U.S. DEPARTMENT OF HOMELAND SECURITY

Fiscal Year 2008

HOMELAND SECURITY GRANT PROGRAM

SUPPLEMENTAL RESOURCE: CYBER SECURITY GUIDANCE

February 2008

U.S. DEPARTMENT OF HOMELAND SECURITY

CYBER SECURITY GUIDANCE

This Annex supports preparedness as a Homeland Security goal by providing guidance to State and local government officials to more fully assess the adequacy and effectiveness of their cyber security programs and measures. Comparing current cyber security activities with the desired level of preparedness (based on requirements and acceptable risk) will enable officials to identify gaps and needed enhancements. This process facilitates informed decision making, including effective use of the DHS Information Technology and Telecommunications (IT&T) Target Capabilities List (TCL)[1] to identify capabilities that can be supported through the Homeland Security Grants Program.

Various national strategies and policy documents, including the *National Strategy to Secure Cyberspace*[2] and the *National Infrastructure Protection Plan* (NIPP)[3], highlight the importance of cyber infrastructure[4] and responsibility for cyber security that is shared across public and private sector entities, including State and local governments, and individual citizens. The NIPP states that:

> The US economy and national security are highly dependent upon cyber infrastructure, which enables the Nation's essential services by supporting business processes and assisting in the control of many critical processes, including drinking and waste water treatment facilities, electric utilities, dams, and mass transit systems.
>
> A spectrum of malicious actors can and do conduct attacks against critical cyber infrastructure on an ongoing basis. DHS and the Federal Sector Specific Agencies (SSA) are committed to working collaboratively with other public, private, academic, and international entities to enhance cyber security awareness and preparedness efforts, and ensure that the cyber elements of critical infrastructure are robust enough to withstand attacks without incurring catastrophic damage; responsive enough to recover from attacks in a timely manner; and resilient enough to sustain nationally critical operations.

[1] The *DHS Information Technology and Telecommunications Target Capabilities List* is currently under development. Information can be obtained by contacting the Strategic Initiatives Branch within the DHS National Cyber Security Division at ncsd_si_branch@hq.dhs.gov.

[2] *National Strategy to Secure Cyberspace* *http://www.whitehouse.gov/pcipb/*

[3] *National Infrastructure Protection Plan* *http://www.dhs.gov/nipp*

[4] *National Infrastructure Protection Plan*, Page 13, The Cyber Dimension: 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. Information and communications systems are composed of hardware and software that process, store, and communicate. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.

Government entities at all levels should recognize their reliance on cyber infrastructure by assessing the risk[5] to government functions supported by that infrastructure, in order to enable informed decision making and to apply resources in the most effective manner.

Each State and local government entity should develop and implement a comprehensive cyber security plan to manage cyber risk. The plan should account for factors such as: size and complexity of the jurisdiction; variety of technologies in use; varying levels of cyber security and technology knowledge; personnel and resource constraints; and staff turnover. In addition to a comprehensive plan, State and local governments should review and update these plans on a periodic basis to address technology and vulnerability changes.

According to the National Institute of Standards and Technology (NIST) National Vulnerability Database[6], 4,883 new computer vulnerabilities were catalogued in 2005; 6,604 in 2006; and at the time of this writing, they continue to increase at a rate of 22 vulnerabilities published per day. The impact of a serious cyber incident or successful cyber attack can be devastating to an organization's assets, systems, and/or networks; on the information contained therein; and, just as importantly, on the confidence of those who trust that government secures those systems.

Therefore, comprehensive vulnerability assessments serve as a resource to facilitate the development and refinement of cyber security plans. By identifying cyber vulnerabilities and applying appropriate mitigations, State and local government entities can reduce the risk to their cyber infrastructure.

All jurisdictions should consider the following ten topic areas when assessing cyber vulnerabilities and developing or updating cyber security plans:

- Cyber Security Policy
- Electronic Access Control
- Personnel Security
- Physical and Environmental Security
- Cyber Security Awareness and Training
- Monitoring and Incident Response
- Disaster Recovery and Business Continuity
- System Development and Acquisition
- Configuration Management
- Risk (and Vulnerability) Management

[5] Risk is a function of threats to, vulnerabilities of, and consequences of the compromise or exploitation of the infrastructure.

[6] National Vulnerability Database *http://nvd.nist.gov/*
The NIST Computer Security Division operates the National Vulnerability Database (NVD), which is co-sponsored by DHS. The NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources.

Each of these areas mitigates cyber vulnerabilities, and when combined, they create a layered defense that addresses the range of cyber security challenges facing organizations.

Local jurisdictions should implement a similar process with the same topic areas, within the perspective of their individual operations. Every government entity that owns and operates IT assets, systems, and networks should have at least a basic cyber security plan that incorporates these ten topics.

The following questions are intended to give State and local officials a framework to identify key issues within each major topic area and develop cyber security plans to represent the desired security posture. They support the four national preparedness activities[7]: prevent, protect, respond, and recover.

Cyber Security Policy (Prevent)

- Does the State have cyber security policies, plans, and procedures in place that set the vision, goals, and objectives for State-wide cyber security? If so, have they been made available to local jurisdictions? And, if so, has the local jurisdiction adapted them for their own use?
- Has the State/local agency designated an individual(s) to be responsible for the cyber security of their IT infrastructure?

Electronic Access Control (Protect)

- Does the State/local agency know if, where, and how their systems and networks are connected to external networks (e.g., Internet, modems, wireless), and if internal systems and networks can communicate with portable electronic devices or media?
- Does the State/local agency practice the concept of least privilege (e.g., users are only granted access to those files and applications based on roles and responsibilities)?
- Does the State/local agency require that all default passwords be changed, and are audits conducted to ensure compliance?

Personnel Security (Protect)

- Does the State/local agency perform background checks for personnel in critical/sensitive positions?
- Does the State/local agency actively maintain access control lists to ensure that all system and network accounts are modified, deleted, or de-activated as personnel leave or transfer into new roles?

Physical and Environmental Security (Protect)

- Does the State/local agency limit physical access to sensitive or restricted IT areas to those with appropriate need?

[7] HSPD-8: National Preparedness. *http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html*

Cyber Security Awareness and Training (Prevent, Protect, and Respond)

- Are there requirements by the State/local agency to ensure their employees receive annual cyber security awareness training commensurate with employees' responsibilities?
- Does the State/local agency test emergency policies, plans, and procedures through different types of exercises (e.g., full-scale, functional, tabletop, etc.) to ensure an appropriate level of preparedness and response to cyber events? Do the exercises produce lessons learned, and corrective action plans that are implemented to improve incident response and operational capabilities? (See Homeland Security Exercise and Evaluation Program[8] and NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006[9].)

Monitoring and Incident Response (Prevent, Protect, and Respond)

- Does the State/local agency have operational cyber incident response plans?
- Does the State/local agency log cyber security events on firewalls and servers? Are cyber intrusion detection systems (IDS) or intrusion prevention systems (IPS) used? And are event logs reviewed regularly by qualified personnel?
- Does the State/local agency mandate virus protection on all systems? If so, does the State/local agency update virus definition files on a regular basis?
- Does the State have an operational 24/7 cyber incident response capability? Can local jurisdictions rely on the State to provide specialized assistance, such as incident response and forensic analysis capabilities?
- Are the State/local agency's system and network management and administration personnel required to report significant cyber security events to senior agency officials, and do they, in turn, report them to State senior officials?

Disaster Recovery and Business Continuity (Prevent)

- Does the State/local agency have documented IT Contingency or Disaster Recovery Plans in place in the event of natural or man-made disasters? Are these IT specific plans fully integrated into State-wide Continuity of Operations or Continuity of Government plans using an all-hazards approach?
- Has the State/local agency identified disaster response roles and responsibilities for key personnel supporting their cyber infrastructure, and is their contact information up-to-date?

System Development and Acquisition (Protect)

- Is cyber security integrated into the system development lifecycle of State/local agency systems and networks, and when procuring IT services, hardware, software, etc.?

Configuration Management (Prevent and Protect)

[8] Homeland Security Exercise and Evaluation Program, Vol. I – III, February 2007 *https://hseep.dhs.gov/*

[9] NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006 *http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf*

- Does the State/local agency have current inventories of all internal (e.g., servers, proxies, routers, firewalls, Voice over Internet Protocol (VOIP) devices, workstations, printers, remote terminal units (RTU), access control systems, closed circuit television (CCTV) systems, private branch exchange (PBX) telephone systems, alarm systems, fire control systems, radio, or wireless, etc.) and external (e.g., Internet, websites, VPN, gateways, routers, firewalls, wireless access points, modems, vendor maintenance connections, IP address ranges, etc.) network nodes?
- Has a business requirement been established for every external connection that provides access to the State/local agency's systems and networks, including wireless and modem connections?
- Does the State/local agency apply/perform regular software and hardware patches, updates, upgrades, and replacements?

Risk (and Vulnerability) Management (Protect)

- Does the State/local agency have a means to identify and measure cyber security risk (including requirements, processes, and procedures) that is based on recognized cyber security methodologies, standards, or best practices?
- Does the State/local agency have a formal program for periodic internal vulnerability assessments, including a process by which assessment results are converted into prioritized remedial actions and tracked to completion?
- Does the State/local agency perform network and system (application) level security tests (e.g., vulnerability scans, penetration tests, open communication line scans, authorized hardware and/or software scans) on a periodic basis to address technology and vulnerability changes?
- Does the local agency maintain a relationship with a State Cyber Security Incident Response Team (CSIRT)? And does the State, in turn, maintain a relationship with entities such as the United States Computer Emergency Readiness Team (US-CERT)[10] at DHS; the Multi-State Information Sharing and Analysis Center (MS-ISAC)[11]; and the National Association of State Chief Information Officers (NASCIO)[12]?

The table below is provided to illustrate the linkage between the Cyber Security Topics above and the TCL Mission Activities. For example, if, by using the ten topic areas, the agency identifies the need to enhance electronic access control, then that need maps to the TCL Activity *Protect: Deploy Protective Controls*. One mitigation strategy could be *enhanced identification and authentication*. The agency can then request resources through the grant process to acquire the solution.

[10] U.S. Computer Emergency Readiness Team (US CERT) http://www.us-cert.gov/
Established by DHS, US-CERT is a 24x7 operation that analyzes and disseminates threat information, works to reduce cyber vulnerabilities, and coordinates incident response. The US-CERT website provides vulnerability information and security bulletins.

[11] Multi-State Information Sharing and Analysis Center (MS-ISAC) http://www.msisac.org/

[12] National Association of State Chief Information Officers (NASCIO) https://www.nascio.org/

Cyber Security Topic	**TCL Mission Activity**
Cyber Security Policy	Prevent: Develop and Maintain Strategies, Plans, and Procedures
Electronic Access Control	Protect: Deploy Security Controls
Personnel Security	Protect: Deploy Security Controls
Physical and Environmental Security	Protect: Deploy Security Controls
Cyber Security Awareness and Training	Prevent: Train Personnel

Monitoring and Incident Response	Prevent: Develop and Maintain Strategies, Plans, and Procedures;
	Monitor Current Infrastructures;
	Protect: Deploy Security Controls
	Respond: Activate Response Plans; and Assess Damage to Infrastructures

Disaster Recovery and Business Continuity	Prevent: Develop and Maintain Strategies, Plans, and Procedures; and Identify Current Infrastructures
System Development and Acquisition	Protect: Deploy Security Controls
Configuration Management	Prevent: Identify Current Infrastructures Protect: Deploy Security Controls
Risk (and Vulnerability) Management	Protect: Assess Risks; Deploy Security Controls

DHS is developing a more comprehensive and objective cyber security vulnerability assessment methodology, the *DHS/National Cyber Security Division (NCSD) Cyber Security Vulnerability Assessment (CSVA),*[13] that leverages concepts from well recognized standards and guidance, such as the International Organization for Standardization (ISO) 27002[14], COBIT[15], NIST SP 800-53[16], and others. The methodology will quickly assess an organization, facility, or system's cyber vulnerability(ies) and provide explanations, examples, and options for consideration when potential cyber security enhancement could be implemented. The topic areas above are extracted from the methodology and can provide State and local officials with

[13] The *DHS/NCSD Cyber Security Vulnerability Assessment* can be obtained by contacting the Critical Infrastructure Protection / Cyber Security Program within the DHS National Cyber Security Division at ncsd_cipcs@hq.dhs.gov.

[14] International Organization for Standardization ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[15] Information Systems Audit and Control Association, *Control Objectives for Information and related Technology* *http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981*

[16] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* *http://csrc.nist.gov/publications/nistpubs/index.html*

an understanding of the perspective of the methodology, and how it will help to identify cyber security needs at the State and local government levels.

Numerous sources exist for guidance on conducting cyber vulnerability assessments, including but not limited to NIST and the ISO. State and local government officials are encouraged to review the information in the references within this guidance, which provide valuable advice, best practices, and opportunities for support and information sharing. State and local government officials are also encouraged to collaborate with key State stakeholders (e.g., Chief Information Officers and Chief Information Security Officers) and information sharing forums such as the Multi-State ISAC and NASCIO to exchange perspectives on the grant process and to identify common cyber security requirements.