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. 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 activity or natural disaster.

> "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

Nation-states, criminal organizations, terrorists, and other malicious actors conduct attacks against critical cyber infrastructure on an ongoing basis. According to the National Institute of Standards and Technology (NIST) National Vulnerability Database, 6,608 new computer vulnerabilities were catalogued in 2006; 6,516 in 2007; and today the database continues to increase at a rate of 11 vulnerabilities published per day. 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 Homeland Security functions operate
- 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 cyber security investments are adequate 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 cyber security and IT leadership (i.e., Chief Information Officer, Chief Information Security Officer, etc.). This due diligence will ensure that grantees amply address their cyber security goals and objectives and assess current activities to bolster the security of state computer network enterprises.

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.

Building Capabilities and Allowable Costs

Establishing cyber security as a 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 2009 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 cyber security 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 Cyber Security Enhancement Equipment, is available on the Responder Knowledge Base, *www.rkb.us*.

- **Planning:** Each SLTT government entity should develop and implement a comprehensive cyber security 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 additional 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.

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. DHS's National Cyber Security Division (NCSD) has established tools to help State and local security officials conduct assessments that can inform where to allocate funding obligations to build cyber security capabilities. NCSD's *Cyber Security Vulnerability Assessment (CSVA)* draws on an automated set of questions to assess an entity's cyber security posture and recommend a suite of remedial actions to address any observed security gaps. The methodology will assess an organization, facility, or system's cyber vulnerabilities and provide explanations, examples, and options for consideration when potential cyber security enhancements could be implemented.

The *FY08 HSGP Supplemental Resource: Cyber Security Guidance* includes a number of questions intended to facilitate the development and refinement of state cyber security plans in HSGP planning that were based the CVSA methodology. The following topic areas are extracted from the CSVA methodology and offer a framework to identify vulnerabilities in cyber systems and to develop cyber security plans to represent the desired security posture. This process can now be automated through adoption and use of the CSVA tool.

- **Cyber Security Policy -** Policies, plans, and procedures are related but serve distinctly different purposes. A policy is the highest level document that states what a company, group, or department will and will not do during a cyber emergency. A plan is the organizational document that describes a methodology for how to achieve the policy's goals. A procedure is the step-by-step instructions to the operator for exactly how a task is to be done.

- **Electronic Access Control -** In order to guard a system against loss or damage, a system of identification and authentication controls is put in place to ensure that only authorized users and system components gain access to sensitive data. Controls come in many different varieties but the purpose is always to mitigate or reduce a risk. An initial step in this risk mitigation

process is authentication, which is the act of identifying with certainty that someone or something is who or what they claim to be. Once the identity of the user is authenticated, or verified, their credentials can be checked to see what they are and are not authorized to access.

- **Personnel Security -** According to the FBI's Cyber Crimes Division, the majority of all data theft and computer related crime occurs from internal sources. As such, it is critical that personnel security measures, appropriate for the type of business and data being protected, are put in place. Implementing protective measures such as performing background checks on new hires, practicing separation of duties and implementing administrative controls like immediate revocation of credentials upon an employee's termination, all serve to mitigate the risk posed by internal personnel.

- **Physical and Environmental Security -** Physical damage to a system can be just as devastating, and sometimes even more so, as a result of an electronic attack. Physical and environmental security guards against five threats: interruptions in data services, physical damage, unauthorized access of information, loss of system integrity, and physical theft. By applying controls in the physical environment, as opposed to controls in a logical data or administrative environment, the risk level of these five threats is significantly reduced.

- **Cyber Security Awareness and Training -** The most vulnerable aspect of a system is the human component. Users who have been granted access to a system need to be instructed in how to keep that access information confidential. Along with access credentials, users possess other knowledge of an organization that can be valuable to someone with malicious intent. In addition to logical controls, physical controls, a comprehensive company policy, and other important security measures, training should be performed regularly in order to maximize the effectiveness of existing security measures and to reduce the risk of social engineering. Security training and reinforcement of that training through ongoing awareness information sessions has been shown to lower the risks associated with the human "component" of a security strategy.

- **Monitoring and Incident Response -** In the event of an emergency that involves a system failure, a detected or active intrusion, or a virus attack, having an established protocol and response team is critical to timely incident response and the ability to limit the extent and degree of the damage. Monitoring and incident response addresses the need for a proactive approach to system incidents. Rather than waiting for incidents to occur and attempting to shape a response when time and resources are not at optimal levels, preparation ahead of time can greatly reduce the damage caused by as well as the time needed to recover from an adverse event. Recognizing security events for what they are and making management aware of the incidents and their potential for harm is a critical element, not only to limit the

damage from cyber attacks, but also to obtain the appropriate support and resources to effectively manage cyber security.

- **Disaster Recovery and Business Continuity -** IT systems are known to be vulnerable to a variety of adverse events, any of which has the potential to impact normal business operations and compromise the confidentiality, integrity, and availability of data. Although planning and mitigation strategies are known to reduce the risks posed by these events, it is impossible to fully eliminate the risks, and the potential damage posed by them. Because of this, due care should be taken to plan what steps an organization will take in the event of a system disruption, no matter the size. By making and testing effective plans ahead of time, the potential damage; and the potential loss of productivity, revenue, and information can be greatly reduced.

- **System Development and Acquisition -** As security has become a higher priority for all systems, security awareness and preparation have become critical issues. Integrating system security into the existing development lifecycle will ensure that money is budgeted, personnel are designated, and requirements are gathered for security at the appropriate time rather than after it is inconvenient, prohibitively expensive, or impossible. Security should be considered and provided for from system design, through procurement, implementation, operation, and disposal.

- **Configuration Management -** A formal configuration management process should be documented and followed. Without a defined process that takes into account policy mandates, security concerns, business impact, authorization, and oversight, configuration changes can weaken the stability and security of a system. A configuration management process ensures the most effective and efficient application of network and system updates, reduces the likelihood of the introduction of malicious code, and reduces the chance of human error. In addition to the security benefits, additional business benefits are gained by following a formal change management process. These benefits include having a repeatable process for recreating a product, the ability to efficiently reuse components of a project or product, and protection against loss of intellectual capital should turnover of key personnel occur.

- **Risk (and Vulnerability) Management -** Cyber risk methodologies usually include various processes to identify and measure risk to a system or group of systems and provide a repeatable method for conducting and monitoring risk. Most common to all methodologies are means to conduct risk assessments, perform system testing including observation, data analysis, and electronic testing (e.g., vulnerability scanning, penetration testing), and finally, a means of tracking and monitoring system weaknesses and mitigation activities (e.g., Plan of Action). The risk identification methodology should be standardized and approved by senior management to ensure results are consistent with one another and throughout the organization.

Once the 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. The involved parties should collectively review at least two additional bodies of information to inform their cyber infrastructure protection strategies: the IT Sector Critical Functions and R&D priorities.

IT Sector Critical Functions

- Provide IT products and services
- Provide incident management activities
- Provide Domain Name resolution services
- Provide identity management and associated trust services
- Provide Internet-based content, information, and communications services
- Provide Internet routing, access and connection services

In recent years, the Government has worked with developers of IT products and services to identify sets of processes that create, provide, and maintain products and services essential to the continued operation of critical cyber infrastructure. The identification of these processes resulted in the development of the critical IT Sector functions. The IT Sector-Specific Plan (SSP), published in May 2007 and updated in May 2008, lists six critical functions of cyber infrastructure that also have application at the State and local level. As such, the list can be informative when determining areas for additional security investment.

Implementing the CSVA's 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. Additional information on the CSVA is available at ncsd_cipcs@hq.dhs.gov.

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 implement mitigation strategies for protecting critical functions, ensure ongoing delivery of services, and protect the safety and wellbeing of citizens.

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:

- *DHS's National Cyber Security Division* (NCSD) works collaboratively with public, private, and international entities to secure America's cyber assets by building and maintaining an effective national cyberspace response system and implementing a cyber-risk management program for protection of critical infrastructure. It has resources that can assist State and local Governments in bolstering their cyber security capabilities. Information is available at *www.dhs.gov/xabout/structure/editorial_0839.shtm.*

- 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/*.