Federal Cybersecurity Programs

A Resource Guide

October 2014

National Governors Association

THE NATIONAL GOVERNORS ASSOCIATION (NGA), founded in 1908, is the collective voice of the nation's governors and one of Washington, D.C.'s, most respected public policy organizations. Its members are the governors of the 55 states, territories, and commonwealths. NGA provides governors and their senior staff members with services that range from representing states on Capitol Hill and before the Administration on key federal issues to developing and implementing innovative solutions to public policy challenges through the NGA Center for Best Practices. NGA also provides management and technical assistance to both new and incumbent governors.

THE NGA CENTER FOR BEST PRACTICES (NGA Center) is the only research and development firm that directly serves the nation's governors and their key policy staff. Governors rely on the NGA Center to provide tailored technical assistance for challenges facing their states, identify and share best practices from across the country, and host meetings of leading policymakers, program officials and scholars. Through research reports, policy analyses, cross-state learning labs, state grants, and other unique services, the NGA Center quickly informs governors what works, what does not, and what lessons can be learned from others grappling with similar issues.

For more information about NGA and the NGA Center, please visit www.nga.org.

LETTER FROM THE CO-CHAIRS

As co-chairs of the National Governors Association (NGA) Resource Center for State Cybersecurity (Resource Center), we have identified cybersecurity as one of the most significant and pervasive challenges facing states. We launched the Resource Center to equip governors with the tools they need to address this challenge.

Last fall, we released *Act and Adjust: A Call to Action for Governors for Cybersecurity*, which provides key recommendations governors can implement immediately to bolster their states' cybersecurity posture. In addition, the Resource Center identified other issues integral to state cybersecurity. One such issue is the need to improve coordination between the states and the federal government with respect to cybersecurity roles and resources.

In an effort to address this issue, the Resource Center worked with key federal agencies to create a document: *Federal Cybersecurity Programs: A Resource Guide*. Though not intended to serve as a comprehensive catalog, this document provides a summary of federal cyber programs that states can use to enhance their cybersecurity capabilities.

We hope you will disseminate this document to each of your associates and partners involved in the cybersecurity enterprise. By compiling the information in one document, we hope to facilitate greater information sharing between the states and federal government to improve cyber preparedness along with our private sector partners.

We look forward to working with you on this very important initiative.

Sincerely,

Governor Martin O'Malley
Maryland

Governor Rick Snyder
Michigan

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Governors Association (NGA) Center for Best Practices launched the Resource Center for State Cybersecurity (Resource Center) to provide resources, tools, and recommendations to governors across a spectrum of issues with the ultimate goal of improved state cybersecurity. The initiative is co-chaired by **Maryland** Gov. Martin O'Malley and **Michigan** Gov. Rick Snyder.

In the course of meetings with representatives from key state and federal agencies, as well as from private industry, the Resource Center identified a need for improving coordination between states and the federal government in terms of cybersecurity roles and resources. In an effort to address that need, the Resource Center worked with key federal agencies to compile this resource guide.

Federal Cybersecurity Programs: A Resource Guide is designed to be a high-level reference document for states that provides information on current federal programs and initiatives. It is not intended to be a comprehensive catalog of federal resources. Rather, it is meant to provide state officials with a summary of federal cyber programs that can assist them in enhancing their cybersecurity posture. The information in this resource guide was sourced primarily from the websites and public documents of the federal agencies mentioned within as well as from the agency representatives who vetted the document. This document has been reviewed by the respective federal agencies and the program descriptions reflect their views and not those of the National Governors Association.

This document is organized by the federal agencies currently working to produce the Presidential Policy Directive 21 and Executive Order 13636 deliverables or who have existing cyber-related programs that would be of interest to states. Programs that are promoted by the entire executive branch are cataloged under the White House section of the document. Certain programs are interagency by their very nature and each section should reflect that.

Each agency section summarizes the overall mission, goals, and priorities of an organization's cyber programs and provides detail on specific programs of interest to the states. Additionally, a number of program descriptions in the guide include contact information, and many program descriptions contain hyperlinks to the relevant federal Internet resource. Some referenced programs do not necessarily provide direct assistance to states; however, awareness of their existence can assist states in their cybersecurity preparedness.

This document contains a matrix that categorizes each federal program according to function. Those functions include training and exercise, operational support, frameworks, educational resources, information sharing, intelligence, and other resources. The matrix allows readers to quickly identify those programs that are of the most interest to them.

WHITE HOUSE

Summary

This section includes initiatives, presidential policy directives, and executive orders that provide the basis for many programs and initiatives discussed throughout this document. Special attention is paid to the 2013 Presidential Policy Directive 21 and Executive Order 136, which lifted cybersecurity to a national priority. The subsections provide general information and timelines for the deliverables.

WHITE HOUSE PROGRAMS AND INITIATIVES	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
The Comprehensive National Cybersecurity Initiative (CNCI)			●				
National Initiative for Cybersecurity Education (NICE)			●				
National Strategy for Information Sharing and Safeguarding (NSIS)			●		●		
National Strategy for Trusted Identities in Cyberspace (NSTIC)			●				
Presidential Policy Directive 21: Critical Infrastructure Security and Resilience			●				
Executive Order 13636: Improving Critical Infrastructure Cybersecurity			●				

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

The Comprehensive National Cybersecurity Initiative (CNCI)

In 2009, President Obama identified cybersecurity as one of the United States' most serious economic and national security vulnerabilities. He ordered a cyberspace policy review, and one of the recommendations to come from the review was to build on the Comprehensive National Cybersecurity Initiative (CNCI) launched in 2008 under President Bush.

The CNCI originally was conceived as a five-year project, but it has now become the building block for a broader, updated U.S. national cybersecurity strategy. The CNCI consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- Establishment of a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the federal government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce current vulnerabilities and prevent intrusions.

- Defense against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.

- Strengthening of the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the federal government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

National Initiative for Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE) evolved from the 2008 CNCI and has the goal of establishing an operational, sustainable, and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. NICE extends the scope of the CNCI initiative beyond the federal workplace to include civilians and students in kindergarten through postgraduate school.

NICE includes more than 20 federal departments and agencies. The National Institute of Standards and Technology (NIST) is leading the NICE initiative to ensure coordination, cooperation, focus, public engagement, technology transfer, and sustainability. Additional stakeholders involved in the initiative include state, local, tribal, and territorial (SLTT) governments, nonprofit organizations, academic institutions, professional associations, community groups, and the private sector.

NICE has four major components:

- **National Cybersecurity Awareness.** Lead agency: U.S. Department of Homeland Security;
- **Formal Cybersecurity Education.** Lead agencies: National Science Foundation and U.S. Department of Education;
- **Cybersecurity Workforce Structure.** Lead agencies: U.S. Department of Homeland Security and the Office of Personnel Management; and
- **Cybersecurity Workforce Training and Professional Development.** Lead agencies: U.S. Department of Homeland Security, U.S. Department of Defense, and the Office of the Director of National Intelligence.

Many NICE activities are already underway, and NIST will highlight these activities, engage various stakeholder groups, and create forums for sharing information and leveraging best practices. NIST will also be looking for gaps in the initiative—areas of the overarching mission that are not addressed by ongoing activities.

National Strategy for Information Sharing and Safeguarding (NSISS)

INFORMATION SHARING ENVIRONMENT (ISE)

The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004 to provide law enforcement, public safety, homeland security, intelligence, defense, and foreign affairs analysts, operators, and investigators from federal, state, local, tribal, and territorial governments with timely and accurate information to achieve their mission responsibilities.

NSISS

NSISS integrates the following ISE-related initiatives:

- Improvement of information sharing through a partnership with federal, state, local, tribal, and territorial entities to protect the homeland;
- Description of the federal government's approach to support state and major urban area fusion centers, as well as national efforts to fight crime and make our local communities safer; and

- Recognition that as information-sharing capabilities are enhanced, it is imperative that the legal rights of Americans continue to be protected.

The NSISS also identified the National Network of Fusion Centers and the National Information Exchange Model as current successes that will continue to enhance information-sharing efforts. (Both of these are described later in this document.)

The National Strategy for Trusted Identities in Cyberspace (NSTIC)

The National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative announced in 2011, charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions. The strategy's vision is: Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.

The realization of the NSTIC's vision requires the development of a vibrant, user-centric "identity ecosystem," an online environment where individuals and organizations will be able to trust each other because they follow agreed-upon standards to obtain and authenticate their digital identities and the digital identities of devices.

The Identity Ecosystem is designed to securely support transactions that range from anonymous to fully authenticated and from low to high value. As envisioned by the NSTIC, the identity ecosystem will increase the following:

- *Privacy protections* for individuals, who will be able trust that their personal data is handled fairly and transparently;
- *Convenience* for individuals, who may choose to manage fewer passwords or accounts than they do today;
- *Efficiency* for organizations, which will benefit from a reduction in paper-based and account management processes;
- *Ease of use*, by automating identity solutions whenever possible and basing them on technology that is simple to operate;
- *Security*, by making it more difficult for criminals to compromise online transactions;
- *Confidence* that digital identities are adequately protected, thereby promoting the use of online services;
- *Innovation*, by lowering the risk associated with sensitive services and by enabling service providers to develop or expand their online presence; and
- *Choice*, as service providers offer individuals different—yet interoperable—identity credentials and media.

ROLE OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS

Individuals interact with their state, local, tribal, and territorial governments as much or more than with the federal government. The identity ecosystem can help those governments decrease costs, even as they increase services offered to their constituents online. Much like the federal government, they are well-positioned to lead efforts to protect individuals, help standardize policies, and act as early adopters in the provision and consumption of identity ecosystem services. As such, state, local, tribal, and territorial governments are encouraged to align with the identity ecosystem framework and support its establishment by participating in its development.

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, which was issued by President Obama on 12 February 2013, outlines three strategic objectives that will drive the federal approach to strengthen critical infrastructure:

1. Refine and clarify functional relationships across the federal government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
2. Enable effective information exchange by identifying baseline data and systems requirements for the federal government; and
3. Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

Achieving these objectives is a shared responsibility among the federal, state, local, tribal, and territorial entities, as well as public and private critical infrastructure owners and operators. The intention is to develop a near real-time situational awareness capability of how the infrastructure is functioning, strengthen the public-private sector partnership, and develop a comprehensive research and development plan. In order to achieve the goals, Presidential Policy Directive 21 tasks the secretary of homeland security with accomplishing several objectives based on the timeline shown in the matrix below.

DATE	TASK
12 June 2013	Develop a description of the functional relationships within the U.S. Department of Homeland Security (DHS) and the federal government related to critical infrastructure security and resilience
12 July 2013	Evaluate the existing public-private partnership model and make recommendations for improving its effectiveness
11 August 2013	Identify baseline data and systems requirements for the federal government to enable efficient exchange of information
10 October 2013	Demonstrate a near real-time situational awareness capability for critical infrastructure
10 October 2013	Update the National Infrastructure Protection Plan (identification of a risk-management framework, methods used to prioritize critical infrastructure and synchronize communication within the federal government, metrics used to manage and reduce risks)
12 February 2015	Create a National Critical Infrastructure Security and Resilience research and development plan

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Executive Order 13636: Improving Critical Infrastructure Cybersecurity, issued by President Obama in 2013, identified cyber threats to critical infrastructure as a serious national security challenge and called for a strengthened public-private partnership to improve information sharing and establish a national set of standards for cyber risk management. The primary objectives outlined in Executive Order 13636 include the following:

- Developing a technology-neutral voluntary cybersecurity framework;
- Promoting and incentivizing the adoption of cybersecurity practices;
- Increasing the volume, timeliness, and quality of cyber-threat information sharing;
- Incorporating privacy and civil liberties protections into every initiative; and
- Exploring the use of existing regulation to promote cybersecurity.

The matrix below shows proposed timeline for specific tasks by various individuals and entities under Executive Order 13636.

DATE	TASK
12 June 2013	U.S. Attorney General, Secretary of Homeland Security, and Director of National Intelligence will ensure the timely production of unclassified reports of cyber threats that identify a specific targeted entity
12 June 2013	Secretary of Homeland Security and Secretary of Defense will establish procedures for a voluntary information sharing program that will expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors
12 June 2013	Secretary of Homeland Security and the Secretaries of the Treasury and Commerce will provide recommendations based upon analysis of the benefits and relative effectiveness of incentives and whether incentives require legislation or can be provided for under existing law
12 June 2013	Secretary of Defense and Administrator of General Services will make recommendations on the feasibility and merits of incorporating security standards into acquisition planning and contract administration
12 July 2013	Secretary of Homeland Security will use a risk-based approach and identify the critical infrastructure at greatest risk
10 October 2013	Director of the National Institute of Standards and Technology (NIST) will publish preliminary Cybersecurity Framework
8 January 2014	Agencies that regulate the security of critical infrastructure will submit a report that states whether or not the agency has clear authority to establish requirements based upon the preliminary Cybersecurity Framework
12 February 2014	U.S. Department of Homeland Security chief privacy officer and officer for civil rights and liberties will assess risks of the programs as stipulated in this order and make recommendations on ways to mitigate such risks in a publically available report
12 February 2014	Director of NIST, with coordination of Secretary of Homeland Security will publish the final Cybersecurity Framework
13 May 2014	If current regulatory requirements are deemed insufficient, agencies that regulate the security of critical infrastructure will propose prioritized, risk-based, efficient, and coordinated actions to mitigate cyber risk
February 2016	Agencies that regulate the security of critical infrastructure will report to the U.S. Office of Management and Budget on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements

A 150-Day Progress Report on the Implementation of Presidential Policy Directive 21 and Executive Order 13636

The U.S. Department of Homeland Security's (DHS) Integrated Task Force formed for the implementation of Executive Order 13636: Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, using a consultative process to engage stakeholders across the community, made significant progress during the first 150-day implementation period. On the basis of the efforts of the DHS Integrated Task Force, the Secretary of Homeland Security submitted the following Executive Order 13636 and Presidential Policy Directive 21 deliverables to the White House:

- An Incentives Report, which analyzes potential government incentives that could be used to promote the adoption of the Cybersecurity Framework;
- A description of critical infrastructure functional relationships, which illustrates the federal government's current organizational structure to deliver risk-management support to stakeholders and make it easier for them to collaborate with the government;
- Instructions on producing unclassified cyber threat reports from all-source information to improve the ability of critical infrastructure partners to prevent and respond to significant threats;
- Procedure for expansion of the Enhanced Cybersecurity Services (ECS) program to all critical infrastructure sectors;
- Recommendations on feasibility, security benefits, and merits of incorporating security standards into acquisition planning and contract administration, addressing what steps can be taken to make consistent existing procurement requirements related to cybersecurity;
- Identification of critical infrastructure, which would reasonably result in catastrophic consequences from a cybersecurity incident (the DHS evaluation identified a relatively small list of U.S. critical infrastructure that if impacted by a cybersecurity incident could reasonably affect our national security, economic security, public health, and safety);
- A process for expedited security clearances to those in the private sector, with an essential need to know for classified cybersecurity risk information (this processing is intended only for those who need access to classified information; for the most part, information sharing should and can be conducted at the unclassified level); and
- A report outlining how well the current critical infrastructure public-private partnership model as articulated in the National Infrastructure Protection Plan (NIPP) of 2013 is working toward promoting the security and resilience of the nation's critical infrastructure, and recommendations to strengthen those partnerships.

U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)

Summary

The U.S. Department of Homeland Security (DHS) coordinates the national protection, prevention, mitigation of, and recovery from cyber incidents; works to protect critical infrastructure; disseminates domestic cyber threat and vulnerability analyses across critical infrastructure sectors; secures federal civilian systems; and investigates, attributes, and disrupts cybercrimes under its jurisdiction.

For many states recovering from a cyber-incident or interested in vulnerability assessments and resources to bolster their current defenses, DHS will be the primary federal government point of contact. DHS-sponsored programs or initiatives that are geared specifically for state, local, tribal, and territorial (SLTT) governments and for private sector critical infrastructure owners/operators that reside within the state are identified in the matrix and discussed further below.

U.S. DEPARTMENT OF HOMELAND SECURITY	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
Cybersecurity framework and Critical Infrastructure Cyber Community (C3) Voluntary Program		●	●				
U.S. Secret Service	●	●			●		
U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI)	●	●			●	●	
State, Local, Tribal, and Territorial (SLTT) Cybersecurity Engagement Program	●	●	●		●		
Multi-State Information Sharing and Analysis Center	●	●			●	●	
State, Local, Tribal, and Territorial (SLTT) Security Clearance Initiative					●	●	
Cyber Resilience Review (CRR)	●	●					
Cybersecurity Evaluation Tool (CSET™)		●					
Continuous Diagnostics and Mitigation (CDM) Program	●	●			●	●	
Enhanced Cybersecurity Services (ECS)					●		
National Initiative for Cybersecurity Education (NICE)	●			●			●
National Centers of Academic Excellence (CAE)				●			
CyberCorps®: Scholarship for Service (SFS)				●			
Cybersecurity Education and Training Assistance Program-Integrated Cybersecurity Education Communities				●			

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

U.S. DEPARTMENT OF HOMELAND SECURITY	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
DHS Secretary's Honors Program				●			
Cyber Student Volunteer Initiative				●			
NIPP 2013: Partnering for Critical Infrastructure Security and Resilience	●		●		●		
Infrastructure Protection (IP) Gateway	●		●		●		

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

Cybersecurity framework and Critical Infrastructure Cyber Community (C3) Voluntary Program

As noted earlier, Executive Order 13636: Improving Critical Infrastructure Cybersecurity, issued by President Obama in 2013, identified cyber threats to critical infrastructure as a serious national security challenge and called for a strengthened public-private partnership to improve information sharing and establish a national set of standards for cyber risk management.

Executive Order 13636 directed the U.S. Department of Homeland Security (DHS) to launch the Critical Infrastructure Cyber Community, or C3 (pronounced "C-Cubed") Voluntary Program. The C^3 Voluntary Program was launched by DHS on February 12, 2014, in conjunction with the release of the final Cybersecurity Framework by the National Institute for Standards and Technology (NIST). The C^3 Voluntary Program is a public-private partnership connecting organizations, as well as federal, state, local, tribal, and territorial (SLTT) partners, to existing resources that will assist their efforts to use the Cybersecurity Framework to manage their cyber risks.

Currently, entities across DHS and the entire government offer many programs and resources to SLTT governments looking to improve their cyber-risk resilience. The C^3 Voluntary Program serves as a central point to access that information to leverage and enhance existing capabilities and resources to promote use of the Cybersecurity Framework.

Executive Order 13636 also called for the development of a voluntary, risk-based cybersecurity framework—a set of existing standards, guidelines, and practices to help organizations manage cyber risks (discussed further below). Cybersecurity framework organizations may need assistance in understanding the purpose of the cybersecurity framework and how it might apply to them. The C^3 Voluntary Program will provide assistance to organizations of all sizes interested in using the cybersecurity framework. More information on the C^3 Voluntary Program and associated resources can be found below and in full detail at **www.dhs.gov/ccubedvp** or **www.us-cert.gov/ccubedvp**.

For more information, contact:
CCubedVP@hq.dhs.gov

DHS Cybersecurity Programs and Resources by Component

U.S. SECRET SERVICE

The U.S. Secret Service has jurisdiction for investigation federal cyber crimes and also trains state and locals on cyber investigations.

- The Secret Service's Electronic Crimes Task Forces (ECTFs) have the mission of partnering with academia, the private sector, and state, local, and federal law enforcement for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

- The Secret Service's Cyber Intelligence Section has directly contributed to the arrest of transnational cyber criminals responsible for the theft of hundreds of millions of credit card numbers and the loss of approximately $600 million to financial and retail institutions.

- The Critical Systems Protection Program identifies, assesses, and mitigates risks posed by information systems to persons and facilities protected by the Secret Service.
  - > More than 800 unique computer networks across numerous critical infrastructure sectors have been assessed.

- The National Computer Forensic Institute, located in Hoover, Alabama, is the nation's only federally funded training center dedicated to instructing state and local officials in cyber-crime investigations.
  - > It is mandated to provide state and local law enforcement, legal, and judicial professionals a free, comprehensive education on current cybercrime trends, investigative method, and prosecutorial challenges.
  - > It has trained more than 1,800 state and local officials, including more than 1,250 police investigators, 430 prosecutors, and 140 judges from all 50 states and three U.S. territories.

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT'S (ICE) HOMELAND SECURITY INVESTIGATIONS (HSI)

U.S. Immigration and Customs Enforcement (ICE) is the principal investigative arm of the U.S. Department of Homeland Security (DHS). ICE's Homeland Security Investigations (HSI) investigates organized cyber crime involving suspected violations of a wide range of federal statutes. ICE-HSI's cyber investigations primarily focus on international cyber-facilitated economic crime, Internet-facilitated smuggling and money laundering, the illegal acquisition and proliferation of export controlled technology and data, the theft and sale of digital intellectual property, and child exploitation crimes.

The ICE-HSI Cyber Crimes Center (C3) manages ICE-HSI's cybercrime strategy and investigative programs. C3 utilizes state-of-the-art investigative techniques and digital forensic technology to conduct and support investigations, and provides subject matter expert advice and technical guidance on complex cybercrime investigations in the field.

NATIONAL PROTECTION & PROGRAMS DIRECTORATE (NPPD), OFFICE OF CYBERSECURITY AND COMMUNICATIONS, STATE, LOCAL, TRIBAL, AND TERRITORIAL (SLTT) CYBERSECURITY ENGAGEMENT PROGRAM

The State, Local, Tribal, and Territorial (SLTT) Cybersecurity Engagement Program of the Office of Cybersecurity and Communication, National Protection & Programs Directorate (NPPD) at the U.S. Department of Homeland Security (DHS) builds partnerships with non-federal public stakeholders including governors, mayors, state Homeland Security Advisors (HSAs), Chief Information Officers (CIOs), and Chief Information Security Officers (CISOs). Through the SLTT Cybersecurity Engagement Program, governors and other SLTT officials receive cybersecurity risk briefings and information on available resources, cybersecurity initiatives, and partnership opportunities with federal agencies.

For more information, contact:
SLTTCyber@hq.dhs.gov

MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER (MS-ISAC)

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a collaborative state, local, territorial, and tribal (SLTT) government-focused cybersecurity organization, bolstering SLTT capacity and network defense capabilities against cyber threats. The MS-ISAC provides a centralized forum for information sharing on cyber threats between the federal government and SLTT governing bodies through a number of crucial services, while providing opportunities to analyze and correlate information among SLTT members.

Funded by the U.S. Department of Homeland Security's (DHS) Cybersecurity & Communications (CS&C) Office, the MS-ISAC has been designated by DHS as the cybersecurity ISAC for SLTT governments. Operationally, the MS-ISAC remains an invaluable mechanism for cybersecurity coordination with SLTT governments and has been identified as a key stakeholder in the National Cyber Incident Response Plan (NCIRP).

Cyber incidents and related information reported by state, local, tribal, and territorial governments to the MS-ISAC will be shared out with DHS Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center (NCCIC) via liaison officers on the NCCIC floor. In this way, the SLTT perspective of the MS-ISAC contributes greatly to the NCCIC's overall situational awareness and comprehensive cyber-threat picture.

All MS-ISAC members receive base services, including situational awareness, early warning dissemination, trends and technical assistance through the MS-ISAC Security Operations Center (SOC), general cybersecurity outreach, awareness, and education and training. The MS-ISAC's Cyber SOC is a 24x7 operational center for SLTT governments. To expand its network intrusion detection and prevention, monitoring, and vulnerability scanning services across SLTT governments, the MS-ISAC developed the Managed Security Services (MSS) program.

Contact: info@msisac.org *or visit* www.msisac.org *for more information.*

THE SLTT SECURITY CLEARANCE INITIATIVE

The SLTT Security Clearance Initiative grants SECRET-level security clearances to State Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs). Clearances received through the SLTT Security Clearance Initiative will enable CIOs and CISOs to receive actionable and valuable classified and sensitive information about current and recent cyberattacks and threats, better informing their cybersecurity risk-management decisions. Cleared CIOs and CISOs can then take advantage of recurring classified briefings.

For more information, contact:
SLTTCyber@hq.dhs.gov

CYBER RESILIENCE REVIEW (CRR)

The DHS Office of Cybersecurity and Communications conducts voluntary, no-cost assessments to help evaluate and enhance cybersecurity capacities and capabilities within the critical infrastructure sectors and SLTT governments through its Cyber Resilience Review (CRR) process. The goal of the CRR is to understand and measure key cybersecurity capabilities and provide meaningful maturity indicators of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis.

For more information or to schedule a CRR, contact: CSE@hq.dhs.gov

THE CYBER SECURITY EVALUATION TOOL (CSET™)

The Cyber Security Evaluation Tool (CSET™) is a self-contained software tool that runs on a desktop or laptop. It evaluates the cybersecurity of an automated, industrial control, or business system using a hybrid risk and standards-based approach. CSET™ helps asset owners assess their information and operational systems' cybersecurity practices by asking a series of detailed questions about system components and architecture, as well as operational policies and procedures. Once the self-assessment questionnaire is complete, CSET™ provides a prioritized list of recommendations for increasing cybersecurity. The tool is available through the U.S. Computer Emergency Readiness Team (US-CERT).

CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) PROGRAM

In support of government efforts to provide adequate, risk-based, and cost-effective cybersecurity, DHS established the Continuous Diagnostics and Mitigation (CDM) Program, an implementation approach consistent with the Information Security Continuous Monitoring methodology. DHS, in partnership with the General Services Administration (GSA), established a government-wide acquisition vehicle (blanket purchase agreement) for continuous monitoring capabilities.

The purpose of the Continuous Monitoring as a Service (CMaaS) blanket purchase agreement, which is available to federal, state, local, and tribal government entities, is to do the following:

- Provide a consistent, government-wide set of continuous monitoring solutions to enhance the government's ability to identify and mitigate the impact of emerging cyber threats.

- Capitalize on strategic sourcing to minimize costs of continuous monitoring implementation.

State and local governments may leverage the CMaaS blanket purchase agreement to obtain discounted prices for tools, sensors, and services.

The CDM Program is in the process of awarding a contract to provide a commercial off-the-shelf (COTS) dashboard for federal government agencies. A subsequent contract with the awarded vendor will provide an opportunity for nonfederal agencies to obtain that dashboard. DHS will also provide online CDM training to state, local, tribal, and territorial (SLTT) partners in Fiscal Year 2015 to promote a broad understanding of CDM principles and approaches.

To participate in the CDM program, state and local governments can request the U.S. General Services Administration (GSA) ordering guide by emailing **cdm@gsa.gov**

ENHANCED CYBERSECURITY SERVICES (ECS)

Enhanced Cybersecurity Services (ECS) is a voluntary information-sharing program that assists critical infrastructure owners and operators as they improve the security and resilience of their systems against cyber threats (exploitation, data exfiltration) and unauthorized access. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS then develops indicators based on this information and shares them with qualified Commercial Service Providers (CSPs), thus enabling them to better protect their customers who are critical infrastructure entities. ECS augments, but does not replace, entities' existing cybersecurity capabilities. The ECS information-sharing process protects Critical Infrastructure entities against cyber threats that could otherwise harm their systems.

For more information about ECS: contact SLTTCyber@hq.dhs.gov

The National Initiative for Cybersecurity Education (NICE)

As noted earlier, the National Initiative for Cybersecurity Education (NICE) has evolved from the 2008 Comprehensive National Cybersecurity Initiative (CNCI) and extends its scope beyond the federal workplace to include civilians and students in kindergarten through post-graduate school. The goal of NICE is to establish an operational, sustainable, and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security.

- The National Initiative for Cybersecurity Careers and Studies (NICCS) page, http://niccs.us-cert.gov/, is a one-stop shop for all cybersecurity careers and studies information.

- October is National Cyber Security Awareness Month. The U.S. Department of Homeland Security (DHS), in tandem with key public and private partners, works to sponsor events and activities throughout the country and to disseminate Awareness Month key messages to state and local partners. Since 2009, all 50 governors have signed the proclamation recognizing October as National Cyber Security Awareness Month.

- The STOP.THINK.CONNECT.™ Campaign, a national cybersecurity awareness campaign aimed at raising awareness among the American public, partners with federal agencies and SLTT governments through the Cyber Awareness Coalition. Coalition members collaborate with the campaign on outreach efforts and are provided access to campaign materials, templates, resources, and tips to assist with promoting cybersecurity.

For more information: contact SLTTCyber@hq.dhs.gov

DHS Education and Workforce Development Initiatives Related to Cybersecurity

NATIONAL CENTERS OF ACADEMIC EXCELLENCE (CAE)

The Centers of Academic Excellence (CAE) program, which the U.S. Department of Homeland Security (DHS) co-leads with the National Security Agency (NSA), promotes information assurance education, training, and awareness nationwide. The CAE program awards CAE designation to academic institutions (that is, two-year, four-year, and graduate institution) providing educational excellence in fields related to information assurance and cybersecurity.

CYBERCORPS®: SCHOLARSHIP FOR SERVICE (SFS)

The Scholarship for Service (SFS) program provides scholarships to selected academic institutions, which distribute these scholarships to undergraduate and graduate students pursuing cybersecurity. Scholarship-recipient students agree to serve at a federal, state, or local government agency in a cybersecurity position for a period of time equivalent to the length of their scholarship. The U.S. Department of Homeland Security (DHS) co-sponsors SFS with the National Science Foundation (NSF).

For more information, contact: SFS@opm.gov

CYBERSECURITY EDUCATION AND TRAINING ASSISTANCE PROGRAM'S (CETAP) INTEGRATED CYBERSECURITY EDUCATION COMMUNITIES (ICEC)

The Cybersecurity Education and Training Assistance Program's (CETAP) Integrated Cybersecurity Education Communities (ICEC) project targets the U.S. high school student population through professional development of high school teachers and cybersecurity education summer camps. The project encourages innovation in education, increases awareness of cybersecurity roles, and provides teachers tools to teach their students about the availability of related career opportunities. CETAP-ICEC focuses its efforts on training teachers to use project-based learning when integrating cybersecurity content into math, science, and humanities studies.

DHS SECRETARY'S HONORS PROGRAM (SHS)

The Secretary's Honors Program at the U.S. Department of Homeland Security (DHS) is a new recruitment initiative for exceptional recent college graduates aimed at recruiting, retaining, and developing talented entry-level people to support DHS's missions, including cybersecurity.

- Information Technology Fellows: a one-year program designed for graduate-level recent graduates with computer science-related academic backgrounds and career paths who are interested in the operation and management of information technology (IT).

- Cyber Fellows: a two-year program for either bachelor or graduate-level recent graduates in computer science, computer or network engineering, or other information assurance/security/technology fields of study. Through rotational assignments, participants see how each DHS component collaborates on cyber-related issues such as identification and analysis of malicious code, forensics analysis, and intrusion detection and prevention.

CYBER STUDENT VOLUNTEER INITIATIVE

The DHS Secretary's Honors Program's Cyber Student Volunteer Initiative is an unpaid student volunteer program for college students pursuing a program of study in a cybersecurity-related field. Originally created in April 2013, the Cyber Student Volunteer Initiative expanded to new DHS offices and locations in 2014, with more than 100 unpaid student volunteer assignments available in over 60 locations across the country.

Offices and components in the Cyber Student Volunteer Initiative include U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) computer forensics labs, the U.S.

Secret Service, the U.S. Coast Guard, the Transportation Security Administration, the Office of Intelligence and Analysis, the DHS Office of the Chief Information Officer, and state and major urban area fusion centers. Student volunteers in the program gain invaluable hands-on experience and exposure to the work done by DHS cybersecurity professionals, and perform a broad range of duties in support of DHS's cybersecurity mission.

DHS Office of Infrastructure Protection's Cyber Resources for States

NATIONAL INFRASTRUCTURE PROTECTION PLAN 2013 (NIPP 2013)

As noted earlier, Executive Order 13636: Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, both issued by President Obama in 2013, highlighted the need to augment the focus on physical protective measures for critical infrastructure with additional emphasis on strengthening security and resilience across interrelated systems.

The National Infrastructure Protection Plan released by the Office of Infrastructure Protection at the U.S. Department of Homeland Security (DHS) in November 2013 (NIPP 2013) provides a framework that integrates a wide range of activities designed to manage critical infrastructure risk into a unified national effort. NIPP 2013 reflects the input and expertise of a wide range of critical infrastructure partners and stakeholders, including federal, state, local, tribal, and territorial governments; regional entities; private sector owners and operators; academic and nonprofit organizations; and the public. In addition, the 2013 NIPP is informed by changes in the risk, policy, and operating environments, as well as lessons learned from exercises and real-world events, such as cyber incidents and natural disasters like Superstorm Sandy.

Although NIPP 2013 retains the basic building blocks of NIPPs issued in 2006 and 2009, it also represents significant evolution in several areas. The NIPP 2013 is streamlined and provides the foundation for an integrated and collaborative approach to achieve the following vision:

A nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened

The 2013 NIPP, among other things, does the following:

- Integrates cyber and physical security and resilience efforts into an enterprise approach to risk management;
- Elevates security and resilience as the primary aim of Critical Infrastructure planning efforts;
- Calls for the establishment of national priorities—determined jointly by public and private sector partners—that will drive action at the national level and inform the development of goals and priorities at the sector, SLTT, and regional levels;
- Builds on and updates the risk-management framework introduced in the 2006 NIPP to streamline and clarify the steps of the framework and emphasize the role of information sharing throughout the risk-management process;
- Reinforces the importance of efficient information sharing, grounded in appropriate legal protections, trusted relationships, enabling technologies,

and consistent processes, to facilitate joint planning and risk management;

- Affirms that effective critical infrastructure security and resilience efforts require international collaboration and informed management of global supply chains;

- Incorporates practical lessons learned from national program implementation and feedback from partners; and

- Includes a detailed Call to Action, with steps that the CI community will undertake to make progress toward security and resilience.

INFRASTRUCTURE PROTECTION (IP) GATEWAY

The Office of Infrastructure Protection (IP) has been working on a single information technology (IT) platform to consolidate all the disparate information about critical infrastructure in a more efficient process.

The IP Gateway provides mission area capabilities to Protective Security Advisors (PSAs), Sector Specific Agents, DHS leadership, and the National Infrastructure Coordination Center.

As part of its development, IP launched a pilot program for state and local governments, which has since ended.

For Fiscal Year 2014, there is a planned expansion of the IP Gateway for 5,000 additional users (SLTT participants) and added functionality.

Stakeholders in the IP Gateway outside of DHS include the following:

- State, Local, Tribal, Territorial, Government Coordinating Council (SLTT-GCC): information searching, uploading, and sharing;

- State Fusion Centers and Emergency Operations Center: retrieve Critical Infrastructure information in support of their mission; and

- First responders (i.e., police departments): input and retrieve Critical Infrastructure information when responding to emergencies.

The IP Gateway does the following:

- Provides benefits to the users by enabling them to access all of its applications through single-sign on;

- Allows data to be shared between applications to further infrastructure protection efforts by those users; and

- Protects data entered by the users through role-based access, and Protected Critical Infrastructure Information (PCII) data-sharing rules.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Summary

Executive Order 13636: Improving Critical Infrastructure Cybersecurity, issued by President Obama in 2013, calls for the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce to lead the development of a baseline framework to reduce cyber risk to critical infrastructure (the "cybersecurity framework"). Executive Order 13636 specifies that the cybersecurity framework is to include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. To the fullest extent possible, it is to incorporate voluntary consensus standards and industry best practices to help organizations manage cyber risks.

The matrix below and discussion that follows highlights deliverables called for in the executive order that NIST has a role in providing, including the first version of the cybersecurity framework. Also presented below is information regarding NIST's Computer Security Division, including a sampling of standards that may be helpful for state organizations. The concluding part of this section focuses on the National Cybersecurity Center of Excellence (NCCoE) established in 2012 through a partnership among NIST, the State of Maryland, and Montgomery County (Maryland).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
The Cybersecurity Framework (to reduce cyber risk to Critical Infrastructure)			●				
NIST Timetable for Activities Related to the Cybersecurity Framework			●				
NIST Request for Information (RFI) Related to the Cybersecurity Framework			●				
Cybersecurity Framework, Version 1.0			●				
NIST Roadmap to the Cybersecurity Framework			●				
NIST's Computer Security Division Standards			●				●
National Cybersecurity Center of Excellence (NCCoE)		●		●			

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

The Cybersecurity Framework for Operators of Critical Infrastructure

To meet the requirements of Executive Order 13636, the voluntary, risk-based cybersecurity framework for operators of critical infrastructure must do the following:

- Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks;
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk;
- Identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations to enable technical innovation and account for organizational differences; and
- Include guidance for measuring the performance of an entity in implementing the cybersecurity framework.
- The following table shows NIST timetable for activities related to the cybersecurity framework.

DATE	ACTION/TASK RELATED TO THE CYBERSECURITY FRAMEWORK	INTENT
26 February 2013	NIST Issues Request for Information (RFI)	Engage cybersecurity framework stakeholders
3 April 2013	First Cybersecurity Framework Workshop in DC	Engage cybersecurity framework stakeholders
8 April 2013	Collect, Categorize, and Post RFI Responses	Organize information
15 May 2013	Analyze RFI Responses	Identify common practices/themes
29-31 May 2013	Second Cybersecurity Framework Workshop at Carnegie Mellon University	Identify common practices/themes
28 June 2013	Draft Outline of Preliminary Cybersecurity Framework	Identify cybersecurity framework elements
10-12 July 2013	Third Cybersecurity Framework Workshop at University of California San Diego	Identify Cybersecurity framework elements
11-13 September 2013	Fourth Cybersecurity Framework Workshop at University of Texas at Dallas	Prepare and publish preliminary cybersecurity framework
10 October 2013	Publish Preliminary Cybersecurity Framework	Prepare and publish preliminary cybersecurity framework
14-15 November 2013	Fifth Cybersecurity Framework Workshop at North Carolina State University	Engage cybersecurity framework stakeholders for feedback
12 February 2014	NIST Voluntary Cybersecurity Framework Rollout	Publish final cybersecurity framework
9-10 April 2014	Privacy Engineering Workshop	Engage cybersecurity and privacy stakeholders
15-16 September 2014	Second Privacy Engineering Workshop	Engage cybersecurity and privacy stakeholders
29-30 October 2014	Sixth Cybersecurity Framework Workshop	Gather input to help NIST understand stakeholder awareness of, and initial experiences with the framework.

Ongoing Engagement: Open public comment and review is encouraged and promoted throughout the process.

NIST REQUEST FOR INFORMATION (RFI) RELATED TO THE CYBERSECURITY FRAMEWORK

On February 26, 2013, following the call for a cybersecurity framework for operators of critical infrastructure as laid out in Executive Order 13636 and Presidential Policy Directive 21, the National Institute of Standards and Technology (NIST) issued a request for information (RFI). In its RFI, NIST requested that respondents focus on a few key critical infrastructure sectors (energy, telecommunications, etc.). To identify themes that recurred in the submitted responses, NIST conducted an initial analysis. NIST then grouped the submitted responses thematically on the basis of considerations the cybersecurity framework for operators of critical infrastructure must include, practices that have a wide utility across different sectors, and gaps where RFI responses failed to address the needs of the Executive Order 13636. The following table shows themes identified by RFI respondents and what areas require further information and discussion.

PRINCIPLES FOR THE CYBERSECURITY FRAMEWORK	COMMON POINTS	NEED FOR INFORMATION
● **Flexibility:** 'not one-size-fits-all,' adaptable, apply across multiple sectors with diverse stakeholder ● **Effect on global operations:** global/international reference for cybersecurity policymaking ● **Risk-management approaches:** encourage use of risk-based approaches over compliance-based ● **Leverage existing approaches, standards, and best practices:** operators should not have to manage overlapping or duplicative approaches, dual standards, and conflicting requirements	● **Senior management engagement:** need for engagement and accountability for cybersecurity to convey its importance to employees ● **Baseline security:** cyber hygiene, common practice ● **Understanding threat environment:** timely and actionable information, situational awareness ● **Business risk/ risk assessment:** evaluation of cyber risk holistically with other risk to pick among traditional strategies ● **Separation of business and operational systems:** single most referenced best practice (referred to as critical) ● **Models/ levels of maturity:** each sector/organization is approaching the threat from a different standpoint—best practices should define objective, not the procedures ● **Incident response:** needed to support 'response' section of framework ● **Cybersecurity workforce:** skilled workforce critical to meet needs	● **Metrics:** how to assure interoperability and scalability ● **Privacy/civil liberties:** legislation, regulation ● **Tools:** measure risk, monitoring, increased situational awareness ● **Dependencies:** organizations rely on other organizations in order to perform (critical functions, i.e., supply chain, information technology dependency) ● **Industry best practices** ● **Resiliency** ● **Critical infrastructure cybersecurity nomenclature:** need for clear definitions and consistency

CYBERSECURITY FRAMEWORK, VERSION 1.0

In February 2014, the National Institute of Standards and Technology (NIST) issued *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, created through public-private collaboration. The cybersecurity framework provides a structure that organizations, regulators, and customers can use to create, guide, assess, or improve comprehensive cybersecurity programs.

The cybersecurity framework document labeled "Version 1.0" is described as a living document that will need to be updated to keep pace with changes in technology, threats, and other factors, as well as to incorporate lessons learned from its use. Updates will ensure the framework meets the needs of critical infrastructure owners and operators in a dynamic and challenging environment.

The document provides a common language to address and manage cyber risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses. The cybersecurity framework allows organizations—regardless of size, degree of cyber risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.

Organizations can use the framework to determine their current level of cybersecurity, set goals for cybersecurity that are in sync with their business environment, and establish a plan for improving or maintaining their cybersecurity. The cybersecurity framework also offers a methodology to protect privacy and civil liberties to help organizations incorporate those protections into a comprehensive cybersecurity program.

The cybersecurity framework document is composed of three main parts:

- **Framework Core.** The Framework Core presents five functions—identify, protect, detect, respond, and recover—that taken together allow any organization to understand and shape its cybersecurity program.

- **Framework Implementation Tiers.** The Framework Implementation Tiers describe the degree to which an organization's cybersecurity risk management meets goals set out in the framework and "range from informal, reactive responses to agile and risk-informed."

- **Framework Profiles.** The Framework Profiles help organizations progress from a current level of cybersecurity sophistication to a target improved state that meets business needs.

NIST ROADMAP FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

The companion *Roadmap for Improving Critical Infrastructure Cybersecurity* discusses NIST's next steps with the cybersecurity framework and identifies key areas of development, alignment, and collaboration. These plans are based on input and feedback received from stakeholders through the cybersecurity framework development process, particularly on the "Areas for Improvement" section of the cybersecurity framework, which has been moved to this document. NIST will continue to serve as a convener and coordinator to work with industry and other government agencies to help organizations understand, use and improve the cybersecurity framework. This will include leading discussions of models for future governance of the framework, such as potential transfer to a nongovernment organization.

NIST Information Technology Laboratory's Computer Security Division: Computer Security Resource Center

The Computer Security Division of the NIST Information Technology Laboratory's issues Special Publication 800 series reports that describe the NIST Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. These reports are of general interest to the computer security community.

Several publications in the 800 series have been developed by NIST's Computer Security Division to further NIST's statutory responsibilities under the Federal Information Security Management Act (FISMA). NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. These publications may be used by nongovernmental organizations on a voluntary basis. While these resources were developed with a primarily federal focus, many of the guidelines and recommendations also apply to state organizations.

The resources identified below are a sampling of the special publications developed by the Computer Security Division of NIST's Information Technology Laboratory that may also be utilized by state organizations. NIST's Information Technology Laboratory's Computer Security Division is constantly updating these standards and has many draft publications available for public comment and review.

GUIDELINES FOR SECURING WIRELESS LOCAL AREA NETWORKS (WLANS)

SP 800-153 (February 2012)

The security of each wireless local-area network (WLAN) is heavily dependent on how well each WLAN component—including client devices, APs, and wireless switches—is secured throughout the WLAN lifecycle, from initial WLAN design and deployment through ongoing maintenance and monitoring. The purpose of this publication is to help organizations improve their WLAN security by providing recommendations for WLAN security configuration and monitoring.

CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS

SP 800-146 (May 2012)

This document reprises the NIST-established definition of cloud computing, describes cloud computing benefits and open issues, presents an overview of major classes of cloud technology, and provides guidelines and recommendations on how organizations should consider the relative opportunities and risks of cloud computing. To understand which part of the spectrum of cloud systems is most appropriate for a given need, an organization should consider deployment models, service models, economic considerations, operational characteristics, service level agreements, and security.

GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING

SP 800-144 (December 2011)

Cloud computing's most common characteristics include on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and displacement of data and services from inside to outside the organization. This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.

INFORMATION SECURITY CONTINUOUS MONITORING FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS

SP 800-137 (December 2011)

In designing the enterprise architecture and corresponding security architecture, an organization seeks to securely meet the information technology (IT) infrastructure needs of its governance structure, missions, and core business processes. Information security is a dynamic process that must be effectively and proactively managed for an organization to identify and respond to new vulnerabilities, evolving threats, and an organization's constantly changing enterprise architecture and operational environment. The Risk Management Framework (RMF) developed by NIST describes a disciplined and structured process that integrates information security and risk-management activities into the system development life cycle.

GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES IN THE ENTERPRISE

SP 800-124 Rev.1 (June 2013)

The purpose of this publication is to help organizations centrally manage the security of mobile devices. This publication provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their life cycles. The scope of this publication includes securing both organization-provided and personally owned (bring your own device, BYOD) mobile devices.

GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

SP 800-122 (April 2010)

This document provides guidelines for a risk-based approach to protecting the confidentiality of PII. The recommendations in this document are intended primarily for U.S. federal government agencies and those who conduct business on behalf of the agencies, but other organizations may find portions of the publication useful. Each organization may be subject to a different combination of laws, regulations, and other mandates related to protecting PII, so an organization‘s legal counsel and privacy officer should be consulted to determine the current obligations for PII protection.

USER'S GUIDE TO SECURING EXTERNAL DEVICES FOR TELEWORK AND REMOTE ACCESS

SP 800-114 (November 2007)

This publication provides recommendations for securing external devices used for telework and remote access. Many organizations limit the types of external devices that can be used for remote access and which resources they can use, such as permitting teleworker-owned laptops to access a limited set of resources and permitting all other external devices to access Web-based email only. If the telework device is not secured properly, it poses additional risk to not only the information that the teleworker accesses but also the organization's other systems and networks.

GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING FOR DESKTOPS AND LAPTOPS

SP 800-83 Rev.1 (July 2013)

Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. This publication provides recommendations for improving an organization's malware incident prevention measures. It also gives extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones.

NATIONAL CHECKLIST PROGRAM FOR IT PRODUCTS: GUIDELINES FOR CHECKLIST USERS AND DEVELOPERS

SP 800-70 Rev.2 (February 2011)

The use of well-written, standardized checklists tailored by each organization to meet particular security and operational requirements can markedly reduce the vulnerability exposure of IT products. NIST maintains the **National Checklist Repository**, a publicly available resource that helps organizations find the current, authoritative versions of security checklists and to determine which ones best meet their needs. For checklist users, this document makes recommendations for how they should select checklists from the NIST National Checklist Repository, evaluate and test checklists, and apply them to IT products.

COMPUTER SECURITY INCIDENT HANDLING GUIDE

SP 800-61 Rev.2 (August 2012)

This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS

SP 800-53 Rev.4 (April 2013)

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation from a diverse set of threats. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The catalog of security controls addresses security from both a functionality perspective and an assurance perspective.

GUIDE FOR ASSESSING THE SECURITY CONTROLS IN FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, BUILDING EFFECTIVE SECURITY ASSESSMENT PLANS

SP 800-53A Rev.1 (June 2010)

This document assists organizations in tailoring and supplementing the basic assessment procedures provided. The tailoring process gives organizations the flexibility needed to avoid assessment approaches that are unnecessarily complex or costly while simultaneously meeting the assessment requirements established by applying the fundamental concepts in the RMF. Supplementation decisions are left to the discretion of the organization in order to maximize flexibility in developing security assessment plans when applying the results of risk assessments in determining the extent, rigor, and level of intensity of the assessments.

BUILDING AN INFORMATION TECHNOLOGY SECURITY AWARENESS AND TRAINING PROGRAM

SP 800-50 (October 2003)

A strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. Failure to give attention to the area of security training puts an enterprise at great risk because security of agency resources is as much a human issue as it is a technology issue. The document identifies the four critical steps in the life cycle of an IT security awareness and training program: Awareness and Training Program Design, Awareness and Training Material Development, Program Implementation, and Post-Implementation.

GUIDE FOR CONDUCTING RISK ASSESSMENTS

SP 800-30 Rev.1 (September 2012)

The purpose of this document is to provide guidance for conducting risk assessments of federal information systems and organizations. Risk assessments, carried out at all three tiers in the risk-management hierarchy, are part of an overall risk-management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. In particular, this document provides guidance for carrying out each of the steps in the risk assessment process (that is, preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment) and how risk assessments and other organizational risk-management processes complement and inform each other. State, local, and tribal governments, as well as private sector organizations, are encouraged to consider using these guidelines, as appropriate.

COMPUTER SECURITY DIVISION'S 2012 ANNUAL REPORT

SP 800-165 (June 2013)

With the continued proliferation of information, the explosion of devices connecting to the expanding communication infrastructure and the evolving threat environment, the need for cybersecurity standards and best practices that address interoperability, usability and privacy continues to be critical for the nation.

The Computer Security Division (CSD) of NIST's Information Technology Laboratory is responsible for developing standards, guidelines, tests, and metrics for the protection of non-national security federal information and communication infrastructure. These standards, guidelines, tests, and metrics are also important resources for the private sector. In 2012, CSD aligned its resources to enable greater development and application of practical, innovative security technologies and methodologies, and to enhance the ability to address current and future computer and information security challenges in support of critical national and international priorities.

National Cybersecurity Center of Excellence (NCCoE)

The National Cybersecurity Center of Excellence (NCCoE), established in 2012 through a partnership among the National Institute of Standards and Technology (NIST), the State of Maryland, and Montgomery County (Maryland), is dedicated to furthering innovation through the rapid identification, integration and adoption of practical, standards-based cybersecurity solutions.

The NCCoE is part of NIST's **Information Technology Laboratory** and operates in close collaboration with the **Computer Security Division (CSD)** of NIST's Information Technology Laboratory. As a part of the NIST organization, NCCoE has access to a foundation of expertise, resources, relationships, and experience. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The NCCoE facilitates rapid, widespread adoption of secure technologies through practice guides, which include all of the material and information needed to deploy a reference design.

The NCCoE works on use cases, which are sector-specific cybersecurity problems, and building blocks, which address technology gaps affecting multiple sectors. Currently, NCCoE has projects in areas that include the following:

- Identity and access management;
- Situational awareness;
- Access rights management;
- IT asset management;
- Mobile device security;
- Trusted geolocation in the cloud;
- Software asset management; and
- Attribute-based access control.

U.S. DEPARTMENT OF JUSTICE (DOJ)

Summary

The U.S. Department of Justice (DOJ) has adopted a comprehensive approach to combating cyber threats. Its approach is built upon the full spectrum of its criminal and national security authorities, tools, and capabilities. DOJ investigates and prosecutes large-scale data breaches, transnational criminal cyber organizations, and hackers who deploy sophisticated tools to steal from and damage computer networks. It also seeks to detect, deter, and interdict cyber threats before they become actual incidents or criminal cases.

To achieve the U.S. government's cyber and information-sharing objectives, DOJ works in collaboration with the U.S. Department of Homeland Security (DHS) and other federal agencies, as well as with state, local, and tribal governments. DOJ programs and initiatives are identified in the matrix and discussion that follows

U.S. DEPARTMENT OF JUSTICE (DOJ)	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
Computer Crime and Intellectual Property Section (CCIPS)							●
National Security Cyber Specialist (NSCS) Network							●
FBI	●	●			●	●	
Cyber Task Forces (CTFs)					●		
Cyber Shield Alliance					●	●	
Regional Computer Forensics Laboratories	●	●			●		
InfraGard					●		
Internet Crime Complaint Center (IC3)					●		●
National Cyber Investigative Joint Task Force (NCIJTF)						●	

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

DOJ Cybersecurity Programs by Component

Components of U.S. Department of Justice (DOJ) cybersecurity programs discussed below are the following:

- DOJ's Criminal Division's (CRM) Computer Crime and Intellectual Property Section (CCIPS);
- DOJ's National Security Division (NSD);
- U.S. Attorneys' Offices (USAOs) (94 across the country); and
- The FBI (special attention is paid to the FBI, as many of its initiatives and programs are designed for state outreach).

DOJ'S CRIMINAL DIVISION'S (CRM) COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION (CCIPS)

The U.S. Department of Justice's (DOJ) Criminal Division (CRM) plays a principal role in DOJ's work against cybercrime. CRM's Computer Crime and Intellectual Property Section (CCIPS) is dedicated to ensuring that a cadre of prosecutors across the country is specially trained to investigate and prosecute high-tech crimes.

CCIPS trains the Assistant U.S. Attorneys who belong to the Computer Hacking and Intellectual Property (CHIP) Network (see below) and routinely provide them with legal advice and technological guidance in cybercrime cases. CCIPS attorneys also work with CHIP attorneys in U.S. Attorneys' Offices (USAOs) to build and prosecute criminal cases. CCIPS also lends its expertise in electronic surveillance laws to other agencies' cyber efforts. In addition, the Office of International Affairs within CRM serves as DOJ's central authority in international criminal matters, works with CCIPS and the USAOs where transnational criminal cases require electronic evidence or law enforcement assistance from abroad.

>> Computer Hacking and Intellectual Property (CHIP) Network

The Computer Hacking and Intellectual Property (CHIP) Network was jointly established by the Computer Crime and Intellectual Property Section (CCIPS) and U.S. Attorneys' Offices (USAOs). The CHIP Network ensures that over 200 prosecutors from USAOs and the litigating divisions of Main Justice are prepared to serve as trained experts and as their districts' legal counsel on matters relating to electronic evidence and cybercrimes and relevant substantive and procedural laws.

Each USAO has one or more designated prosecutors who belong to the CHIP Network that spans all of the 94 USAOs and focuses on investigating and prosecuting cyber and intellectual property cases. Prosecutors within the CHIP network receive training and resources that ensure they are prepared for the newest threats and conversant in the newest technological trends being exploited by criminals. The CHIP program also aids in the coordination of multidistrict prosecutions involving cyber threats.

DOJ'S NATIONAL SECURITY DIVISION (NSD)

DOJ's National Security Division (NSD) conducts and supports investigations and prosecutions of national security intrusions and attacks. In addition, it works closely with elements of the Intelligence Community on cyber issues. NSD attorneys collaborate with the U.S. Attorneys' Offices (USAOs) to identify viable options for disrupting cyber threats, provide leadership and guidance in investigations and prosecutions of national security cyber offenses, review and monitor foreign investments in U.S. companies whose businesses may involve cyber-related services and technologies, and work with other agencies to develop lawful policy options to counter cyber threats. NSD's prosecutors focus specifically on the cyber threats presented by nation state actors and terrorists, looking for opportunities to develop and preserve a criminal prosecution option and otherwise disrupt those threats.

>> *National Security Cyber Specialist (NSCS) Network*

The National Security Cyber Specialist (NSCS) Network specializes in legal tools and advice relating to national security cyber threats, and ensures that all cyber threats that potentially involve terrorists or nation-state actors, or which otherwise threaten national security, are handled in a coordinated manner to ensure effective investigations, prosecutions, and other disruptions. The NSCS Network connects cyber specialists in DOJ's National Security Division (NSD) and Computer Crime and Intellectual Property Section (CCIPS) with the Assistant U.S. Attorneys in each the 94 districts across the country who handle intrusion matters involving terrorists or nation-state actors.

NSCS attorneys often have specialized expertise gained from serving as their offices' CHIP prosecutors or representatives to their districts' Anti-Terrorism Advisory Council ("ATAC"). Like the ATAC, the NSCS Network ensures open communication and coordination across DOJ's Headquarters and Field components and other Departments and Agencies. Finally, NSCS attorneys, both in the field and at DOJ headquarters, often working with the FBI or InfraGard, conduct outreach to companies who may have been—or may become—victims of national security-related cyber intrusions to share useful information and discuss relevant legal issues. Through these engagements, the NSCS Network is able to educate companies on the NSCS mission, encourage voluntary reporting of cyber intrusions, and gain a better understanding of private sector cybersecurity concerns.

U.S. ATTORNEYS' OFFICES (USAOS)

The 94 U.S. Attorneys' Offices (USAOs) across the country play a vital role in DOJ's efforts to combat cyber-crime. The USAOs investigate and prosecute a wide range of offenses under the cyber threat umbrella, including computer crimes, such as hacking and intrusions, as well as trade secret theft, identity theft, and other threats generally termed "cyber-crime."

Each of the 94 USAOs has a designated computer hacking and intellectual property (CHIP) prosecutor who is specially trained to pursue intellectual property (IP) offenses and cyber-crime. CHIP attorneys have four major areas of responsibility, including: (1) prosecuting computer crime and IP offenses; (2) serving as the district's legal counsel on matters relating to those offenses, and the collection of electronic evidence; (3) training prosecutors and law enforcement personnel in the region; and (4) conducting public and industry outreach and awareness activities. CHIPs may work frequently with attorneys CCIPS, who specialize in enforcing the laws related to IP and cyber crime.

As stated above, in 2012 DOJ established the NSCS network to coordinate the response to cyber threats—including economic espionage and trade secret theft—being conducted by nation-state actors or in a manner that otherwise impacts national security. Each USAO has at least one representative to the NSCS network who provides technical and specialized assistance to his or her colleagues within the district and is a point of contact for NSD and CCIPS for information sharing and de-confliction purposes.

There is a growing belief within the USAO community—and DOJ as a whole—that the theft of trade secrets and other information from American businesses through computer intrusions and other means represent some of the most serious attacks on our country's economic national security. Ongoing coordination among the USAOs, NSCS network, CHIP network, the FBI, other investigative agencies, NSD, and CCIPS is critical to addressing this threat.

FEDERAL BUREAU OF INVESTIGATION (FBI)

The FBI plays an important role in addressing the broad range of threats to the nation's cybersecurity. The FBI has a unique dual responsibility: (1) to prevent harm to national security as a member of the intelligence community with domestic responsibilities, and (2) to investigate and enforce violations of numerous federal statutes. These roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises. The FBI's unified mission brings all lawful investigative techniques and legal tools together to combat these threats.

The FBI recognizes that cooperation between federal, state, local, tribal, and territorial (SLTT) government, private sector, and international partners is essential to meet this challenge. The FBI seeks to foster such cooperation through multiple efforts, including the following:

- The FBI operates **Cyber Task Forces (CTFs)** in all its field offices focused on cybersecurity threats, including national security and criminal operations. CTFs synchronize domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions. CTFs also facilitate access for SLTT partners to a broad range of FBI investigative, forensics, and training resources.

- The FBI's Cyber Shield Alliance provides extensive resources for SLTT law enforcement partners via the **Law Enforcement Enterprise Portal**, to access eGuardian as a way to report cyber incidents, to share intelligence, and to access federally-sponsored training.

- The FBI sponsors **Regional Computer Forensics Laboratories** staffed by local, state, and federal law enforcement personnel. 16 facilities located across the country include a full-service forensics laboratory and training center devoted to examining digital evidence in support of investigations (child pornography, terrorism, violent crime, economic espionage, among others).

- The FBI conducts outreach to the private sector in partnership with the U.S. Department of Homeland Security (DHS) and other federal agencies. The FBI supports InfraGard, a nonprofit organization that brings together stakeholders representing government, the private sector, law enforcement, academia, and concerned citizens in a public-private partnership effort to protect the nation's critical infrastructure. Each **InfraGard** chapter is geographically linked with an FBI field office, providing stakeholders access to experts from law enforcement, industry, academic institutions, and other federal, state, and local government agencies. InfraGard members have access to the organization's secure internal website and other resources.

- The FBI administers the **Internet Crime Complaint Center (IC3)**, which collects reports from private industry and citizens about online fraud schemes and provides a simple online tool for reporting complaints. The FBI seeks to partner with SLTT law enforcement agencies to investigate serious and/or widespread complaints made to IC3.

- The FBI hosts the **National Cyber Investigative Joint Task Force (NCIJTF)**, a 24x7 multi-agency national focal point with representation from intelligence, law enforcement, and military agencies to coordinate, integrate, and share information related to cyber threat investigations.

Other Resources

http://www.Stopfraud.gov: This website has resources that should help victims of fraud. The Department of Justice's Office for Victims of Crime worked with the Financial Fraud Enforcement Task Force to develop certain of these resources.

http://www.ovcttac.gov/identitytheft: This website includes links to resources, and it teaches victim service professionals and allied professionals knowledge and skills to more effectively serve victims of identity theft and assist with their financial and emotional recovery.

http://www.nw3c.org/training & **http://www.search.org/get-help/training/high-tech-crime-investigations/:** The Department of Justice Bureau of Justice Assistance uses its funds to sponsor classes in the area of cyber security. These classes are offered to state, local, tribal, and territorial (SLTT) law enforcement, prosecutors, correctional, and probation/parole officers. The dates, times, and locations of these classes are posted on the National White Collar Crime Center (NW3C) and SEARCH websites.

STATE AND MAJOR URBAN AREA FUSION CENTERS

Summary

Fusion centers in states and major urban areas, established in the wake of the 9/11 terrorist attacks, are focal points for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners. Fusion centers conduct analysis and facilitate information sharing, assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.

Fusion centers are an underused resource that can effectively address cyber threats with support from federal agencies such as the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ). The matrix and discussion in this section describe the National Network of Fusion Centers, the National Information Exchange Model (NIEM) launched in 2005, and DHS resources for fusion centers.

STATE AND MAJOR URBAN AREA FUSION CENTERS	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
National Network of Fusion Centers	●	●			●	●	
National Information Exchange Model (NIEM)			●				
DHS Resources for Fusion Centers	●				●	●	

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

The National Network of Fusion Centers

The National Network of Fusion Centers was created following the 9/11 terrorist attacks to close the gaps in information sharing between federal, state and local law enforcement and emergency responders. According to guidelines published by the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ): a fusion center is "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate and respond to criminal and terrorist activity." **The National Network of Fusion Centers consists of 78 fusion centers** across 49 states, 3 territories, and the District of Columbia.

State and major urban area fusion centers serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT), and private sector partners. These fusion centers are owned, operated, and staffed primarily by state and local entities, but they receive support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding. Fusion centers also may have representatives from DOJ or DHS entities, including but not limited to the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), etc. Moreover, the DHS Office of Intelligence and Analysis has deployed more than 90 personnel, including regional directors, intelligence officers, reports officers, and intelligence analysts and deployed the Homeland Secure Data Network (HSDN) to more than 60 fusion centers, which allows secret-level access to federally generated classified threat information.

The National Information Exchange Model (NIEM)

The National Information Exchange Model (NIEM) is a community-driven, standards-based approach to exchanging information with roots in state and local government. It first began with a group of 20 states that joined forces in a grassroots effort called the Global Justice Information Sharing Initiative to overcome the challenges of exchanging information across state and city government boundaries.

The U.S. Department of Justice (DOJ) and U.S. Department of Homeland Security (DHS) began collaborating and united key stakeholders from federal, state, local, and tribal governments to develop and deploy a national model for information sharing. In April 20005, the chief information officers of DHS and DOJ launched the NIEM. In October 2010, the U.S. Department of Health and Human Services joined as the third steward of the model.

Since 2005, there have been four releases of the NIEM model: 1.0 in 2006, 2.0 in 2007, and 2.1 in 2009, and 3.0 in the fall of 2013. Currently, all 50 states and 19 federal agencies are committed to using the NIEM at varying levels of maturity. NIEM facilitates the exchange of cybersecurity information (information on incidents, indicators, and other time-sensitive critical information) with relevant stakeholders through its Cyber Domain. The Cyber Domain (Community of Interest (COI) is a collaborative forum to address needs and standards in exchanging cybersecurity information. It meets regularly via teleconferences and shares information in the NIEM.gov Cyber collaboration zone.

DHS Resources for Fusion Centers

DHS FUSION CENTER LEADERS PROGRAM (FCLP)

The Fusion Center Leaders Program (FCLP) at the U.S. Department of Homeland Security (DHS) is a graduate-level program that examines key questions and issues facing fusion center leaders and their role in homeland security, public safety, and the Information Sharing Environment (ISE). The FCLP is a five-day intensive program designed for leaders of the recognized state and major urban area fusion centers held at the Naval Postgraduate School Center for Homeland Defense and Security campus in Monterey, California.

DHS CYBER ANALYSIS TRAINING COURSE

The DHS cyber-analysis training course will provide a baseline of the concept of cybersecurity, a general overview of technical basics, an in-depth discussion of threats and tactics, the resources and expertise that are currently available to support state and local partners, and a writing and analysis exercise. This course is designed for fusion center, intelligence, and state information security analysts. It is held at the U.S. Secret Service National Computer Forensics Institute in Hoover, Alabama, and is provided to participants at no cost.

U.S. DEPARTMENT OF ENERGY (DOE)

Summary

The U.S. Department of Energy (DOE) is a key partner in helping the U.S. Department of Homeland Security (DHS) meet goals related to infrastructure. DOE's Office of Electricity Delivery and Energy Reliability (OE) and the nonprofit regulatory authority the North American Electric Reliability Corporation (NERC) are primarily responsible for cybersecurity in the energy sector. NERC is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system in North America. Some program and initiatives that fall under these entities are identified in the matrix that follows and described further below.

U.S. DEPARTMENT OF ENERGY (DOE)	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
DOE's Office of Electricity Delivery and Energy Reliability (OE)							●
Cybersecurity for Energy Delivery Systems (CEDS) Program							●
Cybersecurity Risk Management Process (RMP) Guideline for the Electricity Subsector			●	●			
Cybersecurity Capability Maturity Model (C2M2)		●	●	●	●		
Federal Energy Regulatory Commission's (FERC) Office of Energy Infrastructure Security (OEIS)			●		●		
North American Electric Reliability Corporation (NERC)	●	●	●	●	●		

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

DOE's Office of Electricity Delivery and Energy Reliability (OE)

The U.S. Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE), which leads DOE's efforts to ensure a resilient, reliable, and flexible electricity system, has five divisions:

- **Advanced Grid Integration (AGI):** This division manages the smart grid investment projects and advances smart grid interoperability and cybersecurity through standards, information exchange, and initiatives that increase the efficiency and effectiveness of grid modernization investments;
- **Power Systems Engineering Research & Development:** This division accelerates discovery and innovation in electric transmission and distribution technologies and create "next generation" devices, software, tools, and techniques to help modernize the electric grid. Projects are planned and implemented in concert with partners from other federal programs; electric utilities; equipment manufacturers; regional, state, and local agencies; national laboratories; and universities;
- **Energy Infrastructure Modeling and Analysis (EIMA):** This division is focused on ensuring the reliability

and resiliency of the U.S. electric grid through robust analytical, modeling, and assessment capabilities to address energy issues of national importance;

- **National Electricity Delivery Division (NEDD):** This division leads DOE's efforts to provide technical assistance to states, regional entities, and tribes to help them develop and improve their programs, policies, and laws that will facilitate the development of reliable and affordable electricity infrastructure; and

- **Infrastructure Security and Energy Restoration (ISER):** This division leads efforts to secure the U.S. energy infrastructure against all hazards, reducing the impact of disruptive events, and responding to and facilitating recovery from energy disruptions, in collaboration with all levels of industry and State and local governments.

DOE's OE's Cybersecurity for Energy Delivery Systems (CEDS) Program

The Cybersecurity for Energy Delivery Systems (CEDS) Program of the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (OE) assists energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.

In 2011, the CEDS program released *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, which identifies five project areas:

- **Build a culture of security.** Through extensive training, education, and communication, cybersecurity "best practices" are encouraged to be reflexive and expected among all stakeholders;

- **Assess and monitor risk.** Develop tools to assist stakeholders in assessing their security posture to enable them to accelerate their ability to mitigate potential risks;

- **Develop and implement new protective measures to reduce risk.** Through rigorous research, development, and testing, system vulnerabilities are revealed and mitigation options are identified which has led to hardened control systems;

- **Manage incidents.** Facilitate tools for stakeholders to improve cyber intrusion detection, remediation, recovery, and restoration capabilities; and

- **Sustain security improvements.** Through active partnerships, stakeholders are engaged and collaborative efforts and critical security information sharing is occurring.

OE continues to offer grants through the CEDS program, most recently in February 2013.

Cybersecurity Risk Management Process (RMP) Guideline for the Electricity Sector Developed by DOE, NIST, and FERC

A cybersecurity Risk Management Process (RMP) guideline for the electricity subsector was developed by the U.S. Department of Energy (DOE), in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC). Members of industry and utility-specific trade groups were included in authoring the RMP guideline so that it would be meaningful and tailored for the electricity subsector.

The electricity subsector cybersecurity RMP guideline is intended to be used by entities responsible for the generation, transmission, distribution, and marketing of electric power, as well as by supporting organizations to such entities (e.g., vendors). It is written to enable organizations (regardless of size or organizational structure) to apply effective and efficient risk management processes and tailor them to meet their organizational requirements. The guideline may be used to implement a new cybersecurity program within an organization or to build upon an organization's existing internal cybersecurity policies, standard guidelines, and procedures.

NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and System View, published in 2011, provided the foundational methodology for the electricity subsector cybersecurity RMP guideline.

The Cybersecurity Capability Maturity Model (C2M2)

The Cybersecurity Capability Maturity Model (C2M2) was originally developed in 2012 as part of a White House initiative led by the U.S. Department of Energy (DOE) in partnership with the U.S. Department of Homeland Security (DHS) and involving close collaboration with industry, other federal agencies, and other stakeholders.

The C2M2 model allows energy delivery system owners and operators assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity. It combines elements from existing cybersecurity efforts into a common tool that can be used consistently across the industry.

Version 1.0 of C2M2, released in 2012, pertained only to the electricity subsector. The C2M2 model was updated in February 2014 to include oil and natural gas subsector organizations, as well as sectors that overlap with energy or have responsibilities in other sectors entirely.

Federal Energy Regulatory Commission (FERC)'s Office of Energy Infrastructure Security (OEIS)

The Federal Energy Regulatory Commission (FERC) is an independent government agency, officially organized as part of the U.S. Department of Energy (DOE). FERC's Office of Energy Infrastructure Security (OEIS), created in September 2012, provides leadership, expertise, and assistance to FERC to identify, communicate, and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyber attacks and physical threats such as electromagnetic pulses.

FERC's OEIS is also tasked with providing assistance, expertise and advice to other federal and state agencies, jurisdictional utilities and Congress in identifying, communicating and mitigating potential cyber and physical threats and vulnerabilities to FERC-jurisdictional energy facilities and participating in interagency and intelligence-related coordination and collaboration efforts with appropriate federal and state agencies and industry representatives on cyber and physical security matters related to FERC-jurisdictional energy facilities.

North American Electric Reliability Corporation (NERC)

Acting under authority granted by the 2005 Energy Policy Act, FERC designated the

North American Electric Reliability Corporation (NERC) as the “Electric Reliability Organization” tasked with developing mandatory and enforceable reliability standards for the wholesale transmission system.

- NERC’s reliability standards include 10 Critical Infrastructure Protection (CIP) standards that touch on ensuring cybersecurity for transmission assets and operations.

- FERC’s Office of Electric Reliability oversees the development and review of mandatory reliability and security standards and ensures compliance with the approved mandatory standardsbytheusers,owners,andoperators of the bulk power system.

- FERC’s Office of Electric Reliability may coordinate with the applicable federal agencies; other governments; state agencies and regulators including the National Association of Regulatory Utility Commissioners (NARUC); the Electric Reliability Organization and Regional Entities (RE); the Independent System Operator (ISO)/Regional Transmission Organizations (RTOs); users, owners and operators of the bulk power system; stakeholders; customers; etc. to facilitate energy reliability and security.

- NERC’s Critical Infrastructure Protection Committee (CIPC) was formed to help NERC advance the physical security and cybersecurity of the critical electricity infrastructure of North America. CIPC consists of both NERC–appointed regional representatives and technical subject matter experts.

U.S. DEPARTMENT OF DEFENSE (DOD)

Summary

The role of the U.S. Department of Defense (DoD) in cybersecurity is primarily to protect military networks and defending the nation against cyber attacks beyond its borders, from both nation state and nonstate actors. Statutory restrictions on domestic military operations and a defined mission space for supporting military-related cybersecurity requirements limit DoD's ability to support states in this area. The U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) have been designated as key agencies for coordinating with states on cybersecurity.

Through the Council of Governors,[1] (Council), the National Governors Association (NGA) and governors are working to broker relationships with DoD and further explore how, when, and what DoD resources may be brought to bear in support of both federal and state cybersecurity needs. The Council is working with DoD and the National Guard Bureau to identify opportunities, legal barriers, and resource requirements to enhance the National Guard's ability to assist state government, critical infrastructure owners and operators, and local businesses with cybersecurity.

U.S. DEPARTMENT OF DEFENSE (DOD)	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
Components Responsible for Cybersecurity						●	
Role of National Guard in Defending Domestic Networks	●	●					

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

[1] Created in statute (National Defense Authorization Act for FY 2008) and formally established by Presidential Executive Order 13528, issued on January 11, 2010, the Council of Governors (Council) serves as a mechanism for governors and key federal officials to address matters pertaining to the National Guard, homeland defense, and defense support to civil authorities. The Council consists of 10 governors appointed by the President—five from each party—with two governors serving as co-chairs. Executive Order 13528 specifically names a number of federal participants in the Council, including the Secretaries of Defense and Homeland Security, the President's Homeland Security and Counterterrorism Advisor, the Commander of U.S. Northern Command, and the Chief of the National Guard Bureau, among others.

DoD Components Responsible for Cybersecurity in Support of National Defense

The components of the U.S. Department of Defense (DOD) responsible for cybersecurity in support of national defense are the following:

- U.S. Cyber Command;
- Army Cyber Command;
- Navy Cyber Forces; and
- Air Forces Cyber 24th Air Force.

Role of National Guard in Defending Domestic Networks

The National Guard currently supports DoD cybersecurity missions (mostly in support of federal Title 10 military activities), and their capability is growing. The National Guard currently has dedicated cyber units in several states, and many of these units are now actively engaging with their home state to support state cybersecurity needs through their State Active Duty authorities.

The Council of Governors is working with DoD and the National Guard Bureau to promote a more active role for the National Guard and ensure future investment in cyber capabilities can support both federal Title 10 and State Active Duty cybersecurity missions. Several states are already actively utilizing National Guard personnel in a number of cybersecurity support roles under their State Active Duty status, including the following:

- Engaging with their respective governor's office, state emergency management agencies, state chief information officers, public utilities and other state, local and federal officials in the development of state cyber incident response plans and cyber-resiliency planning;

- Participating with state and national-level cyber planning, training and exercises such as Cyber Guard and the National Level Exercise, which are evaluating the level of capability and coordination between state agencies, National Guard units and law enforcement at all levels of government during cyber attacks on state critical infrastructure;

- Performing limited cybersecurity support missions such as vulnerability assessments, standards compliance evaluation, incident planning and response, and threat analysis, for other state agencies under State Active Duty status (as directed by the governor);

- Participating in state-led evaluations of critical infrastructure and key resource assets and provides subsequent vulnerability assessments; and

- Co-locating in the state fusion center which facilities a dual-support role for National Guard cyber units including collaborative education efforts, tabletop exercises, and strategic planning.

NATIONAL SECURITY AGENCY (NSA)

Summary

The National Security Agency (NSA) is a U.S. intelligence agency devoted to analyzing electronic communications to identify and defend against threats to crucial networks. The NSA is focused on global threats to the security of the United States, as well as offensive and defensive responses. In addition, the NSA has several education programs that may be of interest to states as they work to succeed in educating and training a skilled cyber workforce.

NATIONAL SECURITY AGENCY (NSA)	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
National Information Assurance Education and Training Program				●			
NSA/DHS National Centers for Academic Excellence in Information Assurance Education				●			
NSA Education Opportunities				●			

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

National Information Assurance Education and Training Program (NIETP)

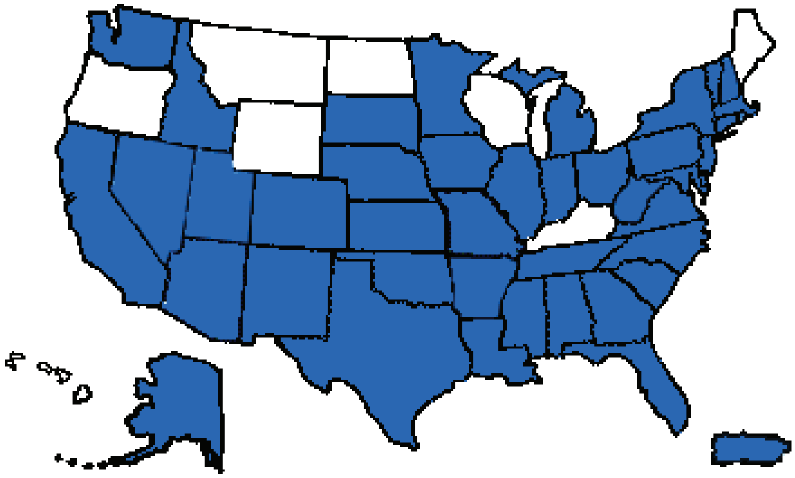
NSA and the U.S. Department of Homeland Security (DHS) jointly sponsor? the National Information Assurance Education and Training Program (NIETP). NIETP operates under national authority as the national manager for Information Assurance (IA) education and training relating to national security systems. NIETP programs prepare professionals entrusted with securing our critical information.

NSA/DHS National Centers for Academic Excellence (CAE) in Information Assurance Education (IAE)

- NSA and DHS jointly sponsor the National Centers of Academic Excellence (CAE) in Information Assurance Education (IAE), IA 2-year Education and Training (CAE/2Y) and IA Research (CAE/R) programs.

- The goal of these CAE in IAE is to reduce vulnerability in our national information infrastructure by promoting higher education and research in Information Assurance (IA) in support of the goals of the National Initiative for Cybersecurity Education (NICE).

- The following figure shows which states sponsor CAE in IAE as of 2013:



SOURCE: http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml#pr

- Information Assurance Education List by State

- Information Assurance Research List by State

- Cyber Operations: Four new National Centers of Academic Excellence (CAE) in Cyber Operations for academic years 2013–2018: Air Force Institute of Technology (AFIT), Ohio; Auburn University, Alabama; Carnegie Mellon University, Pennsylvania; Mississippi State University, Mississippi. In addition to these four institutions, there are centers at: Dakota State University, South Dakota; Naval Postgraduate School, California; Northeastern University, Massachusetts; and University of Tulsa, Oklahoma.

NSA Education Opportunities

There are several initiatives sponsored by the NSA to help promote math and science education at the elementary, middle, and high school levels.

- Mathematics Education Partnership Program
- Partners in Education Program

UNDERGRADUATE

- Cooperative Education Program
  > Designed for Computer Engineering or Computer Science majors
- Scholarships
  > SMART (Science, Mathematics, and Research for Transformation) Program
  > Information Assurance Scholarship Program (IASP)

- Internships
  > Computer Science Intern Program (CSIP)
  > Cryptanalysis and Exploitation Services Summer Program (CES SP)
  > Cyber Summer Program (CSP)
  > Semester Intern Program for Science and Technology (SIP/ST)
  > Summer Intern Program for Information Assurance (SIP/IA)

GRADUATE

- Scholarships
  > SMART (Science, Mathematics, and Research for Transformation) Program

- Internships
  > Computer Science Intern Program (CSIP)
  > Cyber Summer Program (CSP)
  > Summer Intern Program for Information Assurance (SIP/IA).

NATIONAL SCIENCE FOUNDATION (NSF)

Summary

The National Science Foundation (NSF) is devoted to promoting the progress of science. NSF is the funding source for approximately 20 percent of federally supported research conducted by U.S. colleges and universities. In supporting national defense objectives, NSF has made cyber research a priority.

This section primarily explores the undergraduate and graduate science, technology, engineering, and math (STEM)-related opportunities that NSF provides. Through programs such as the Secure and Trustworthy Cyberspace (SaTC) program and the CyberCorps®: Scholarship for Service (SFS) program, NSF seeks to address cybersecurity education and workforce development at the state, local, territorial, tribal (SLTT), and federal government levels.

NATIONAL SCIENCE FOUNDATION	FUNCTION*						
	TE	OS	F	ED	IS	INT	O
Secure and Trustworthy Cyberspace Program				●			
CyberCorps®: Scholarships for Service				●			

*KEY: TE = Training and exercises; OS = Operational support; F = Frameworks; ED = Educational resources; IS = Information sharing; I = Intelligence; O = Other resources

Secure and Trustworthy Cyberspace (SaTC) Program

In December 2011, the National Science and Technology Council (NSTC) with the cooperation of NSF issued a broad, coordinated Federal strategic plan for cybersecurity research and development to "change the game," minimize the misuses of cyber technology, bolster education and training in cybersecurity, establish a science of cybersecurity, and transition promising cybersecurity research into practice. This challenge requires a dedicated approach to research, development, and education that leverages the disciplines of mathematics and statistics, the social sciences, and engineering together with the computing, communications and information sciences.

The Secure and Trustworthy Cyberspace (SaTC) program welcomes proposals that address Cybersecurity from a Trustworthy Computing Systems (TWC) perspective and/or a Social, Behavioral and Economic Sciences (SBE) perspective, or from the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) perspective. In addition, the SaTC program seeks proposals focusing entirely on Cybersecurity Education with total budgets limited to $300,000 and durations of up to two years.

CyberCorps®: Scholarship for Service (SFS)

Through the CyberCorps®: Scholarships for Service (SFS) program, NSF provides educational opportunities for undergraduate and graduate students. The SFS program supports institutions that may provide support to individuals at those institutions. It has two tracks:

The SFS program's *Scholarship Track* provides funding to award scholarships to students in cybersecurity. In return for their scholarships, recipients will work after graduation for a federal, state, local, or tribal (SLTT) government organization in a position related to cybersecurity for a period equal to the length of the scholarship.

The SFS program's *Capacity Track* seeks innovative proposals leading to an increase in the ability of the United States higher education enterprise to produce cybersecurity professionals.

ACKNOWLEDGMENTS

This paper was written by Laura Saporito and Timothy Blute of the National Governors Association Center for Best Practices. The authors would like to thank a number of individuals whose input and comments were essential to the writing of this guide: David Behen, State of Michigan; Elliot Schlanger, State of Maryland; Cheri Caddy, National Security Council; Alaina Clark, Department of Homeland Security; Dan Lohrmann, Security Mentor, Inc.; Kiran Raj, Department of Justice; Adam Sedgwick, National Institute of Standards and Technology; Dana Thompson, Maryland Governor's Office; Carissa Vandermey, Department of Energy; and Sandra Waldstein, Federal Energy Regulatory Commission.

Support for the NGA Resource Center for State Cybersecurity comes from the American Gas Association, Citigroup, Deloitte, Edison Electric Institute, FireEye, Hewlett-Packard, IBM, Intuit, Nuclear Energy Institute, and Symantec.

NGA CENTER DIVISIONS

The NGA Center is organized into five divisions with some collaborative projects across all divisions. The NGA Center provides information, research, policy analysis, technical assistance and resource development for governors and their staff across a range of policy issues.

- **Economic, Human Services & Workforce** covers workforce development focused on industry-based strategies; pathways to employment and populations with special needs; and human services for children, youth, low-income families and people with disabilities.

- **Education** focuses on helping governors develop effective policy and support its implementation in the areas of early education, readiness, and quality; the Common Core State Standards, Science Technology Engineering and Math, and related assessments; teacher and leader effectiveness; competency-based learning; charter schools; data and accountability; and postsecondary (higher education and workforce training) access, success, productivity, accountability, and affordability. The division also works on policy issues related to bridging the system divides among the early childhood, K-12, postsecondary and workforce systems.

- **Environment, Energy & Transportation** focuses on several issues, including improving energy efficiency, enhancing the use of both traditional and alternative fuels for electricity and transportation, developing a modern electricity grid, expanding economic development opportunities in the energy sector, protecting and cleaning up the environment, exploring innovative financing mechanisms for energy and infrastructure, and developing a transportation system that safely and efficiently moves people and goods.

- **Health** covers issues in the areas of health care service delivery and reform, including payment reform, health workforce planning, quality improvement, and public health and behavioral health integration within the medical delivery system. Other focus areas include Medicaid cost containment, state employee and retiree health benefits, maternal and child health, prescription drug abuse prevention, and health insurance exchange planning.

- **Homeland Security & Public Safety** focuses on emerging policy trends across a range of homeland security and public safety issues. Current issues include cybersecurity, prescription drug abuse, public safety broadband, sentencing and corrections reform, homeland security grant reform, justice information-sharing, and public health preparedness.

National Governors Association

444 North Capitol Street, Suite 267
Washington, D.C. 20001
202-624-5300
www.nga.org/center