Nationwide Cyber Security Review

The cyber threats facing our Nation are not limited to Federal networks. As such, we depend on the preparedness of our partners in all sectors and in State and local governments. To gauge the nationwide level of cybersecurity readiness the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) will measure the adoption of controls and risk-based cybersecurity processes within States and Urban Areas Security Initiative (UASI) metropolitan area governments.

House Report 111-298 for Public Law 111-83 directs "[the National Protection and Programs Directorate] (NPPD), in cooperation with the [Federal Emergency Management Agency] (FEMA) and relevant stakeholders, shall develop the necessary tools for all levels of government to complete a cyber network security assessment" in order to measure the gaps and capabilities of cybersecurity programs within States and local governments.

The responsibility for completing this mandate, known as the Nationwide Cyber Security Review (NCSR), has been delegated to DHS NCSD. NCSD will start this review as part of National Cyber Security Awareness Month on October 1, 2011 and will conclude on November 15, 2011.

Scope

NCSD seeks participation from Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and Chief Technology Officers (CTOs) from the 50 States, State agencies, 31 UASI areas, and other cities/counties/municipalities throughout the United States.

Methodology

The NCSR relies on six escalating categories of security control maturity. These levels of maturity are based on key milestone activities for information risk management. These milestones are closely aligned with security governance processes and maturity indexes embodied within ISO 27001 Information Security Management System, Control Objectives for Information Technology (CobIT), Statement on Auditing Standards Number 6 (SAS #6) and National Institutes of Standards and Technology (NIST) Special Publications 800 series methodologies for information security management and control.

Partners

NCSD has partnered with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the National Association of State Chief Information Officers (NASCIO) to develop and implement the NCSR.

MS-ISAC Multi-State Information Sharing & Analysis Center

NASCIO Representing Chief Information Officers of the States

Benefits of Participation

The NCSR is a no-cost review that delivers:

- An individualized report for each participant
- Recommendations to improve an organization's cybersecurity posture
- Metrics that may assist in cybersecurity investment justifications
- A benchmark to gauge year-to-year progress and to compare cybersecurity measures against peers

Participants will have access to the US-CERT Secure Portal, which includes:

- US-CERT 24x7 Secure Operations Center alerts
- Cybersecurity best practices
- Cybersecurity training resources

2011 NCSR

Located on the United States Computer Emergency Readiness Team (US-CERT) Secure Portal, the NCSR is designed to be completed in approximately one to two hours. All information provided by participants is safeguarded in accordance with the DHS Protected Critical Infrastructure Information (PCII) Program (www.dhs.gov/PCII).

The 2011 NCSR provides participants with instructions and guidance, and additional support is available through an NCSR helpdesk via the US-CERT Secure Portal.

Once complete, participants will have immediate access to an individualized report which measures the level of adoption of security controls within their organization and includes recommendations on how to raise the organization's risk awareness. After the review period, NCSD will aggregate all review data and share in-depth statistical analysis with all participants via the 2011 NCSR Summary Report. The names of participants and their organizations will not be identified in this report.

About DHS and NCSD

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. NCSD leads DHS's efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber or email NCSR@hq.dhs.gov.