U.S. DEPARTMENT OF HOMELAND SECURITY

Preparedness Directorate
Office of Grants and Training

FY 2007 Homeland Security Grant Program

Supplemental Resource:
Cyber Security Guidance

January 2007

U.S. DEPARTMENT OF HOMELAND SECURITY

Cyber Security Guidance

Government entities at every level must have appropriate policies in place, understand where vulnerabilities exist, weigh the risks involved and make informed decisions on how to spend resources to secure data. Some 10,000 new computer viruses were reported last year, and it now only takes a few minutes to compromise an unprotected computer that is connected to the Internet. The negative impact of a virus or successful cyber attack can be devastating on networks, on the information contained within systems and, just as importantly, on the confidence of those who trust that government is working to increase protection.

Each State and local government entity should develop and execute a comprehensive cyber security plan that demonstrates due diligence in cyber security. The plan must account for factors such as limited staff and resources (and staff turnover); varying size and complexity of the State and local government entities; varying cyber security and technology knowledge base within government; and a wide variance in technology being used. In addition to a comprehensive plan, government must periodically test and exercise this plan, using vulnerability assessments to identify gaps and training needs.

All jurisdictions should ensure that their cyber security plan addresses four main areas: Policy, Training, Technology Deployment, and Vulnerability Assessment. Each of these areas supports the others, and together they meet emerging standards of due diligence in information security. The questions below are designed to identify key issues within each major area at the State level.

Policy:

- **Does the State have a cyber security plan in place that sets the vision, goals, and objectives for Statewide cyber security?**
- **Has the State published a clear policy statement on cyber security to support the plan, including "permitted use" policy for all State-owned cyber assets? Has this policy set been made available to jurisdictions within the State so that it can be adapted for their user?**
- **Has the State established a certification/accreditation program for information systems?**
- **Does the State have a designated cyber security office/officer whose primary focus is on protecting the State's cyber infrastructure?**
- **Does the State have established cyber security metrics? Does the State have a mechanism for rating its cyber security alert level?**
- **Does the State maintain a current inventory of cyber assets, including personnel?**
- **Has the State established public, private, or academic partnerships for cyber security collaboration?**
- **Does the State have a capability for internal secure information sharing (Statewide secure portal)?**

- **Does the State have a formal mechanism for information sharing with external partners (including local government)?**
- **Does the State have a cyber operational center that functions 24/7? Does the State have an ad-hoc 24/7 capability if an operational center does not exist?**
- **Does the State have a Statewide Computer Security Incident Response Team?**
- **Does the State have a response plan for responding to critical cyber related events?**
- **Does this plan include a continuity of communications component?**
- **Does the State maintain a relationship with Federal entities such as the United States Computer Readiness Response Team (US-CERT)?**

Training:

- **Are there requirements by the State to ensure employees have cyber security training and awareness on an annual basis?**
- **Are training programs available at multiple levels commensurate with employees' responsibility (e.g., general awareness, system administrator, network administrator)?**
- **Does the State have an outreach program to ensure the greatest penetration possible for cyber security awareness throughout State and local governments?**
- **Does the State have a web presence that provides cyber security guidance?**
- **Does the State have a program to establish and maintain a set of best practices for cyber security, both for its own use and to share with local jurisdictions?**

Technology Deployment:

- **Has the State deployed appropriate technology for basic cyber security requirements such as anti-virus protection and network intrusion detection?**
- **Has the State deployed specific technology (including modifications and patches to existing systems and software) to respond to vulnerabilities identified by internal or third-party vulnerability assessments?**
- **Does the State have a system in place for tracking software versions in use, relevant known vulnerabilities, and available patches to counter those vulnerabilities.**
- **Does the State have cyber forensics capabilities to serve both civilian and criminal matters for the State?**

Vulnerability Assessment:

- **Does the State have a formal program for periodic internal vulnerability assessment?**
- **Does the State supplement its internal assessment program with third-party vulnerability assessments?**
- **Is there a formal process by which assessment results are converted into prioritized remedial actions and tracked to completion?**

Local jurisdictions should review many of the same questions, scaled to their individual needs. *Every government entity that owns and operates information technology equipment should have at least a rudimentary cyber security plan, and establish an Information Security Officer (ISO) or single point of contact (POC) for cyber security, including up-to-date 24/7 contact information.* Smaller jurisdictions should rely on their parent entities to provide sample policy documents and plans, as well as specialized assistance such as forensic analysis.

Grantees are urged to review the information at the following site, which provide valuable advice, best practices, and opportunities for support and information sharing:

National Institute of Standards and Technology (NIST)
http://csrc.nist.gov/
Founded in 1901, 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.

Multi-State Information Sharing and Analysis Center (MS-ISAC)
http://www.cscic.state.ny.us/msisac/index.html
A public site identifying what the MS-ISAC is and what its mission, goals and objectives are in improving the Nation's cyber security posture from a State and local perspective. The goal is to have this MS-ISAC include all fifty States, which would provide a valuable centrally-coordinated mechanism for sharing important security intelligence and information between the States. The MS-ISAC can serve as a critical point of contact between the States and the Federal government. A primary goal of the MS-ISAC is to eliminate duplicative efforts.

U.S. Computer Emergency Readiness Team (US CERT)
http://www.us-cert.gov/
Established in 2003 to protect the Nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the Nation.

The SANS™ Institute

http://www.sans.org
SANS is an example of non-government cyber security resources, and is one of the largest sources for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and operates the Internet's early warning system - Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face.

National Strategy to Secure Cyberspace
http://www.whitehouse.gov/pcipb/
The National Strategy to Secure Cyberspace is part of our overall effort to protect the Nation. It is an implementing component of the national Strategy for Homeland Security and is complemented by a national Strategy for the Physical Protection of Critical Infrastructures and Key Assets. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.