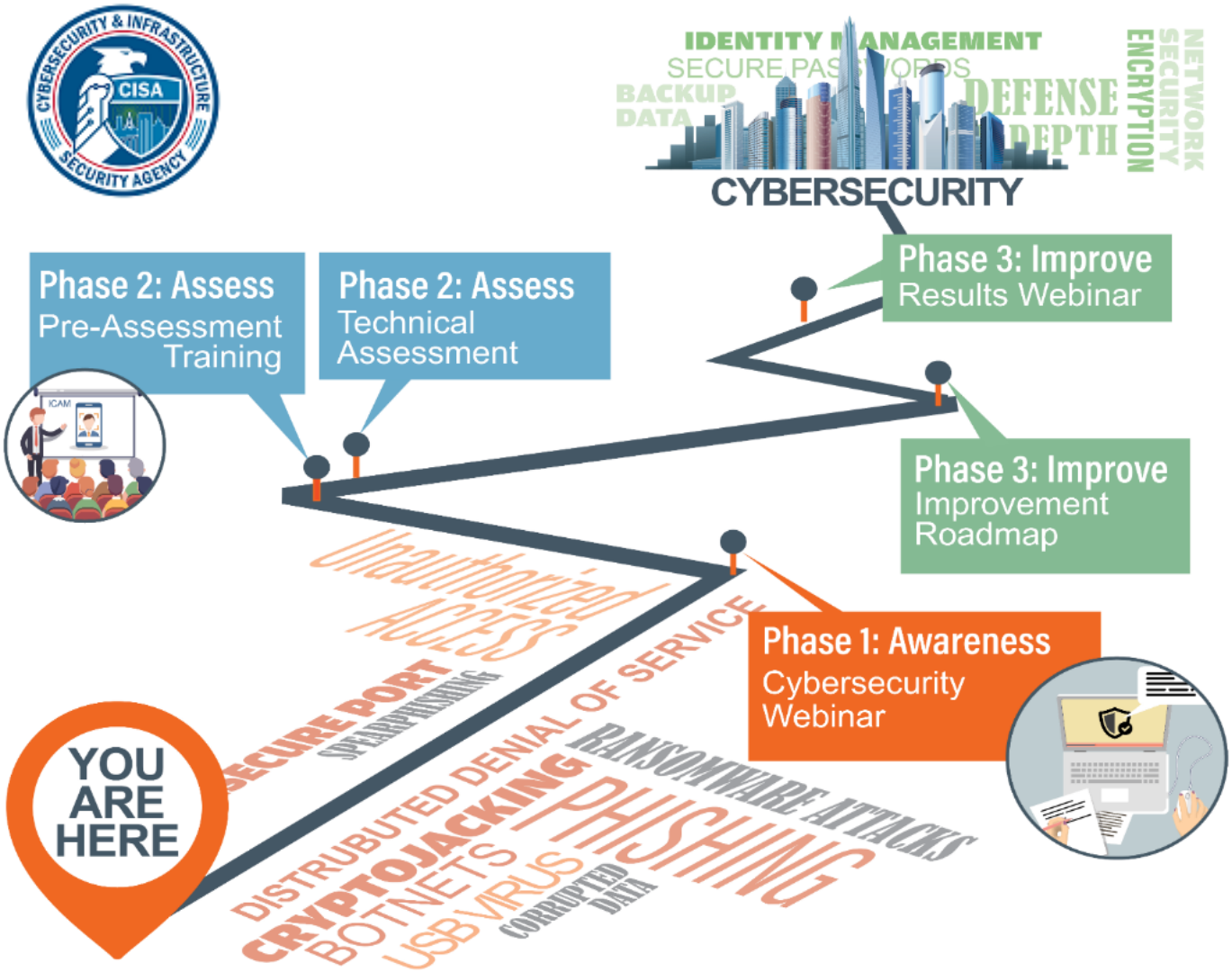


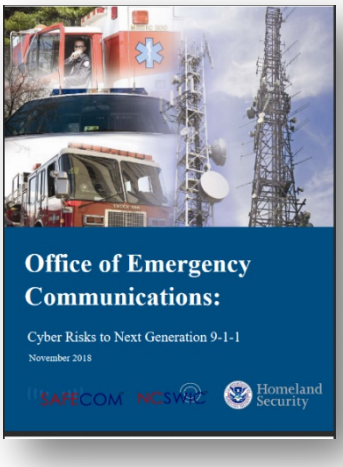
Cybersecurity Awareness Webinar

Handout and Reference Information

Contractor Support to the Interoperable Communications and Technical Assistance Program
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

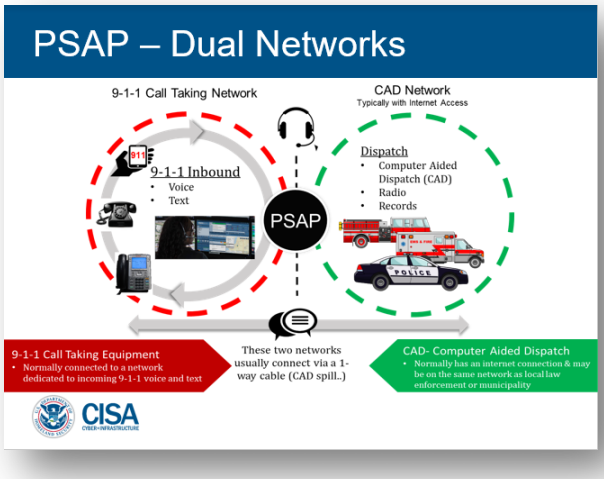
Basic Facts Concerning PSAPs

- PSAPs are critical infrastructure and components are high-value – Your community expects to be able to reach 9-1-1 at any time for assistance
- Disrupting PSAPs creates confusion, disrupts law enforcement for crimes in progress, destroys evidence and harms the public by delaying access to emergency assistance
- An attack on a PSAP may be part of a multi-pronged attack, preventing people from calling for help during an event/attack
- Cyber criminals could potentially infect a 9-1-1 center and then "at will" take it offline prior to some event/attack
- Because PSAP services are so vital, they are more likely to pay a ransom to recover their networks and/or data



PSAP Technology & Communications Ecosystem

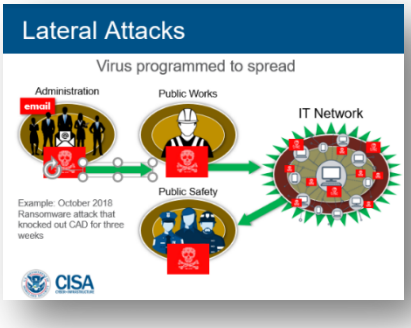
- There are multiple computer systems inside the PSAP for 9-1-1 call handling, text to 9-1-1, CAD, records, and radio/LMR. Each of these systems may have a separate vendor, maintenance contractor and support staff.
- Dispatch network goes beyond the communications center to in-vehicle AVL, MCTs, and LMR
- PSAP management has overall responsibility for all of these support systems
- The 9-1-1 call taking system typically provides a "one-way handoff" of location data to the CAD. The CAD normally sits on a network that is provided locally by the county or municipality. The nature of the physical connection helps to isolate the 9-1-1 call taking equipment <u>BUT</u> there are other ways that the 9-1-1 system can be infected.



Cybersecurity Threats to PSAPs

- **USB Port Awareness:** USB sticks or flash drives are powerful in that they can, in some instances, bypass system security measures
- **Vendor Access:** No matter how well you are supported by a local or regional firm, a third-party maintenance provider or the equipment vendor, their ability to remotely access your systems is a security threat
- **Software Updates:** In July 2017, Equifax (1 of the 3 major credit bureaus) suffered a massive data breach, exposing the sensitive data of approximately 150 million people. Data potentially exposed included names, addresses, driver's license & Social Security numbers, and birthdates
    - Hackers accessed through a known vulnerability in one of their web applications
    - A patch for this security vulnerability was available two months prior to the breach, but the Equifax had not updated its software
- **Outdated Hardware/Equipment:** Older computers, smartphones, and other IT equipment may need to be updated/replaced to maintain performance and/or prevent exposing the network through hardware vulnerabilities. Outdated or discontinued equipment will be more vulnerable because patches, updates, and maintenance are no longer available.
- **Telephony Denial of Service (TDoS):** Disrupting 9-1-1 service via telephone can directly attack via calling 9-1-1 or attacking the admin lines that may also terminate in the 9-1-1 call taking equipment.
- **Browser-based attacks**: Malicious software is injected on websites or delivered with ads.
- **Phishing Attack**: "Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication" Phishing attacks can also be conducted over SMS text message on mobile devices rather than e-mail.
    - When someone clicks on an infected attachment, it loads directly onto the computer, accesses the network and begins to run in the background.
- **Ransomware:** Ransomware is malicious software that hijacks systems & holds data hostage and is accompanied by ransom demands (to be paid in Bitcoin) by a deadline, or risk erasure.

- **Lateral Attacks** –
  - Attacks can be lateral, that is where entry is gained through different departments or government entities connected to the PSAP
  - The malware is programmed to spread
  - In smaller PSAPs, with limited network security budget, this could be a vulnerability



- **Cryptojacking/Cryptomining Progression**
  - ***1st Wave*** - Hack into computer system, steal data (such as credit card information) and then sell it for profit
  - ***2nd Wave***- Hack into computer system, lock it down with ransomware and demand payment in Bitcoin
  - ***3rd Wave***- Hack into computer system and use the computing power, electricity and network access that someone else pays for to 'mine' cryptocurrencies for profit Their goal is to stay undetected – provides them with an ongoing revenue stream.
  - **Insider Attack:** There have been cases where an employee intentionally loads the cryptojacking malware on an employer's computer.

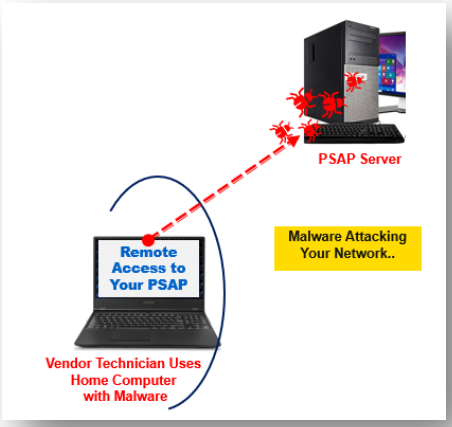
Examples of Cyberattacks on Public Safety Organizations

- Ransomware attack that affected the Augusta (Maine) Police Department, however 9-1-1 was still working
- **Recent Attack Scenarios** in Florida, Arizona, Maryland and Others – TDOS – VOIP
  - Atlanta ransomware attack aftermath article
  - Forbes article on municipal cyberattacks (2021)
  - Business Insider article on how 8 cities were crippled by cyberattacks and what they did to fight them
- **Phishing Examples**
  - **False e-mail addresses -** *ITmanager@cityofbaltimore.com*
  - **Fake URLs & hyperlinks -** *http://cityofbaltimore911.com/login/unlock.html*
  - **"Urgent problem" messages -** *Your password has expired and must be reset immediately. Click Here to reset your login*

- **Illegal activity scares -** *Warning: your account has been suspended for policy violation—xxx adult sites. Contact your IT manager for more information*
- **Unclaimed Prizes -** *Congratulations! You have been selected to receive a $50 amazon gift card. Click Here to claim your valued customer reward*

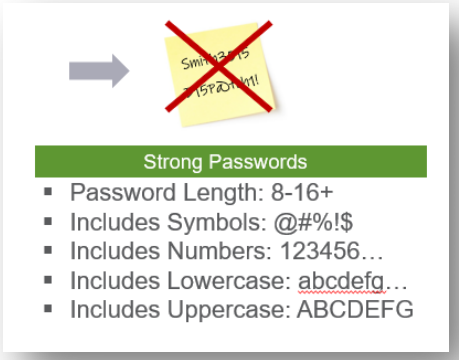
Best Practices & Cyber Hygiene 101

- **Access Related**
  - **Logins**:
    - In numerous PSAPs across the country, all Telecommunicators use a single username and password for the 9-1-1 systems, which provides no logging or auditing capability
    - Create individual logins for all users, vendor staff and guests
    - Periodically, review and update and/or audit log ins
  - **Remote (Vendor) Access:**
    - Any "Closed Network" becomes vulnerable by allowing remote access
    - IT systems maintenance is often the responsibility of vendors who respond to the site or have remote access to resolve "trouble tickets" and perform other services.
      - Be sure that staff are aware of what vendors have permission to access in your physical and virtual spaces
      - Have procedures in place so that you are aware of when these services are scheduled, being performed, finished, etc.
      - Managing vendor access so that you have good records of who, what, when, and why people had access



    - Request an audit of who has access to your system
      - Insist your system have a unique login for each "outsider"
      - Understand how each vendor handles passwords after an employee event (termination, resignation, promotion, etc.).

- **Passwords** - Strong passwords are a part of identification management and baseline defense against intrusion
    - Strong passwords are a part of identification management and baseline defense against intrusion
    - Regularly change user passwords
    - NEVER allow passwords to be posted where they are visible to other personnel, visitors, or could accidentally be seen in social media posts, etc.
    - Never send passwords over the Internet.
    - Do not use the same password across logins & accounts.



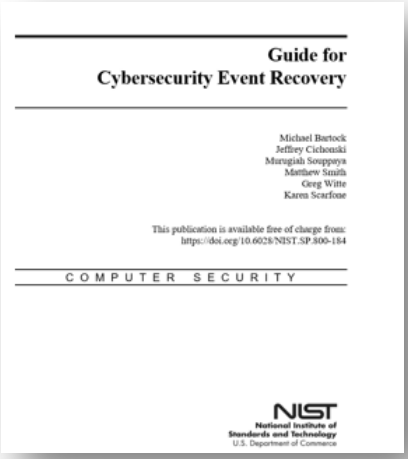
- **Consider Multi-Factor Authentication** – Beyond just your staff
    - During major events/emergencies, mutual aid or staff shortages additional staff may be required to successfully manage the emergency.
    - Have a system in place ahead of time that will verify and keep track of who is getting access to the PSAP physical and network spaces, to make sure they are who they say they are.

- **<u>Procedural</u>**
    - **USB Ports**
        - USB drives on all PSAP/Dispatch Center workstations should be locked out, so they are only active when the workstation is accessed by using an administrator password
        - Personal smartphones and tablets should not be allowed to be charged via a USB attached to any computer on the PSAP/Dispatch Center network
    - **Social Media**
        - All PSAPs and Dispatch Centers must have a written social media policy
        - Should not allow social media access or personal web-based email access from the network
        - Consider a separate WI-FI network for non-official/public access, especially if the PSAP/Dispatch Center is located in a building with public access for other uses
        - If you choose to allow access:
            - Require the use of two factor authentication for login
            - Remind staff that clicking on any link May Be Dangerous

        - It is critical that you provide training and instruct staff on the dangers of phishing, not only to them personally but on the potential negative impact on your operations
    - **Software Updates**
        - Understand and document how your vendors process and/or how quickly they review and install updates to your systems
        - Understand and document how they receive update alerts and agree to a maximum timeframe to address/implement the updates
    - **Offline Backups Are Critical**
        - Plans/procedures must be in place to ensure regularly scheduled backups
        - Should be stored offline, meaning if you are attacked, the backups should be isolated from the attacked network
        - Must review handling of backups to ensure that they are not re-infected
    - **Hardware Inventory** – Includes equipment manufacturer, model number, manufacturing/release date, serial number, physical location, etc.
        - To address potential hardware needs, PSAPs/Dispatch Centers should maintain a regularly updated inventory of hardware/electronic assets.
        - Outdated and/or discontinued hardware/equipment will be more vulnerable because patches, updates, and maintenance are no longer available.
    - **Use of Wi-Fi Printers In Your Center** – Do not allow individuals to bring in printers from home or their offices with Wi-Fi access and connected to the Dispatch or Emergency Operations Centers network because they tend to be easily hacked.
- **Separate Your Internal Networks**
    - Distinct portions of the network (for example the municipality Finance Department and the PSAP) should reside on separate subnets to minimize the impact of a lateral attack.
    - Put sensitive information and/or HIPAA related data behind additional firewalls.
    - Some larger PSAPs have had their vendors place groups of workstations on separate segments – This will help contain malware/ransomware or other negative events.
- **Watch for signs of Cryptojacking/Cryptomining**
    - Slow performing CAD computers
    - Spike in electricity bill
    - Review outbound internet traffic periodically to detect anomalies
- **Training – Cybersecurity & Phishing -** It's important for PSAPs/Dispatch Centers to conduct periodic training covering all major cybersecurity risk areas and related operating procedures. It is especially important to cover phishing awareness, so employees know to contact IT before clicking on potentially suspicious links and accidentally exposing the network.

Responding and Reporting Cyber Incidents

- Utilize the Cyber Security Incident Response Plan specifically created for your organization OR follow Review the NIST Publication 800-184
- In the event of a cyberattack, follow the NIST Guide for Cybersecurity Event Recovery
- If you are currently experiencing a cyberattack, APCO recommends the following:
  1. Contact your local authorities
  2. Contact your vendors (phone company, CAD, Records, etc.)
  3. Implement your cyber response plan (If you don't have one, you should)
  4. Contact the Department of Homeland Security National Coordinating Center – National Cybersecurity and Communications Integration Center (DHS NCCIC) at 703-235-5080 or ncc@hq.dhs.gov
  5. File a complaint with the FBI Internet Crime and Complaint Center (IC3) at ic3.gov. Include keywords "PSAP, Public Safety" in the description of the incident
  6. Contact APCO at cybersecurity@apointl.org (Note: this email address is not monitored 24/7)



Key Federal Points of Contact

Threat Response	*Asset 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 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.*
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.*	

Organization	Description and Link
Association of Public-Safety Communications Officials-International (APCO)	APCO has sections dedicated to cybersecurity, as well as other helpful materials on its website: https://www.apcointl.org/advocacy/topics/cybersecurity.html • "An Introduction to Cybersecurity" https://www.apcointl.org/download/introduction-to-cyber-security-a-guide-for-psaps/?wpdmdl=6250
Alliance for Telecommunications Industry Solutions (ATIS)	ATIS provides public safety industry best practices ranging from "important", "highly important", to "critical" for PSAPs. http://www.atis.org/bestpractices/Search.aspx
Center for Internet Security (CIS)	CIS gives cybersecurity tips and warnings on discovered recently vulnerabilities and threats. https://www.cisecurity.org/resources/
Government Technology	Government Technology magazine reports the latest on public sector information technology. There is a section dedicated to NG9-1-1 on its website. http://www.govtech.com/em/next-gen-9-1-1/
ISACA	ISACA develops practices for information systems. Their COBIT 5 framework provides IT governance and management practices. http://www.isaca.org/cobit/
International Telecommunications Union (ITU)	PSAPs can utilize ITU's Security Standards Roadmap to develop security standards and gain understanding of existing standards and those that are in progress. http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/default.aspx
National Emergency Numbering Association (NENA)	NENA's website contains a complete archive of all its 9-1-1 standards, including those related to NG9-1-1, such as the i3 suite of standards and the NG-SEC standard (NENA 75-001). https://www.nena.org/?page=Standards
Open Web Application Security Project (OWASP)	OWASP is an online community that focuses on web application security. The website hosts free security related resources. https://www.owasp.org/index.php/Main_Page
SANS Institute	SANS Institute's 20 Critical Security Controls details prioritized cyber defense actions that can help PSAPs prevent and mitigate cyber risks. https://www.sans.org/critical-security-controls
SecuLore Solutions	SecuLore offers public safety oriented cybersecurity products and services. Its resource webpage archives cyber-attacks, cyber guidelines, and webinars. https://www.seculore.com/resources
Urgent Communications	Urgent Communications provides news and publications on information and communication technology. There is a section dedicated to NG9-1-1 on its website. http://urgentcomm.com/topics/ng-9-1-1

Funding and Sustainment:

- **2015 Funding Mechanisms Guide**: Provides a variety of funding mechanisms state and local governments can leverage in place of grant funding
- **2018 Emergency Communications Lifecycle Planning Guide**: Assists stakeholders in their efforts to fund, plan, procure, implement, support, and maintain public safety communication systems
- **Life Cycle Planning Tool**: Provides a worksheet to assist stakeholders in planning for public safety communications projects

Priority Services:

- **Priority Telecommunications Services for First Responders**: Provides a variety of tools and resources for improving interoperability and communications

Websites:

GETS: www.dhs.gov/gets

WPS: www.dhs.gov/wps

TSP: www.dhs.gov/tsp

GET/WPS Document: www.dhs.gov/publication/getswps-documents

Training Videos: www.dhs.gov/pts-videos

Technology:

- **Public Safety Communications: Ten Keys to Improving Emergency Alerts, Warning, and Notifications: Top Ten Keys:** Provides best practices for improving emergency alert, warning, and notification systems
- **The Internet of Things: Impact on Public Safety Communications**: Provides an overview of the Internet of Things, including benefits and resources

Resilience:

- **Public Safety Communications Resiliency: Ten Keys to Obtaining a Resilient Local Access Network:** Provides best practices for public safety communication resiliency
- **Resiliency Fact Sheet:** Provides an overview of ECD's available resiliency resources
- **Public Safety Communications Resiliency Self-Assessment Guidebook:** Provides a self-assessment methodology for public safety entities to identify and address potential points of failure

Federal Points of Contact
Federal Asset Response Contacts:

Upon voluntary request, federal asset response includes providing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents while identifying other entities that may be at risk, assessing potential risks to the sector or region, facilitating information sharing and operational coordination, and providing guidance on how to best use federal resources and capabilities

What You Can Expect:

- Specific guidance to help evaluate and remediate ransomware incidents
- Remote assistance to identify the extent of the compromise and recommendations for appropriate containment and mitigation strategies (dependent on specific ransomware variant)
- Phishing email, storage media, log and malware analysis, based on voluntary submission (full-disk forensics can be performed on an as-needed basis)
- **Contacts:**
  - **CISA:**
    - www.us-cert.cisa.gov/report, Central@cisa.gov or (888) 282-0870
  - **Cybersecurity Advisor**
    - www.cisa.gov/cisa-regions

        - [Enter your local CISA CSA's phone number and email addresses.]
    - **MS-ISAC:**
        - soc@msisac.org or (866) 787-4722

Federal Threat Response Contacts:

Upon voluntary request, federal threat response includes law enforcement and national security investigative activity: collecting evidence and intelligence, providing attribution, linking related incidents, identifying additional affected entities, identifying threat pursuit and disruption opportunities, developing and executing action to mitigate the immediate threat, and facilitating information sharing and operational coordination with asset response.

What You Can Expect:

- Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, to include system images and malware samples.
- **Contacts:**
    - **FBI:**
        - www.fbi.gov/contact-us/field-offices
        - Your local FBI field office https://www.fbi.gov/contact-us/field-offices/
    - **US Secret Service:**
        - www.secretservice.gov/contact/field-offices/
        - Your local USSS field office https://www.secretservice.gov/contact/field-offices

Ransomware Resources

- **Ransomware: What it is and What to do about it (CISA):** General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf
- **Ransomware (CISA):** Introduction to ransomware, notable links to CISA provide products to protecting networks, specific ransomware threats, and other resources: www.us-cert.cisa.gov/Ransomware

- **Security Primer-Ransomware (MS-ISAC):** Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: www.cisecurity.org/white-papers/security-primer-ransomware/
- **Ransomware: Facts, Threats, and Countermeasures (MS-ISAC):** Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/
- **Security Primer-Ryuk (MS-ISAC):** Overview of Ryuk ransomware, a prevalent ransomware variant in the SLTT government sector, that includes information regarding preparedness steps organizations can take to guard against infection: www.cisecurity.org/white-papers/security-primer-ryuk/