Homeland Security

DHS Cybersecurity: Services for State and Local Officials

September 2016

DHS Office of Cybersecurity and Communications

Mission

[We are] Responsible for enhancing the security, resiliency and reliability of the Nation's cyber and communications infrastructure. CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent and respond to catastrophic incidents that could degrade or overwhelm these strategic assets

Practice

DHS provides services and expertise to infrastructure owners to assist with protecting their systems

Interest in Elections

As the capabilities that enable elections are becoming increasingly accessible from and dependent upon networked technologies, 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 FCEB, SLTT, and critical infrastructure public cybersecurity posture
  - Understand how we 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

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC Classification Level:
UNCLASSIFIED
NCCIC
U.S. DEPARTMENT OF HOMELAND SECURITY

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)

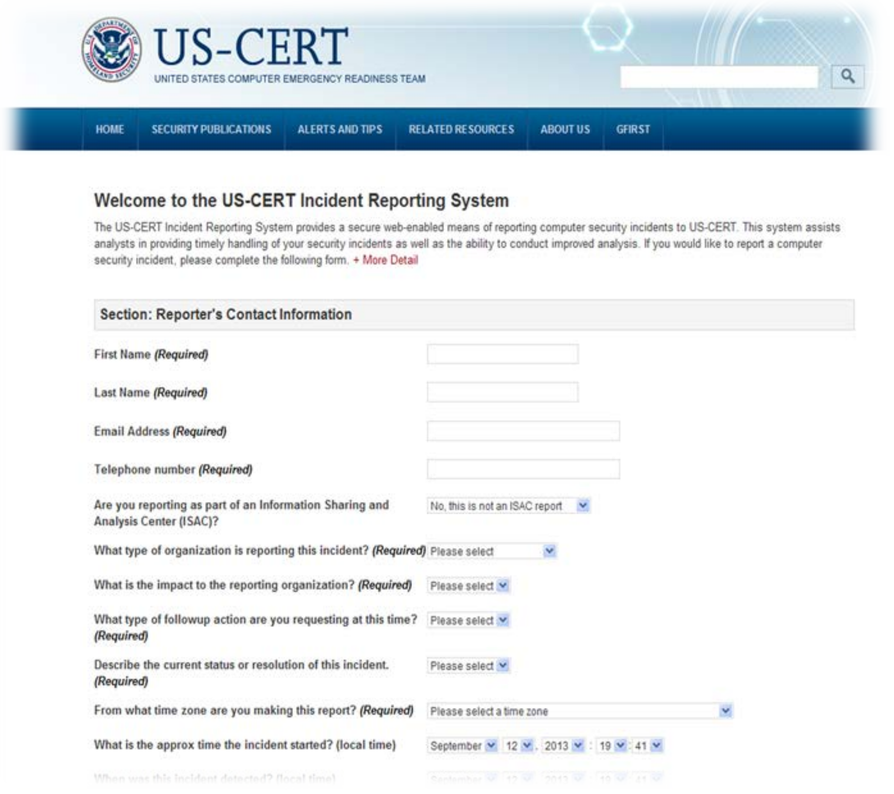
Reporting an Incident

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

MS-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:

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
- 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

Homeland Security

Q&A

SLTTCyber@hq.dhs.gov