DHS Cybersecurity

Election Infrastructure as Critical Infrastructure

May 2017

Homeland Security

Department of Homeland Security

Safeguard the American People, Our Homeland, and Our Values

- Established in March of 2003 and combined 22 different Federal departments and agencies into a unified, integrated Department
- Homeland security is a widely distributed and diverse national enterprise
  - Collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners to maintain critical homeland security capabilities
- 2014 QHSR 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

Homeland Security

National Protection and Programs Directorate

Enhance the Resilience of the Nation's Infrastructure

- Our mission is to protect cyber and critical infrastructure
  - Terrorism and other physical threats
  - Growing cyber threats
- 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

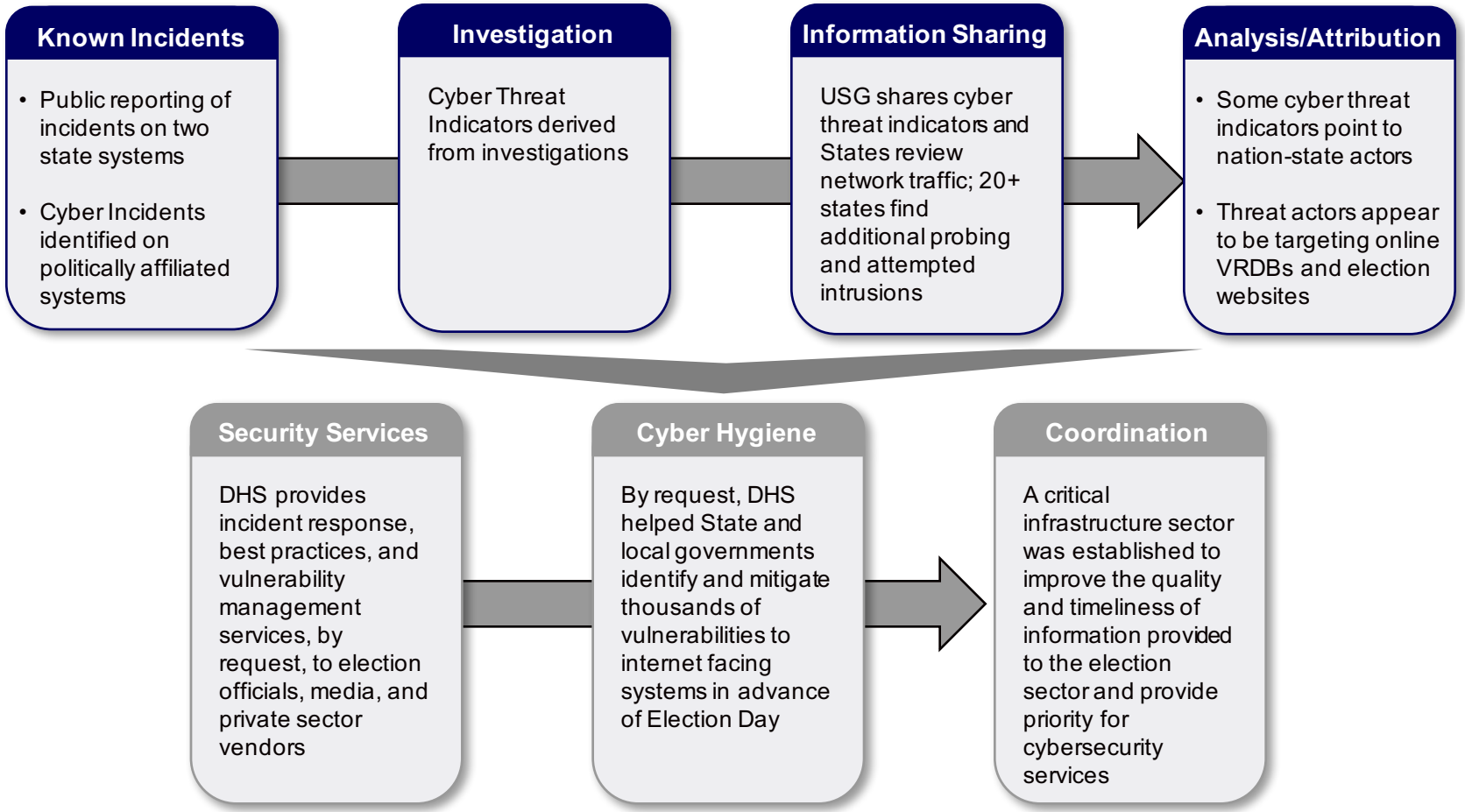
Interest in Elections

Ensuring Election Officials Receive Same Benefits

- As the capabilities that enable elections are becoming increasingly dependent on information and communications technology, election officials are assuming greater responsibility for the cybersecurity of these systems
- DHS has built trusted relationships with state and local IT officials to strengthen the security of their networks and is providing outreach to election officials to ensure that they are aware of the no-cost cybersecurity services that are available to them
- DHS services are available only upon request, and are voluntary; they do not entail regulation or binding directives of any kind

Homeland Security

Cybersecurity of 2016 Election Infrastructure



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

Homeland Security

DHS Cybersecurity Services

Needs	DHS Services	Summary
Identifying and Limiting Vulnerabilities	Cyber Hygiene Scanning	Automated, recurring scans of internet facing systems that provide the perspective of the vulnerabilities and configuration errors that a potential adversary could see
	Risk and Vulnerability Assessment	• Penetration testing • Social engineering • Wireless access discovery • Database scanning • Operating system scanning
Assessing Threats and Sharing Information	NCCIC Tips and Alerts	Provides alerts, analysis reports, bulletins, best practices, cyber threat indicators, guidance, points-of-contact, security tips, and technical documents to stakeholders
	MS-ISAC Security Tips	
Applying security expertise and best practices	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.
	Cyber Resilience Reviews	Policy oriented review of an organization's information security practices
Incident Response	NCCIC	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.
	MS-ISAC	

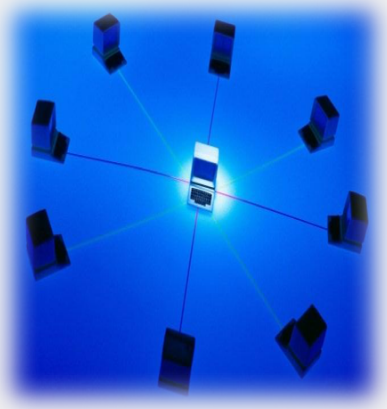
Homeland Security

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

Identifying Vulnerabilities

Cyber Hygiene

- Overview
  - A no-cost, remote, recurring, un-credentialed scan of internet-facing systems for known vulnerabilities and configuration errors
  - Provides the perspective of how your networks appear to an attacker
  - DHS provides a regular report of scan findings and will work with organizations to proactively mitigate vulnerabilities and reduce exposure to known threats
  - The recurring cadence of the scanning and reporting enables newly identified vulnerabilities to be scanned for and provides a progressively improving picture of the organizations cybersecurity posture
  - Specific findings are for that organization's eyes only



Homeland Security

Identifying Vulnerabilities

Risk and Vulnerability Assessment (RVA)

- Overview
  - A no-cost, in-depth assessment of internal and external networks
  - Parties can choose from a series of assessment services (below)
  - Assessments may be conducted onsite, remotely, or both

Assessment Services	Description
Penetration Testing	Exploit weakness or test responses in systems, applications, network and security controls
Social Engineering	Crafted e-mail at targeted audience to test Security Awareness / Used as an attack vector to internal network
Wireless Discovery & Identification	Identify wireless signals (to include identification of rogue wireless devices) and exploit access points
Web Application Scanning and Testing	Identify web application vulnerabilities
Database Scanning	Security Scan of database settings and controls
OS Scanning	Security Scan of Operating Systems deployed throughout network

Security Expertise and Best Practices

Cyber Security Advisors (CSA) & Protective Security Advisors (PSA)

- Regionally-based DHS personnel
- Direct coordination to bolster the preparedness, risk mitigation, and incident response capabilities of SLTT governments and private sector critical infrastructure entities at no-cost
- Provide actionable information and able to connect election officials to a range of tools and resources available to improve the preparedness of election IT systems and the physical site security of voting machine storage and polling places
- Available to assist with planning and incident management assistance for both cyber and physical incidents
- Currently 8 CSAs and ~100 PSAs

Homeland Security

Security Expertise and Best Practices

Cyber Resilience Reviews

- Overview
  - A no-cost, assessment of the resilience of an organization's cybersecurity program through its policies and procedures
  - The review is based on the CERT Resilience Management Model and aligns with NIST's Cybersecurity Framework
  - It seeks to understand the key capabilities needed to improve an organization's cybersecurity risk management posture.
  - May be conducted as a self-assessment or in-person interview

Homeland Security

Information Sharing

National Cybersecurity and Communications Integration Center

- DHS NCCIC is a 24x7 cyber situational awareness, incident response, and management center and a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement

- The NCCIC leads the protection of the federal civilian agencies in cyberspace, provides support and expertise to critical infrastructure owners and operators, and works with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide information to SLTT governments

Homeland Security

Incident Response

Multi-State Information Sharing and Analysis Center (MS-ISAC)

- Membership includes all 50 States and over 1000 local government organizations, U.S. territories and tribal nations
- Supports CS&C's efforts to secure cyberspace by disseminating early warnings of cyber threats to SLTT governments
- Shares security incident information and analysis
- Runs a 24-hour watch and warning security operations center
- Provides Albert II Intrusion Detection

If there is a suspected or confirmed cyber incident that:

- Affects core government functions;
- Affects critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems; or
- Indicates malicious software is present on critical systems.

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

Homeland Security

Call: (866) 787-4722
Email: soc@msisac.org

Establishing a Critical Infrastructure Sector

Homeland Security

Election Infrastructure as Critical Infrastructure

How did we get here?

- 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
- 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
- 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 assessments and services
- Greater 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
  - U.S. can hold foreign actors accountable for cyber attacks on critical infrastructure systems

Homeland Security

Benefits of Designation

Reduce System Vulnerabilities

In addition to the services already discussed…

- Designation as a sub-sector establishes mechanisms to rapidly share information across the community to identify and mitigate system vulnerabilities
- Coordinating councils will be established, focused on the physical and cyber security and resilience of the election infrastructure
  - Coordinating councils are used to share information on vulnerabilities and threats and to enable collaboration across Federal, state, and local governments, as well as with private sector partners, to determine ways to mitigate risks
  - Participation in the council is voluntary
  - Coordinating Councils are used widely by the private sector critical infrastructure community (Energy SCC, FS-SCC, IT-SCC, etc)

Homeland Security

Benefits of Designation

Reduce System Vulnerabilities (continued)

- Critical Infrastructure Partnership Advisory Council (CIPAC) protections
  - Allows sector coordinating councils to include private vendors and experts from information technology firms to actively participate in sensitive security conversations and planning alongside their government partners
  - This would provide election officials with greater access to a broad range of technical and security expertise
- Protected Critical Infrastructure Information (PCII)
  - Operators of critical infrastructure can voluntarily share information with DHS via PCII to exempt that information's dissemination in Freedom of Information Act (FOIA) requests, use in civil litigation, and regulatory use
  - States, vendors, or individuals that identify vulnerabilities in election infrastructure can share this information, to the benefit of all who leverage these systems, without fear that it will be used against them
  - Provides an effective mechanism for election officials to share vulnerability information and ensure that mitigations can be applied by all

Homeland Security

Benefits of Designation

Understand Threats to Election Infrastructure

In addition to the services already discussed…

- Designation as a subsector allows DHS to provide security clearances to election officials, as appropriate
- Election officials could be briefed on relevant classified intelligence and leverage that to secure their systems in a manner more informed of the threats they face

Homeland Security

Benefits of Designation

Respond to Incidents and Malicious Cyber Actors

In addition to the services already discussed…

- Designation as a sub-sector allows owners and operators of election infrastructure to benefit from the U.S. government's strategic and policy-based efforts to protect critical infrastructure
  - Promotion of international norms that prohibit peacetime cyber attacks against critical infrastructure
  - Use of Executive Orders to respond to attacks on critical infrastructure

Homeland Security

Executive Order 13964

Respond to Incidents and Malicious Cyber Actors

- As a sub-sector of critical infrastructure, the Secretary of Treasury is able to sanction persons responsible for cyber enabled activities that harm or compromise a computer that supports an entity in a critical infrastructure sector
  - This would cover malicious cyber attacks that, for example, deleted data, impaired the function of a system, or destroyed a system
- On 29 December 2016, EO 13694 was amended to enable the Secretary of Treasury to also sanction persons responsible for cyber enabled activities that tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions
  - These protections may serve to deter future malicious cyber behaviors or allow the U.S. government to hold cyber actors accountable for their actions.

Homeland Security

Critical Infrastructure Designation in Practice

What does it all mean?

- The authorities, responsibilities, and sovereignty of state and local governments over elections does not change due to this designation
- Some election officials may—
  - Receive more information from the Federal Government regarding the threats and vulnerabilities seen impacting election infrastructure
  - Receive security clearances
- This designation does not allow DHS to tell election officials to operate in any directive manner. This means:
  - There will not be any DHS security requirements (other than the handling of classified information)
  - DHS will not provide binding recommendations or regulations
  - DHS is not “taking over” elections.
- DHS will provide elections officials who are interested with risk management information and resources, to support their risk-informed decision making.

Homeland Security

Homeland Security

SLTTCyber@hq.dhs.gov