Homeland Security

Cybersecurity: A National Asset and Homeland Security Priority

New York State Cyber Security Conference

June 2, 2015

Vikingdom Cyberattacks

- Vikingdom is a malicious hacking group that recently targeted private/public websites throughout the United States
- They published a list of 44 **.gov** websites which they targeted, including: Mass.gov, NYC.gov, Texas.gov, etc.
- In March of 2015, Vikingdom claimed to have attacked the State of Maine's government website 3 days in a row
  - One of the attacks targeted the Maine Department of Transportation, sending outdated road closures and construction alerts
  - The remaining intrusions were Distributed Denial-of-Service (DDoS) attacks aimed at the main government website

City of Longview Website Cyberattack

- In January of 2015, the City of Longview, TX experienced a Distributed Denial-of-Service (DDoS) cyberattack on its website
- In February, after continually experiencing similar DDoS attacks, the City of Longview decided to pull down the website indefinitely
- Longview Public Library services and online water bill payment services have also been discontinued as a precaution

South Carolina Department of Revenue's Cyber Theft

- In September of 2012, the State of South Carolina experienced a cyber-attack on its tax records
- The Nation's largest hacking of a state agency
- 6.4 million people and businesses compromised
- $25 million spent to address the breach over the first six months
  - $3 million contract awarded to evaluate State agencies' computer systems and offer recommendations
  - $12 million no-bid, emergency situation contract awarded for credit monitoring
  - $840,000 to plug the security hole left by the breach and determine the cause
- An additional $25 million dollars set aside for credit monitoring and cybersecurity improvements immediately following the breach

Office of Cybersecurity and Communications

"The cyber threat is one of the most serious economic and national security challenges we face as a Nation."

President Barack Obama, March 2010

Mission

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

National Cybersecurity and Communications Integration Center (NCCIC)

Report Types and National Cyber Awareness System Products

To sign up for US-CERT's National Cyber Awareness System products, visit:

- Mailing Lists & Feeds *(http://www.us-cert.gov/ncas)*

To receive the "Weekly Analytic Synopsis Product" or the "Cyber SnapShot" please contact *NCCIC@hq.dhs.gov*

- Advisories
- Alert & Situation Reports
- Analysis Reports
- Current Activity Updates
- Daily Summaries
- Indicator Bulletins
- Periodic Newsletters
- Recommended Practices
- Weekly Analytic Synopsis Product
- Weekly Digest
- Year in Review

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC Technical Assistance, Analysis and Reporting

- **U.S. Computer Emergency Readiness Team (US-CERT):** responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

- **Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT):** works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors.

- **National Cybersecurity Assessment & Technical Services (NCATS):** provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks.

National Cybersecurity and Communications Integration Center (NCCIC)

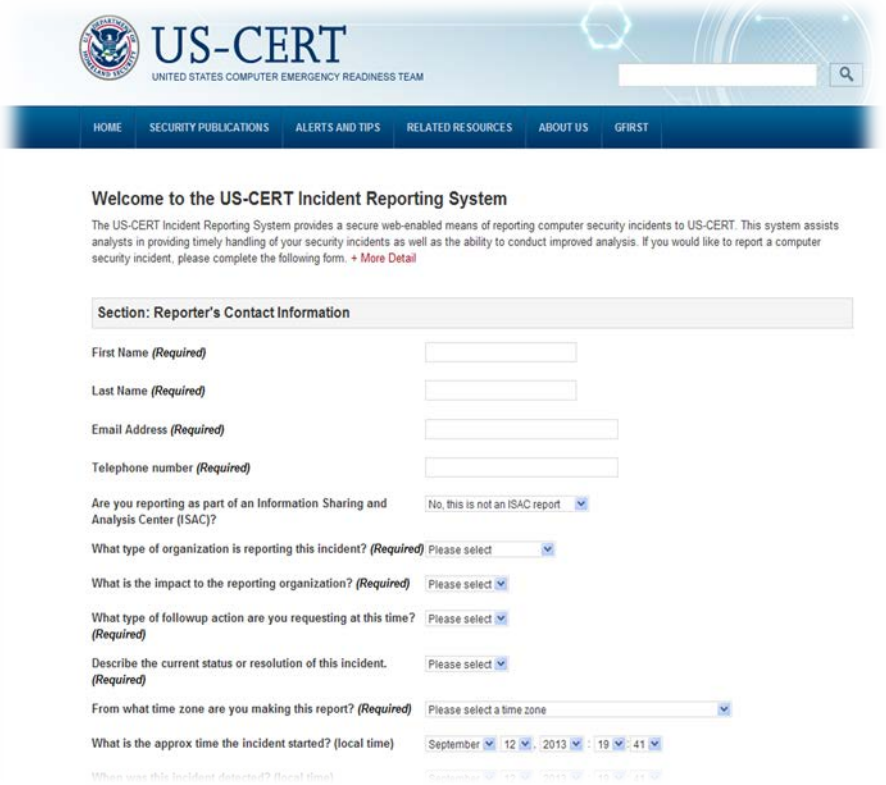
Reporting an Incident

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



The SLTT Cybersecurity Engagement Program

SLTT Mission

The mission of the SLTT Cybersecurity Engagement Program is to build trusted relationships with non-federal governments and associations to manage cyber risk. We lead and coordinate CS&C's efforts that motivate actions to protect SLTT cyber interests. We also provide Federal government products, resources and personnel to build partner capacity in an evolving threat environment.

Established Partnerships: MS-ISAC

CENTER FOR INTERNET SECURITY

MULTI-STATE Information Sharing & Analysis Center

Multi-State Information Sharing and Analysis Center

- Membership includes all 50 States, over 700 local government organizations, 3 U.S. territories and 8 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 managed security services to 29 States, 7 locals and 1 territory

Established Partnerships: MS-ISAC

How to Report a Suspected Incident:

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

The DHS National Cybersecurity and Communications Integration Center (NCCIC):

Call: (888) 282-0870

Email: NCCIC@hq.dhs.gov

When in doubt, please contact us.

Cybersecurity Resources

- C^{3}VP is the coordination point within the Federal Government to leverage and enhance existing capabilities and resources to promote the adoption of the **National Institute of Standards and Technology (NIST) Cybersecurity Framework**, a Risk-based approach to cybersecurity strategy and policy.
- The C^3 Voluntary Program website offers an overview of the program, downloadable tools, and outreach materials
  - Existing programs/resources have been aligned with the NIST Framework Core Function Areas (Identify, Protect, Detect, Respond, Recover)
    - Resources have been broken out by stakeholder type (Federal, State, local, tribal, and territorial (SLTT) government, Businesses)
    - This alignment demonstrates what DHS can offer to support the Framework's principles to reinforce cybersecurity risk management and resilience

For more information: www.us-cert.gov/ccubedvp

Cybersecurity Resources

Cybersecurity Assessments

Cyber Resilience Review

- Measures and enhances the implementation of key cyber security policies and capabilities of critical infrastructure entities

- Comprehensively assesses the overall practice, integration, and health of the organization's cyber security program

- Ensures that core process-based capabilities exist, are measureable, and are meaningful

- Identifies opportunities for improvement in cyber security management and reduce operational risks related to cyber security

Now available as a self-assessment

Cybersecurity Assessments

Nationwide Cybersecurity Review

- The NCSR is a voluntary self-assessment of State and Large Urban Area government IT services designed to measure cybersecurity preparedness and resilience
- DHS successfully completed the first NCSR in November 2011 and the summary report in March 2012
  - 49 States participated along with 2 U.S. territories
  - About 85% of all State CISOs participated in the inaugural review
- To develop and conduct the 2013 iteration, DHS partnered with the MS-ISAC and the National Association of State Chief Information Officers (NASCIO)
  - All 50 States, 93 Local Governments, 151 State Agencies, 8 Academia, 2 Tribal Governments (87% increase in participation from 2011)
- The 2014 iteration of the NCSR is the first to align to the NIST Cybersecurity Framework.
  - The 2015 NCSR question set is currently in development.
  - The 2014 iteration will inform efforts for the 2015 NCSR question set.

Cybersecurity Exercise Resources

National Cyber Exercise and Planning Program (NCEPP)

- The NCEPP team improves the Nation's cyber security readiness, protection, and incident response capabilities by developing, designing, and conducting scenario-based cyber exercises and workshops at the State, Federal, regional, and international level, focusing on risks to information technology infrastructure

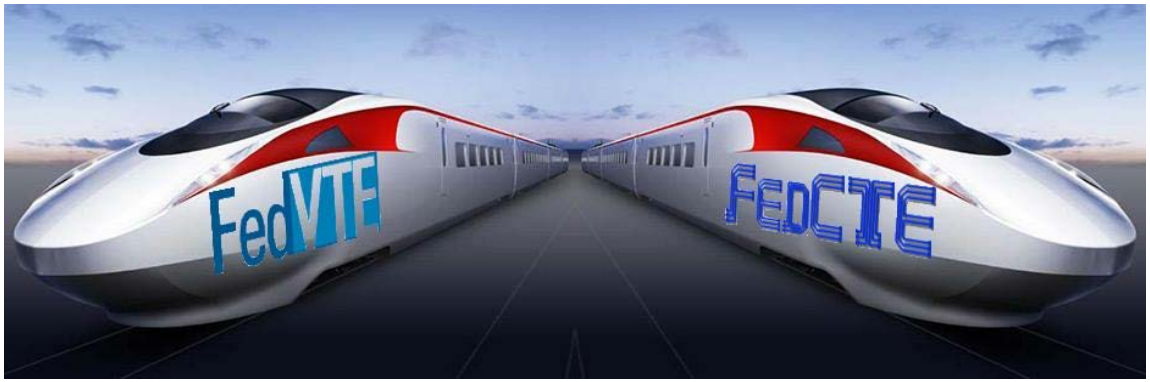
- Through exercises, participants are able to validate policies, plans, procedures, processes, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations (COOP)

- Developed an adaptable and scalable cyber tabletop exercise package (CTEP), allowing SLTT and private sector planners to produce high-quality, discussion-based cyber exercises that suit their needs

Cybersecurity Training Resources

Cyber professionals can continue to improve their skills through hands-on and virtual training opportunities.

- **Federal Virtual Training Environment (FedVTE)** – An online, on-demand training center that provides Federal cybersecurity and IT professionals with hands-on labs and training courses.
- **Federal Cybersecurity Training Events (FedCTE)** – Learning and networking opportunities at no cost for Federal cybersecurity and information technology (IT) professionals.



Cyber Education and Awareness

As part of the Cyberspace Policy Review, President Obama identified cybersecurity education and awareness as a key gap.

DHS leads the following activities that are filling this gap:

- Cyber Awareness Programs
- Formal Cybersecurity Education
- National Professionalization and Workforce Development Programs
- Training and Education Programs
- Strategic Partnerships

Cybersecurity Awareness

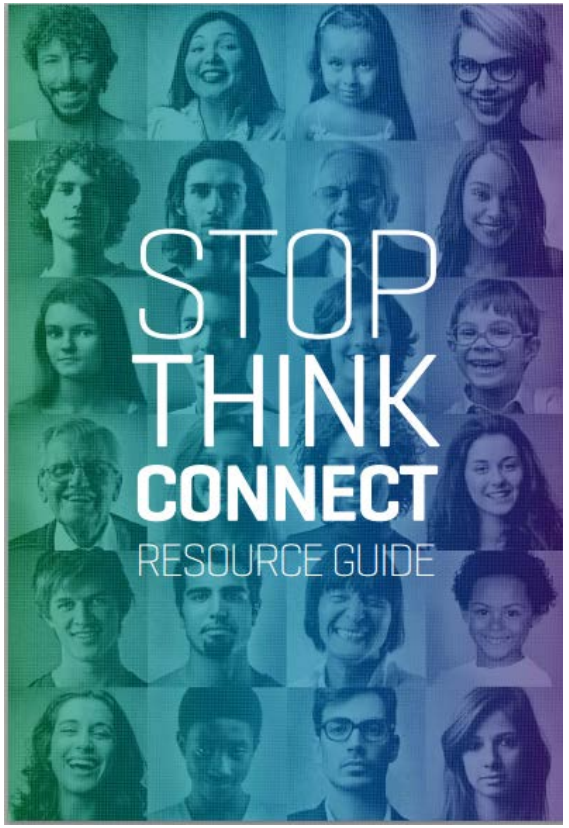
STOP | THINK | CONNECT®

- DHS launched the Stop.Think.Connect. campaign in October 2010 to inform the American people about how to use technology safely
- The Stop.Think.Connect. campaign has over 170 government, nonprofit, and academic partners and more than 200 industry partners working with the National Cyber Security Alliance.
- The campaign is a year-round national awareness and education effort among government, industry, nonprofits, academia and the American public

Stop.Think.Connect. Resources

The Stop.Think.Connect. Campaign provides a number of resources to the public, with toolkit materials designed for:

- Government
- Industry
- Law Enforcement
- Older Americans
- Parents and Teachers
- Students (K-8, 9-12 & undergraduate)
- Young Professionals



Download at:
www.dhs.gov/stopthinkconnect

National Cyber Security Awareness Month

National Cyber Security Awareness Month

Every October, DHS and its public and private sector partners celebrate National Cyber Security Awareness Month, an annual public awareness campaign that encourages Americans to become safer and more secure online.

STOP | THINK | CONNECT®

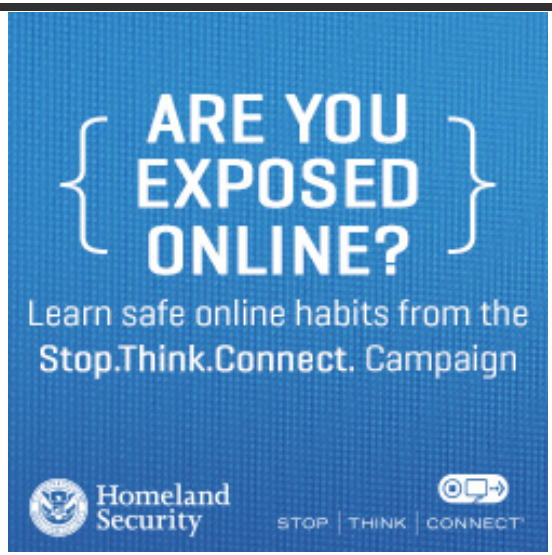
StaySafeOnline.org
National Cyber Security Alliance

MS-ISAC

Help Make the Internet Safer and More Secure

Become an advocate in your community to help educate and empower the American public to take steps to protect themselves and their families online.

- Link to DHS Stop.Think.Connect. resources
- Join the Campaign as a government, nonprofit, or academic partner organization; there are no fees or financial obligations
- Sign up as a *Friend* of the Campaign at www.dhs.gov/stopthinkconnect
- Share cybersecurity tips and resources on social media, newsletters, and during events
- Participate in National Cyber Security Awareness Month (October)



Thank You

Erin.Meehan@hq.dhs.gov