# DEPARTMENT OF HOMELAND SECURITY:

# FALLING SHORT IN SECURING CYBERSPACE ON THE STATE AND LOCAL LEVEL

PREPARED BY THE HOUSE COMMITTEE ON HOMELAND SECURITY, DEMOCRATIC STAFF

January 2006

# DEPARTMENT OF HOMELAND SECURITY: FALLING SHORT IN SECURING CYBERSPACE ON THE STATE AND LOCAL LEVEL

Prepared by the Committee on Homeland Security, Democratic Staff
January 2006

Threats to our nation's security come in numerous forms and on multiple fronts. Our borders and ports must be secure from terrorist entry and criminal activity to keep the enemy away from our communities. Our food supply must be protected from field to fork from disease and sabotage. Our critical infrastructure – electrical grid, chemical and nuclear plants, dams, and numerous other locations – must be made safe. Yet, as we protect these and other basic elements of the American way of life, we cannot forget to protect the physical infrastructure and digital information that comprises our part of the global cyberspace.

Protecting the nation's cyberspace is a job tasked primarily to the Department of Homeland Security (Department), created in 2002 to consolidate federal agencies for the common purpose of improving national security. In addition to protecting federal cyber infrastructure, one of the Department's primary obligations in securing cyberspace is to provide assistance to state and local governments in identifying vulnerabilities in critical infrastructure and offer training and technical assistance in securing those vulnerabilities. Protecting state and local cyberspace is critical to achieving success in the field: state and local systems contain sensitive information, including personal data (like medical records, financial information, and proprietary business information), security-related data, and a wide range of other information that must be kept secure.

Unfortunately, a joint survey conducted by the National Association of State Chief Informational Officers (NASCIO) and the Metropolitan Information Exchange (MIX) released this week suggests the Department is falling short in fulfilling its basic obligations to state and local governments. Though the Department created several initiatives geared towards assisting and improving state and local protection, additional steps to improve training, communications, and coordination must be taken to achieve truly national cyber security. This analysis will describe the current federal and state responsibilities in securing cyberspace, summarize the findings of the NASCIO/MIX national survey, and suggest specific areas that the Department can improve to better assist state and local governments.

## The Federal Role in Protecting State and Local Government Cyberspace

The federal government maintains overall authority in providing training, ensuring the viability of state and local cyber strategies, and developing emergency recovery plans in the event of a cyber attack. In December 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), establishing a national policy for federal departments and agencies to identify and prioritize American critical infrastructure and key resources and to protect them from terrorist attacks. This policy specifically provides for the protection of critical infrastructure and key resources against terrorist acts that could undermine the capacity of state and local governments to

maintain order and to deliver minimum essential public services.[1] HSPD-7 confirms the federal role in protecting state and local resources laid out in the 2002 National Strategy for Homeland Security.[2]

The effort to protect national critical infrastructure is led by the Department of Homeland Security, which is responsible for developing plans to ensure the security of state and local cyberspace. The federal government has specific responsibilities regarding the coordination of the efforts to prevent damage, unauthorized use, exploitation, and enable the restoration of electronic information and communications systems and the information contained therein to ensure information confidentiality, integrity, and availability.[3] The Department is responsible for "providing specific warning information and advice about appropriate protective measures and countermeasures to state and local organizations."[4] The Department is also responsible for "providing technical assistance to state and local government with respect to emergency recovery plans for failures of critical information systems."[5]

To accomplish these goals, the Department encourages state and local governments to consider establishing IT security programs and to participate in ISACs with similar governments.[6] The following represents a partial list of these efforts:

- MS-ISAC – The Department launched a national cyber security awareness effort in partnership with the Multi-State Information Sharing and Analysis Center (MS-ISAC), an information sharing organization among representatives of state and local governments "that analyzes, sanitizes, and disseminates information pertaining to cyber events and vulnerabilities to its constituents and private industry through a series of conference calls and national web casts."[7]

- US-CERT – The Department established a US-CERT Portal to serve as a communication mechanism that allows the safe sharing of sensitive cyber-related information with government and industry members.

---

[1] Homeland Security Presidential Directive 7, Dec. 17, 2003.

[2] National Strategy for Homeland Security, July 2002, at 30. According to the National Strategy, "government and emergency services are considered critical infrastructure industries."

[3] Draft National Infrastructure Protection Plan, Appendix A: Cross-Sector Cyber Element, Nov. 2005, at 107.

[4] National Strategy to Secure Cyberspace, at ix.

[5] *Id.*

[6] *Id.* at 48.

[7] *Critical Infrastructure Protection: Department of Homeland Security faces Challenges in Fulfilling Cybersecurity Responsibilities*, Government Accountability Office, May 2005, at 31.

- Cybercop Portal – The Department facilitates and supports the Cybercop Portal, a group of more than 5,000 law enforcement members involved in electronic crimes investigations. Members represent all fifty states, working across all government agencies and more than forty countries. Members of the portal conduct a daily, secret-level conference call among multiple government agencies to discuss classified daily cyber intelligence data and increase information sharing among federal watch teams.

- InfraGard – In August 2005, the Department created an official Memorandum of Understanding with InfraGard, a Federal Bureau of Investigation (FBI) program designed to enhance information sharing and analysis efforts between the public and private sectors. With more than 11,000 active members across the country, InfraGard serves a key role in protecting the nation's infrastructure by serving as subject matter resources to local, state and Federal government and law enforcement agencies.

Though the federal government plays a key role in overseeing the security of state and local cyberspace and cyber infrastructure, state and locals are also responsible for developing specific plans to protect their own infrastructure. According to the Department's Draft National Infrastructure Protection Plan (NIPP),[8] state and local governments are responsible for two main areas:

- Managing the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that computer systems are not used to enable attacks against the nation's critical infrastructure.

- Establishing IT security programs, including awareness, audits, and standards.

## Survey Respondents Call for Department Improvements in Cyber Security

Though countless documents and strategies have delineated federal, state, and local roles in securing cyber infrastructure, a disconnect between the Department and the state and local governments is preventing state and local systems from achieving the highest levels of cyber security. To identify weaknesses in the federal/state/local relationship, NASCIO and MIX conducted a survey intended to identify the condition of state and local officials on cyber security and assess the nature of their relationship with the Department's cyber security programs and resources.[9] The results of the survey

[8] Draft National Infrastructure Protection Plan, Appendix A: Cross-Sector Cyber Element, Nov. 2005, at 109.

[9] The NASCIO survey was conducted from August 16-31, 2005. NASCIO invited responses from the chief information officers (CIO) or chief information security officers (CISO) of all fifty states and the District of Columbia. NASCIO garnered 27 responses from states representing 57% of the nation's population. The MIX survey was conducted from August 16-October 14, 2005. MIX invited responses from county and municipal chief information officers from dozens of the most populous cities and counties throughout the country, garnering 23 responses from jurisdictions representing 7% of the nation's population. This is referred to as the NASCIO/MIX survey because both surveys contain virtually identical language.

indicate that the Department must improve communications, training, alerting systems, and inter-governmental coordination to better assist state and local governments in securing cyberspace.

### A. *The Department Must Improve Communication with State and Local Information Officers*

The Department's greatest challenge is to improve outreach and communications efforts with state and local government officials. Though the Department is responsible for providing specific warning information and advice about appropriate protective measures to state and local organizations, over half of state officials and 85% of local officials told surveyors that they never asked for cyber security assistance from the Department.[10] On an encouraging note, many state officials who managed to contact the Department reported a positive experience; unfortunately, most local officials described significant dissatisfaction with the Department's response. Several state and local officials complained of the Department's non-responsiveness. As one state CISO summarized, "I'd like to see a much higher level of engagement between DHS and the States."[11]

The Department should better publicize the essential cyber strategies so that state and local officials are aware of the federal efforts underway. The Federal Information Security Management Act (FISMA), the National Strategy to Secure Cyberspace (National Strategy), and Homeland Security Presidential Directive 7 (HSPD-7) – all important documents and strategy guides in the Department's efforts in securing cyberspace – are surprisingly unfamiliar to many of the survey's respondents. For instance, when asked about their awareness of the Interim National Infrastructure Protection Plan (Interim NIPP), a majority of state officials were not "familiar" with the plan, though the NIPP is the base plan for protecting the nation's federal, state, and local cyber infrastructure.[12] The Department must do a better job of marketing and promoting these documents directly to the state and local information security officers, but beyond promotion, the Department should seek to ensure that the cyber security elements of each document can be extracted to form a coherent, actionable set of goals in terms of preparedness, response, and recovery from cyber incidents.[13]

Treating state and local officials as real partners in cyber security will go a long way towards addressing the confusion and frustration that state and local officers describe in dealing with the Department. State and local officials welcome a closer relationship

---

[10] Metropolitan Information Exchange, 2005 Strategic Cyber Security Survey (hereinafter MIX Survey) at 12; National Association of State Chief Information Officers, 2005 Strategic Cyber Security Survey (hereinafter NASCIO Survey), at 16-17.

[11] NASCIO Survey, at 19

[12] *Id.* at 5. Most officials placed themselves in either the "heard of it" or the "never heard of it" category, rather than the "familiar with it" category.

[13] *Id.* at 3.

with the Department: according to NASCIO's strategic recommendations, state information security officers "would gladly accept a closer relationship with the DHS, as opposed to the more detached, private-sector based approach that is in place."[14] To improve outreach, NASCIO recommends an aggressive and comprehensive approach to provide information and preparation to state and local officials.[15] At the least, the federal government needs to better market the major federal cyber security agencies and programs directly to the state and local CISOs. Providing these officials with items such as a regularly updated organizational chart of relevant federal entities would go far in improving the inter-governmental relationship between all involved.

### B. *The Department Should Create a More Comprehensive, Centralized Alert System*

The Department is responsible for providing "specific warning information and advice about appropriate protective measures and countermeasures to state and local organizations."[16] To achieve that goal, the Department created the United States Computer Emergency Readiness Team (US-CERT), a partnership between the Department and the public and private sectors. US-CERT coordinates defense against and responses to cyber attacks across the nation by analyzing and reducing cyber threats and vulnerabilities and disseminating cyber threat warning information.

But according to survey respondents, the Department's current efforts are duplicative and not as helpful as they could or should be. Many state and local officials requested that the Department improve its alert system coordination, specifically calling for a more centralized, comprehensive reporting and database center where all threats and potential threats are maintained and analyzed to show patterns or organized attempts of disruption.[17] A centralized status report of the level of threat on the Internet, as well as the tools to deal with that threat as quickly as possible, would be extremely helpful for those officials.[18]

As with the cyber strategies, the Department must do a better job publicizing its threat alert system to local officials. Though many state officials are familiar with US-CERT, a majority of local officials responded that they never used US-CERT, and only several respondents think US-CERT is "somewhat useful."[19] This stands in sharp contrast to respondent opinions about the SANS Institute/Internet Storm Center, where the overwhelming response was that the program is "definitely or somewhat useful." Not

[14] *Id.*

[15] MIX Survey, at 14.

[16] National Strategy to Secure Cyberspace at ix.

[17] NASCIO Survey at 19.

[18] MIX Survey at 15.

[19] *Id.* at 3.

only should the Department improve its marketing effort, but it should also consider creating a stronger command and control structure. NASCIO recommends creating a "cyber 911" phone number and portal that would make US-CERT's portal and help desk a true clearinghouse for all federal cyber security resources.[20]

Obviously, the long-standing impediments in information sharing that exist between the public and private sector must also be ironed out between the federal government and state and local governments. However, improving relationships and active intergovernmental communication will likely go a long way in mending these issues.

### C. *The Department Must Offer More High-Quality Training of State and Local Officials*

Adequate training of state and local officials will be critical in securing cyberspace. According to the President's National Strategy, the Department is responsible for providing "advice about appropriate protective measures and countermeasures to state and local organizations."[21] The Department is also responsible for "providing technical assistance to state and local government with respect to emergency recovery plans for failures of critical information systems."[22] But although efforts to train state and local officials are underway, the Department must continue to promulgate progressive practices, scenarios, and tools for conducting exercises as well as the lessons learned from them. Survey respondents requested that the Department provide more high-quality training and technical support, and some requested Department staff or consultants assist them in developing their cyber security program. Both local and state officials are interested in federally funded fellowships with the National Cyber Security Division (NCSD).[23]

Most state CISOs are confident in their ability to handle automated-external threats, but more emphasis needs to be placed on external-directed attacks as well as internal ineptitude and maliciousness. These are issues requiring specialized analysis, training and awareness, and procedures that could be better addressed by the various private-sector services providers as well as US-CERT, the MS-ISAC, CERT/CC, the Secret Service, the FBI Cybercrime Division, and InfraGard.

The Department should also identify and reward outstanding achievement on the state and local level. According to NASCIO, the federal government has undertaken several initiatives in partnership with research and academic communities to better educate and train future cyber security practitioners. However, the Department does not have any current program to recognize teams at the state and local government level, but

---

[20] NASCIO Survey at 3.

[21] National Strategy to Secure Cyberspace, at ix.

[22] *Id.*

[23] MIX Survey at13; NASCIO Survey at 18.

is open to collaborating with industry to identify recommendation. NASCIO recommends that the Department develop a "Cyber Security Excellence Award" to recognize teams at the state and local government level, rather than individuals.

### D. *The Department Should Improve MS-ISAC Coordination*

The Multi-State Information Sharing and Analysis Center (MS-ISAC) serves as an important source for state information officers and technology professionals to share information related to each state's cyber security readiness and resilience. Many of the state survey respondents listed the MS-ISAC as being critical in their response to and recovery from cyber attacks.[24] Though MS-ISAC is independent of the Department, US-CERT nevertheless has partnered with MS-ISAC and industry to develop web based training tools and a series of web casts, produced at no cost to the government. This initiative focuses on developing a series of national web casts that will examine critical and timely cyber security issues. These web-based training tools can be produced at no cost to government, as the web tools for online training and content for online training courses are usually provided by the private sector.

But in spite of these developing partnerships, the Department must continue to use the MS-ISAC to promote its own cyber security programs as well as to develop and promulgate best practices, consistent methodologies, and tools for a variety of needs (e.g., Carnegie Mellon's OCTAVE), including risk assessments, continuity of operations planning, training, exercises, and contracting alliances. The Department must also encourage the sector ISACs to promulgate progressive practices, templates, and assessment tools for developing and benchmarking information security programs.[25] Finally, the Department should encourage local participation in the MS-ISAC. Over 80% local officials surveyed reported that they never used the MS-ISAC.[26] The Department must improve its publicity and marketing efforts to ensure that more local officials are utilizing the threat information available from MS-ISAC.

### E. *The Department and NCSD Must Help Incorporate Cyber Security into the SHSAS Process*

States currently applying for homeland security grant funding should be required to provide evidence of their use of cyber risk assessments. As it stands now, the cyber security component of the State Homeland Security Assessment and Strategy (SHSAS) process does not require a cyber assessment from each state. Ideally, evidence of the assessments will ensure that cyber security is adequately considered at the federal, state, and local levels.

---

[24] NASCIO at 16.

[25] *Id.* at 4.

[26] MIX Survey at 4.

Though the Office of State and Local Government Coordination and Preparedness (ODP) maintains authority over this issue, the National Cyber Security Division (NCSD) should encourage ODP to obtain this information from the states (and pressure those states who have not developed cyber assessments) in order to better understand the level of preparedness on cyber threat.

### F. *The Department Should Encourage State and Local Continuity of Operations Exercises*

One of the Department's major responsibilities in the field of cyber security is to provide "technical assistance to state and local government with respect to emergency recovery plans for failures of critical information systems."[27] Fortunately, many survey respondents reported that they have developed an IT-oriented continuity of operations plan intended to help maintain order and deliver minimum essential public services and emergency services in the event of a major cyber/physical attack or disaster. However, respondent comments indicate that while many state and local plans may exist, more training is necessary to ensure a timely and effective response in the event of cyber failures. Many respondents stated that although draft plans were either complete or "under development with initial components complete," a majority of those surveyed indicated that they had not been able to test the continuity of operations plan in an exercise that included responses to cyber and physical disruptions.[28] Simulations and testing are extremely important in order for efficient and effective response in the event of a disaster. The Department should continue to conduct more frequent and wider ranging cyber and TOPOFF-type exercises, which will help refine the cyber-exercise methodology and produce information to share with all of the information security officers at the conclusion of the exercise.[29]

### G. *The Department Should Seek More Funding of the NCSD*

Though the Congress and the President claim that cyber security is a pressing issue, relatively low funding levels at the Department show otherwise. In 2005, Congress appropriated $870 million to the Department's Information Analysis and Infrastructure Protection Directorate, which is responsible for cyber security and critical infrastructure protection. Of that money, however, cyber security efforts received $73.3 million.[30]

State and local officials responding to the NASCIO/MIX survey listed lack of funding for their initiatives as one of the biggest obstacles towards achieving security in cyberspace. As one survey respondent commented, "I am disheartened by how few people are willing to acknowledge and provide funding for cyber security related

[27] National Strategy to Secure Cyberspace at ix.

[28] NASCIO Survey at 14.

[29] *Id.* at 6.

[30] Federal Computer Week, Jul. 25, 2005.

issues."[31] Many of the local information officers remain concerned about obtaining funding to implement new federal laws. One local official requested that the Department "provide funding for any new laws or mandates that implements new information security and privacy policies that are imposed on local government for implementation."[32] The Department would be well-served to address issues of funding and work with state and local officials to achieve a mutually agreeable solution.

## Summary

Though the Department is taking positive steps in protecting the nation's cyberspace, the NASCIO/MIX survey indicates that the Department must improve training, funding, and intercommunication efforts between the federal, state, and local governments in order to secure our national cyberspace. Fortunately, many of these recommendations can be initiated by the Department utilizing existing vehicles, rather than requiring reinvention of the Department.

According to NASCIO, for instance, the existing efforts of InfraGard and the Multi-State ISAC provide "an underutilized foundation upon which to promote existing Department cyber security programs as well as to develop and promulgate best practices, consistent methodologies, risk assessments, continuity of operations planning, training, exercises, and contracting alliances."[33] Because most states participate in the MS-ISAC, the Department can utilize this portal to communicate with information officers across the country to answer questions, offer solutions, and work with officials to develop practical resolutions.

We encourage the Department to work within its structure to find ways to better assist state and local governments in meeting their cyber security objectives. The current state of interaction between state and local information officers and the federal government is not acceptable. An effort by the Department to promote and publicize its key cyber documents, offer high quality training to state and local officials, and create a budget that reflects its priority towards securing state and local cyberspace will go far in achieving the national cyber security that all Americans desire.

[31] NASCIO Survey at 19.

[32] MIX Survey at 14.

[33] NASCIO Survey at 3.