DHS Cybersecurity

Election Infrastructure as Critical Infrastructure

June 2017

Homeland Security

Department of Homeland Security

Safeguard the American People, Our Homeland, and Our Values

- Homeland Security Missions
  1. Prevent Terrorism and Enhance Security
  2. Secure and Manage Our Borders
  3. Enforce and Administer Our Immigration Laws
  4. Safeguard and Secure Cyberspace
  5. Strengthen National Preparedness and Resilience

- Our work provides a holistic risk management approach for the 16 critical infrastructure sectors with unique legal authorities supporting true private public collaboration

- We support State and local governments, Federal partners, and private sector owners and operators in the management of their cyber and physical risk

Homeland Security

DHS and Election Security

Ensuring Election Officials Receive Benefits

- DHS's mission to assist state and local officials in strengthen the security of their networks has established trusted relationships between DHS and state and local CIOs and CISOs.
- DHS has provided numerous no-cost, voluntary cybersecurity services to these officials.
- As state and local officials, election officials are eligible for all of the same benefits and services. In the course of outreach, we learned that in many states, election officials were not aware of nor benefiting from these services.
- DHS has since made a concerted effort to reach out to the election community.
- DHS services are available only upon request, and are voluntary; they do not entail regulation or binding directives of any kind

Homeland Security

Free DHS Cybersecurity Services

DHS Services	Summary
Cyber Hygiene Scanning	Automated, recurring scans of internet facing systems to identify public facing vulnerabilities and configuration errors. This service provides the "**adversary view**" of your networks
Risk and Vulnerability Assessment	• **Penetration testing** • Social engineering • **Wireless access discovery** • Database scanning • Operating system scanning
Cyber Resilience Reviews	Policy oriented review of an organization's information security practices
Phishing Campaign Assessment	Longer term engagement testing an organization's aptitude for handling and addressing **spearphishing** attempts of various degrees of sophistication
NCCIC/ MS-ISAC Security Tips, Alerts, and Information Sharing	Provides **alerts**, **analysis reports**, bulletins, best practices, **cyber threat indicators**, guidance, points-of-contact, security tips, and technical documents to stakeholders
Cyber Security Advisors & Protective Security Advisors	Regionally located personnel who engage state and local governments, election crime coordinators, and vendors to offer **immediate and sustained assistance**, coordination, and outreach to prepare and protect from cyber and physical threats.
NCCIC/ MS ISAC Incident Management	24x7 cybersecurity operations centers that maintained close coordination among the private sector, government officials, the intelligence community, and law enforcement to provide situational awareness and **incident response**, as appropriate.

Homeland Security

For more information on services, please email **SLTTCyber@hq.dhs.gov**

Social Engineering and Phishing Attacks

Security Tip (ST04-014) https://www.us-cert.gov/ncas/tips/ST04-014

- In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.
- Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization.
- Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as
  - Natural Disasters
  - Epidemics and Health Scares
  - Economic Concerns
  - **Political Elections**

Homeland Security

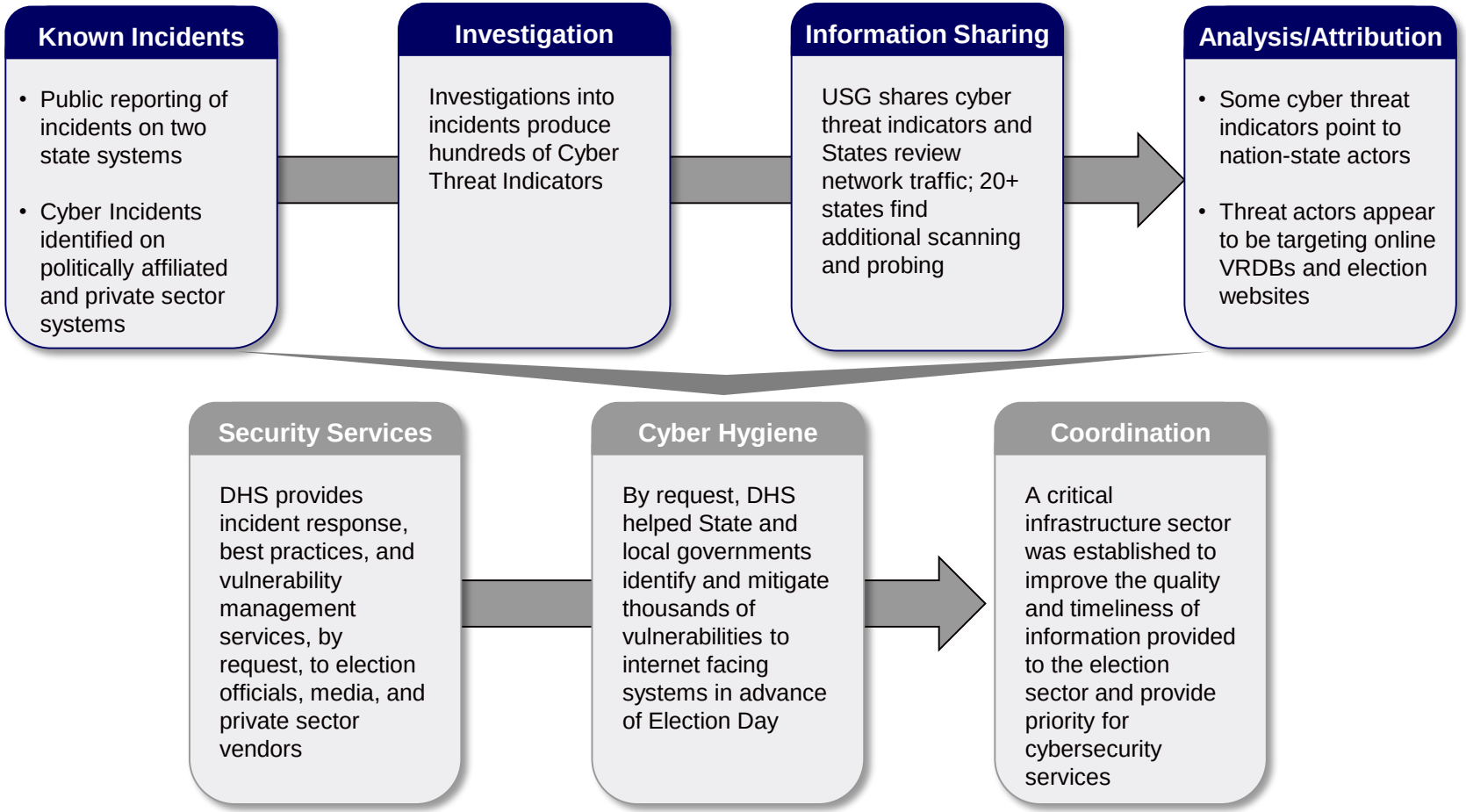
Social Engineering and Phishing Attacks

Security Tip (ST04-014)

- How do you avoid being a victim?
  - Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
  - Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
  - Don't send sensitive information over the Internet before checking a website's security.
  - Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain
  - Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. Take advantage of any anti-phishing features with email client/ web browser.
- What do you do if you think you are a victim?
  - If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
  - If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
  - Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future. Watch for other signs of identity theft.
  - Consider reporting the attack to the police, and file a report with the Federal Trade Commission.

Homeland Security

2016 Election Cycle



At this time, we have no evidence of voting systems being targeted, impacted, or votes having been manipulated

Homeland Security

Election Infrastructure as Critical Infrastructure

How did we get here?

- On January 6, 2017, Secretary Jeh Johnson established election infrastructure as a critical infrastructure sub-sector of the existing government facilities sector. This announcement meant that:
  - DHS had determined that systems and assets included in election infrastructure meet this definition of critical infrastructure; and
  - DHS would establish a voluntary mechanism for coordinating with the members of this critical infrastructure community
- Definition of Critical Infrastructure: “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”
- State, Local, Tribal, and Territorial Governments are existing participants in critical infrastructure mechanisms
- The objective of establishing this sub-sector is to provide State and Local election officials and private sector election community with timely and tailored threat information and cybersecurity services

Homeland Security

Election Infrastructure

Election infrastructure represents the assets, systems, and networks most critical to the security and resilience of the election process, which includes:

- **Storage facilities**, which may be located on public or private property that may be used to store election and voting system infrastructure before Election Day
- **Polling places** (including early voting locations), which may be physically located on public or private property, and may face physical and cyber threats to their normal operations on Election Day
- **Centralized vote tabulation locations**, which are used by some State and localities to process absentee and Election Day voting materials
- IT infrastructure and systems used to **maintain voter registration databases**
- **Voting systems** and associated infrastructure, which are generally held in storage but are located at polling places during early voting and on Election Day
- **Information technology infrastructure and systems used to manage elections**, which may include systems that count, audit, and display election results on election night on behalf of state governments, as well as for postelection reporting used to certify and validate results

Homeland Security

Benefits of Designation

An Overview

- Prioritization of services
  - Critical infrastructure has priority over non- CI sectors for certain government offered services and resources
- Liability Protections for Threat and Vulnerability Information Sharing
  - Classified information briefings, as appropriate
  - Voluntary **coordinating councils** to share information with certain Critical Infrastructure Partnership Advisory Council (CIPAC) policy protections
  - Protected Critical Infrastructure Information: Operators of critical infrastructure can voluntarily share vulnerability information with DHS via PCII mechanism to ensure that mitigations can be applied by all while **exempting that information's dissemination** in Freedom of Information Act (FOIA) requests, use in civil litigation, and regulatory use
- Attribution/ Enforcement benefits (EO 13964)
  - U.S. can hold foreign actors accountable for cyber attacks on critical infrastructure

Homeland Security

SLTTCyber@hq.dhs.gov
Geoffrey.Hale@hq.dhs.gov