Homeland Security

DHS Cybersecurity: Services for State and Local Officials

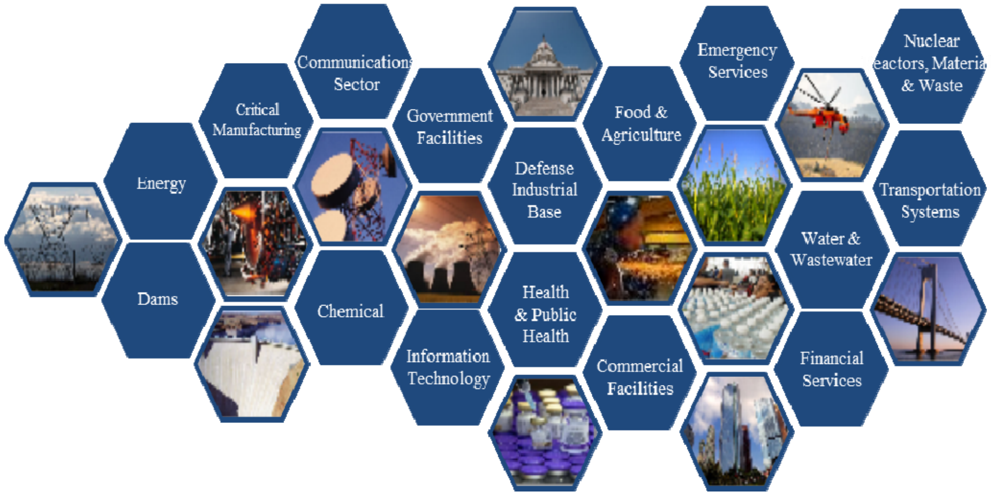
January 2017

Department of Homeland Security

- 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

National Protection and Programs Directorate

- 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 build cyber and physical risk management capacity of Federal partners, private sector owners and operators, state and local agencies, and others



Our Cybersecurity Responsibilities

- Protect Federal Civilian Executive Branch networks from malicious cyber actors

- Support private sector and state, local, tribal, and territorial governments in the management of their cyber risk

- Provide technical assistance in the event of a cyber incident, as requested

Lines of Effort

Information Sharing

Risk Assessments

Incident Response

Cyber Ecosystem

Federal Common Cybersecurity Baseline

Interest in Elections

- 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

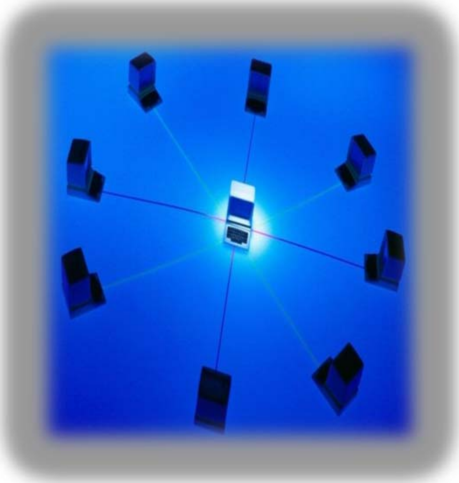
- DHS services are available only upon request, and are voluntary; they do not entail regulation or binding directives of any kind

Cyber Hygiene (CH)

- Overview
  - Assess stakeholders internet accessible systems for known vulnerabilities and configuration errors on a recurring basis
  - DHS will work with impacted agencies to proactively mitigate threats and risks to their systems prior to exploitation by malicious third parties
  - Agency specific data is for that agency’s eyes only

- Objectives
  - Establish enterprise view of the Federal, SLTT, and critical infrastructure public cybersecurity posture
  - Understand how your networks appear to an attacker

- Benefits
  - Complements an agency’s existing security program and capabilities
  - Provides an objective view of an agency’s public security posture
  - Reduced exposure to known threats



Risk and Vulnerability Assessment (RVA)

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
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

In-depth, onsite assessments of internal and external networks

National Cybersecurity and Communications Integration Center (NCCIC)

National Cybersecurity and Communications Integration Center (NCCIC)

- The DHS National Cybersecurity and Communications Integration Center (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

National Cybersecurity and Communications Integration Center (NCCIC)

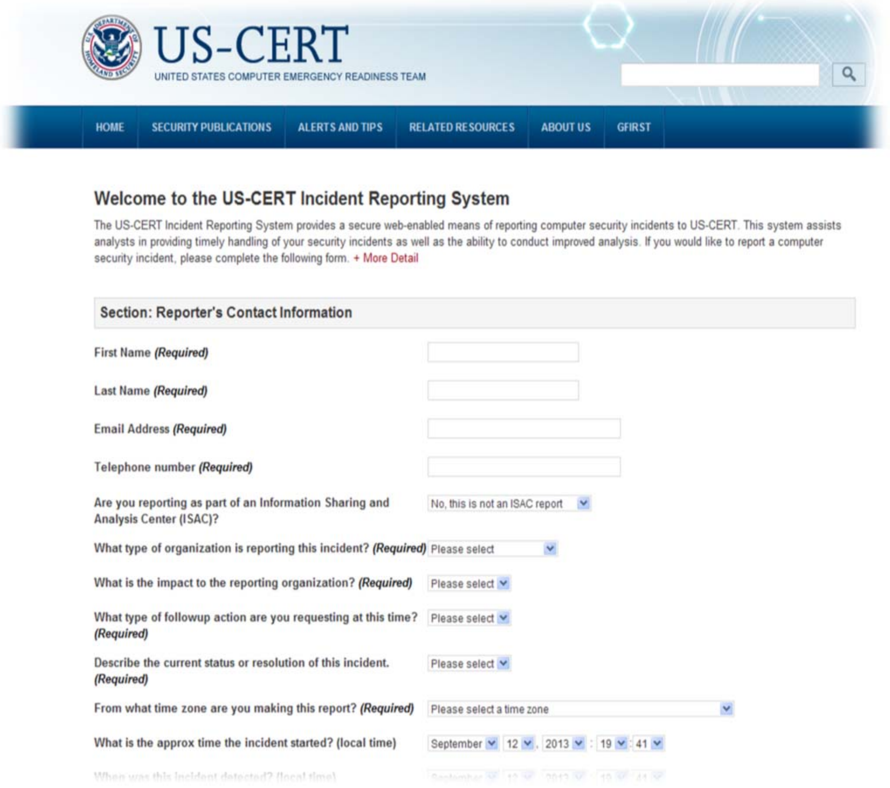
Reporting an Incident

The NCCIC operates 24x7x365 and can be reached at 1-888-282-0870 or by visiting https://forms.us-cert.gov/report.

When to Report an Incident

If there is a confirmed cyber or communications event or incident that:

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



Welcome to the US-CERT Incident Reporting System

The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to US-CERT. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. + More Detail

Section: Reporter's Contact Information

First Name *(Required)*	
Last Name *(Required)*	
Email Address *(Required)*	
Telephone number *(Required)*	
Are you reporting as part of an Information Sharing and Analysis Center (ISAC)?	No, this is not an ISAC report
What type of organization is reporting this incident? *(Required)*	Please select
What is the impact to the reporting organization? *(Required)*	Please select
What type of followup action are you requesting at this time? *(Required)*	Please select
Describe the current status or resolution of this incident. *(Required)*	Please select
From what time zone are you making this report? *(Required)*	Please select a time zone
What is the approx time the incident started? (local time)	September 12 , 2013 : 19 : 41
When was this incident detected? (local time)	September 12 , 2013 : 19 : 41

Multi-State ISAC

MS-ISAC

MULTI-STATE
Information Sharing
& Analysis Center™

Multi-State Information Sharing and Analysis Center

- 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

MS-ISAC

How to Report a Suspected Incident:

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

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.

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

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

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

- Regionally-based DHS personnel
- Direct coordination to bolster the cybersecurity 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 cybersecurity preparedness of election 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

In Summary

Needs	DHS Services	Summary
Vulnerability Identification and Mitigation	Cyber Hygiene Scanning	Automated scans of internet facing systems: • Configuration error • Vulnerability scanning
	Risk and Vulnerability Assessment	• Penetration testing • Social engineering • Wireless access discovery • Database scanning • Operating system scanning
Information Sharing	NCCIC Alerts	Provides support and expertise to critical infrastructure owners and operators, and SLTT governments.
	MS-ISAC	Provides advisories, newsletters, cybersecurity guides and toolkits from the central resource for situational awareness and incident response for SLTT
Local, In-Person Support	Cyber Security Advisors Protective Security Advisors	Regionally located personnel that provide immediate and sustained assistance, coordination, and outreach to prepare and protect from cyber and physical threats.
Incident Response	NCCIC	The Federal Government's 24X7 cyber situational awareness, incident response, and management center.
	MS-ISAC	24X7 Security Operations Center serving as a central resource for situational awareness and incident response for SLTT governments.

For more information email SLTTCyber@hq.dhs.gov

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
  - Information technology 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

Election Infrastructure as Critical Infrastructure

- 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.”

- DHS has determined that systems and assets included in election infrastructure meet this definition of critical infrastructure

- On January 6, 2017, Secretary Jeh Johnson established election infrastructure as a critical infrastructure sub-sector of the existing government facilities sector
  - Secretary Johnson identified DHS’s National Protection and Programs Directorate as the sector specific agency for the election infrastructure sub-sector

Designation of Critical Infrastructure Sectors

Energy

Dams

Critical Manufacturing

Communications Sector

Chemical

Government Facilities

Information Technology

Defense Industrial Base

Health & Public Health

Food & Agriculture

Commercial Facilities

Emergency Services

Water & Wastewater

Financial Services

Nuclear eactors, Materia & Waste

Transportation Systems

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)

Benefits of Designation – Reduce system vulnerabilities (cont)

- 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

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

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

Executive Order 13964

- 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

Q&A

SLTTCyber@hq.dhs.gov