FISCAL YEAR 2013

HOMELAND SECURITY GRANT PROGRAM

SUPPLEMENTAL RESOURCE: CYBER SECURITY GUIDANCE

U.S. DEPARTMENT OF HOMELAND SECURITY

CYBER SECURITY GUIDANCE

With the pervasiveness of information technology (IT) and cyber networks systems in nearly every aspect of society, effectively securing the Nation's critical infrastructure requires investments in network resiliency as well as cyber infrastructure protection. As all levels of government now rely on cyber networks and assets to provide national security, public safety, and economic prosperity, their operations depend on information systems that are maintained, protected, and secured from exploitation and attack. In recognition of this importance, President Barack Obama has identified the digital infrastructure as a strategic national asset.

> "Many of the Nation's essential and emergency services, as well as our critical infrastructure, rely on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyber attack could be debilitating to our highly interdependent CIKR and ultimately to our economy and national security."
>
> National Strategy for Homeland Security, October 2007

The increasing frequency and sophistication of cyber attacks on critical infrastructure and key resources (CIKR) requires planning across all State, local, Tribal, and Territorial (SLTT) homeland security components to develop robust strategies to prepare for and respond to events that can degrade or destroy SLTT governments' abilities to deliver essential services to citizens and prepare for the impact of terrorist or criminal activity or natural disaster.

Nation-states, criminal organizations, terrorists, and other malicious actors conduct attacks against critical cyber infrastructure on an ongoing basis. The impact of a serious cyber incident or successful cyber attack would be devastating to SLTT governments' assets, systems, and/or networks; the information contained therein; and the confidence of those who trust governments to secure those systems.

SLTT planning should incorporate intra-state coordination with sound assessment and mitigation practices to drive development and maintenance of robust cyber security capabilities within the All-Hazards framework of homeland security. To effectively address the security of SLTT cyber assets, consider the following preparedness measures:

- The degree to which government IT, communications, and cyber infrastructures provide operational support for the systems on which State essential services, including Homeland Security, function
- How a loss or degradation of these systems would hinder homeland security operations and essential functions

- How state preparedness and response efforts benefit from assessments of threats and vulnerabilities to these systems and as well as analysis of the malicious and potentially illegal activity occurring on them

As a means to guide these efforts, State Administrative Agencies (SAA), security officials, and authorities at all levels of government should review cyber infrastructure and assets based on appropriately tailored vulnerability assessments. Doing so will better enable coordinated investments and protective measures, increasing return on investment and overall security.

This Annex outlines parameters for SLTT government officials to coordinate preparedness planning efforts to ensure cybersecurity investments are considered and supported in long term development considerations. Potential grantees should review the guidance provided below prior to submitting proposals and discuss how to apply it to SLTT planning with cybersecurity and IT leadership (i.e., Chief Information Officer, Chief Information Security Officer, etc.). This due diligence will ensure that grantees amply address their cybersecurity goals and objectives and assess current activities to bolster the security of state computer network enterprises.

A. The Role of Cyber Systems

IT network infrastructure enables the functions and services of all sectors, resulting in a highly interconnected and interdependent global CIKR network. The U.S. Department of Homeland Security (DHS) is leading efforts to engage and work with security partners at the State and local level, as well as in the private sector and academia, to ensure that the cyber elements of critical infrastructure are robust, responsive, and resilient. As such, state planning should consider the full scope of cyber assets and network infrastructure in mission critical systems that support incident response and emergency management, physical security protection, law enforcement and intelligence gathering, and other State homeland security functions. For example:

> **Cyber infrastructure** includes electronic information and communications systems, and the information contained in those systems. Computer systems, control systems such as Supervisory Control and Data Acquisition (SCADA) systems, and networks such as the Internet are all part of cyber infrastructure.
>
> – National Infrastructure Protection Plan (NIPP), 2006

- Malicious activity originating in cyberspace can affect physical system components and potentially lead to property damage and loss of life. Aligning State and local cyber incident response activity to national policies and protocols, and assigning responsibility to a central authority will ensure a uniform, coordinated response to any such event.
- Shifting to Internet protocol (IP) networks for such services as interoperable emergency communications and 911 systems provides State and local responders with new capabilities for prevention, response, and recovery. It also

introduces new vulnerabilities, which, if ignored, can severely hamper communications during a time of crisis.

- Degradation or disruption of IT and communications functions can inhibit execution of continuity of governance or continuity of operations plans following a catastrophic event or other physical security incident. Accounting for redundant and alternative systems for supplying essential functions in emergency response planning reduces "down time" on critical systems.
- Other infrastructures, including transportation, water treatment, electric power, and other control systems-based elements owned and operated by States and municipalities are vulnerable.
- State and local Fusion Centers rely on IP networks to communicate vital data for tactical and operational decision-making. The failure of IT networks could hamper analysis of a developing crisis, hurting decision making at critical junctures, especially if errors coincide with a larger man-made or natural disaster.
- Malicious and criminal activity online against government systems and assets can accompany criminal activity in the physical world. Information on such activity can contribute greatly to law enforcement investigations and prosecutions and should be available to SLTT law enforcement entities.
- Effectively addressing cyber threats to the SLTT enterprise requires situational awareness across the multiple systems and coordination by a central authority. Two-way sharing of information on malicious activity and cyber attacks significantly contributes to situational awareness as well as appropriate response measures.

B. Building Capabilities and Allowable Costs

Establishing cybersecurity as a primary target capability in preparedness planning provides the foundation on which to build operational functions in cyber response and recovery, and enhanced coordination of activities though all levels of government. **As such, funds from each of the fiscal year 2011 Homeland Security Grant Program (HSGP) components – State Homeland Security Program, Urban Areas Security Initiative, Metropolitan Medical Response System, and Citizen Corps Program – can be used to invest in functions that support and enhance SLTT cybersecurity programs.**

- **Equipment:** Expenditures that cover a wide range of investments including network protection, intrusion detection, and encryption technologies. More information on the DHS Approved Equipment List, including a breakdown of Cybersecurity Enhancement Equipment, is available on the Responder Knowledge Base, *www.rkb.us*.

- **Planning:** Each SLTT government entity should develop and implement a comprehensive cybersecurity approach to manage cyber risk that is fully incorporated into overall State homeland security plans and operations. The plans should be reviewed and updated on a periodic basis to address technology and vulnerability changes, cover the full scope of threats facing State enterprises,

and account for IT and computer systems owned and operated by all State, regional, local, Tribal, and Territorial governments.

- **Training:** Expanding government employees knowledge of cyber threats and security measures and well as enhancing capabilities of existing IT and cyber security staff contributes to overall security posture of the government enterprise. Information on various training courses is available at *www.nw3c.org*, *www.sentinelproject.net* and *www.fema.gov/about/training*.

- **Exercises:** Scenarios must be based on events that adhere to State Homeland Security strategies and focus on testing and validating existing capabilities. Cyber events are unique in that they can result in physical impacts to systems that are highly localized in nature, yet be driven by anonymous actors operating outside of regional authorities.

- **Personnel/Operations:** In addition to staff to support the above activities, grantees can apply for funds to hire analysts to monitor and assess the health of critical computer systems as well as coordinate information sharing and response efforts to cyber incidents.

C. Guiding Investment Decisions

Securing cyber systems requires a layered defense that accounts for the range of security challenges facing organizations, including logical and physical threats to cyber-based systems. There are a number of resources available to help State and local security officials conduct assessments – all of which can help inform where to allocate funding obligations to build cyber security capabilities. Resources include: the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) and the DHS Office of Cyber Security and Communications (CS&C). NIST provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services. NIST develops guidance on securing information systems, methods for assessing the effectiveness of security requirements, and managing risk from information systems (in addition to many other topics). In addition, CS&C establishes tools, techniques, and methods specific for critical infrastructure organizations and SLTT agencies. CS&C methods evaluate both practice adoption as well as capability management for cyber security – using techniques that draw on existing cyber security guidance and standards to assist organizations in assessing their security posture for strategic and operational gaps.

- The Cyber Security Evaluation Tool (CSET) is a DHS product, allows for self-evaluation or facilitated capture, and provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. The CSET tool is designed to raise awareness and foster discussions on cyber security within an organization. It highlights security controls and vulnerabilities – termed as gaps in controls – in the organization's systems and provides *options for consideration* on ways to address control deficiencies. The results of the CSET assessment can be used as a starting point

for making informed investment and as input to risk-based decisions; and organizations can use CSET results to demonstrate the degree to which they have adopted best practices in cyber security. Additional information on the CSET is available at cset@hq.dhs.gov.

The Cyber Resilience Review (CRR) is a DHS service, facilitated by an evaluation team, and used to measure and enhance key cyber security capacities and capabilities required to protect and sustain mission-critical services. The goal of the CRR is to evaluate an organization's operational resilience and ability to manage cyber risk to its critical services and assets during normal operations and during times of operational stress and crises. The CRR is a repeatable cyber review and allows for an evaluation and organization's overall cyber security management policies, practices, and procedures. The CRR can also be used to support resource allocations for cyber security capability improvements, in such areas as: strategic and operational planning, personnel management, operational risk management, and service continuity. For more information about the CRR, contact the CSEP program at cse@hq.dhs.gov.

In addition to identifying security gaps and measuring capability, organizations can use either technique (i.e., CSET or CRR) to document "options for consideration," and/or produce a prescriptive list of security control deficiencies that require funding consideration. Armed with this information, formal risks assessments further contextualize this information against other information on assets, threats, known vulnerabilities in people, process, and technology, and consequences. Once a risk assessment is complete, State and local security officials should work with State HSAs and state planning entities to ensure that identified gaps receive adequate funding for mitigation activities and equipment. Finally, implementing the CSET, the CRR, or any assessment tool/methodology for use in identifying cyber security vulnerabilities should be conducted in partnership with all State homeland security components to account for the full range of functions supported by cyber systems.

D. Conclusion

It is the recommendation of the U.S. Department of Homeland Security that State Homeland Security Advisors, State Administrative Agencies, and all state homeland security planning entities evaluate the full scope of cyber threats and vulnerabilities to all existing and envisioned homeland security functions, systems, and procedures before applying for funding under the Homeland Security Grant Program. By incorporating assessments of the systems and assets that support State IT and cyber infrastructure, State planners can more effectively seek funding for and implement mitigation strategies for protecting critical functions, ensure ongoing delivery of services, and protect the safety and wellbeing of citizens.

It is also the recommendation of the U.S. Department of Homeland Security that State Homeland Security Advisors incorporate cybersecurity in supported and long term development considerations. As the underpinning of most of our CIKR, cyber elements of critical infrastructure need to be robust, responsive, and resilient.

Comparing current cyber security activities with the desired level of preparedness will enable officials to identify gaps and needed enhancements that can be accounted for in investment justifications. Establishing and enhancing cyber security capabilities that are fully-integrated into ongoing state preparedness efforts provides the foundation on which to enhance collaboration and coordination from across state functions and through all levels of government in building All-Hazards capabilities. As more and more technologies are integrated into our Nation's prevention protection, response, and recovery activities, cyber security will be an essential requirement. Investing now may help lay the foundation SLTT stakeholders need for future All-Hazards efforts.

Grantees are urged to review information provided by the following resources, which provide valuable guidance, best practices, and opportunities for support and information sharing:

- The *Office of Cybersecurity and Communications* (CS&C), within the National Protection and Programs Directorate, is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.
  http://www.dhs.gov/office-cybersecurity-and-communications

- The *United States Computer Emergency Readiness Team* (US-CERT) is a partnership between DHS and public and private sector security partners. Established in 2003 to protect the Nation's Internet infrastructure, it coordinates defense against and responses to cyber attacks across the Nation by collaborating with State and local Governments and sector information sharing and analysis centers (ISACs), analyzing cyber threats and vulnerabilities, and disseminating cyber threat warning information.
  Information is available at *www.Us-Cert.gov/*.

- The *National Institute of Standards and Technology* (NIST) is a non-regulatory Federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. The NIST Information Technology Laboratory, Computer Security Division provides a variety of tips, newsletters, and publications to support cyber security efforts.
  Information is available at *www.nist.gov*.

- The *National Association of State Chief Information Security Officers* (NASCIO) provides a mechanism for collaboration on security investment priorities among state CIOs and leading IT officials in the states. Through its Information Security and Privacy Committee, NASCIO identifies security-related issues that States may encounter and offers insight and effective security practices to address those issues. Topics addressed have included the security and privacy implications of emerging technologies, such as wireless technologies, the role of the Chief Information Security Officer, and insider threats.
  Information is available at *www.nascio.org/.*

- The *Multi-State Information Sharing and Analysis Center* (MS-ISAC) is a focal point for information sharing on IT and cyber security between and among State and local governments. It is a voluntary and collaborative organization with participation from all 50 states and the District of Columbia that provides a common mechanism for raising the level of cyber security readiness and response in each State and with local governments. In addition, DHS has officially recognized the MS-ISAC as the national center for States to coordinate cyber readiness and response. The US-CERTand MS-ISAC exchange information regularly to facilitate National coordination of cyber security detection, prevention, and response activities.
  Information is available at *www.msisac.org/.*