DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

Letter Report:

DHS Needs to Prioritize Its Cyber Assets

OIG-08-31

March 2008

Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 26, 2008

MEMORANDUM FOR: Elaine C. Duke
Acting Undersecretary for Management

Richard L. Skinner

FROM: Richard L. Skinner
Inspector General

SUBJECT: *Letter Report: DHS Needs to Prioritize Its Cyber Assets*

We initiated an audit to determine the Department of Homeland Security's progress in identifying and prioritizing its internal cyber critical infrastructure in accordance with Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*. This directive established a national policy for the federal government to identify, prioritize, and protect United States critical infrastructure, including the internal critical assets used by each department.

The department has not completed all the steps to produce a prioritized inventory of its internal cyber critical infrastructure. Further, the department's Management Directorate was not coordinating related efforts to secure these assets. We recommend that the department designate a specific office to determine protection priorities for its internal cyber critical infrastructure. Additionally, the department should develop a process to coordinate internal efforts to protect these assets in accordance with Homeland Security Presidential Directive 7.

We hope our recommendations will be of assistance as you move forward to implement actions to protect the department's internal cyber critical infrastructure and key resources. Should you have any questions, please call me, or your staff may contact Frank Deffer, Assistant Inspector General, Information Technology, at (202) 254-4100.

Background

Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003, established a national policy to identify and prioritize critical infrastructures. These critical infrastructures are both physical and cyber-based, and span all sectors of the economy. According to the National Infrastructure Protection Plan (NIPP), June 2006,

> Cyber infrastructure includes electronic information and communications systems, and the information contained in those systems. Computer systems, control systems…and networks such as the Internet are all part of cyber infrastructure.

Further, HSPD-7 references the *USA Patriot Act of 2001* (Public Law 107-56) to define the term "critical infrastructure" as those:

> …systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The Department of Homeland Security (DHS) planned to determine protection priorities for its internal cyber critical infrastructure using the Project Matrix methodology. Project Matrix is a systematic approach that seeks to discover the domino or cascading effects of the loss of critical functions and services. This is accomplished through an understanding of how these functions and services are provided and the impact of the loss should it occur. This approach was designed to assist the department in identifying and prioritizing critical functions and services performed by DHS in support of national security, economic stability, and public safety.

According to the *ISSM Guide to the DHS Information Security Program*, Version 2.0, July 19, 2004, the DHS Continuity Planning Program Director is responsible for Project Matrix and reports to the DHS Chief Information Security Officer (CISO).

DHS Needs To Determine Protection Priorities for its Internal Cyber Critical Infrastructure

HSPD-7 established a national policy for federal departments and agencies to identify and prioritize their critical cyber infrastructure. In compliance with HSPD-7, DHS uses an enterprise management tool, Trusted Agent FISMA, to identify its high-risk systems. However, DHS has not determined which of these high-risk systems must be given priority when allocating protection resources.

For example, according to *DHS 4300A Sensitive Systems Handbook*, restoration priorities are to be based on DHS mission criticality. DHS plans for restoring critical systems following a service disruption or disaster include the establishment of the National Center for Critical Information Processing and Storage (NCCIPS). This center is to host departmental applications, network connectivity, and critical data storage. Additionally, the NCCIPS and a second data center, yet to be established, are to have "active – active" processing capability to ensure each mission critical system has a complete disaster recovery capability. However, the current DHS schedule for migrating systems to the NCCIPS is not based on system criticality, but instead is based on which component can fund the migration of a system. As a result, DHS may not be providing a secure processing and backup facility for its most critical systems.

For prioritization purposes, the most significant assets fall within the nationally critical category. These nationally critical assets are considered necessary for the daily operation of the federal government. Project Matrix is a methodology that would allow DHS to set protection priorities across the department, and thus determine which cyber assets are nationally critical. For example, a nationally critical function of DHS is to identify, examine, and inspect all high-risk cargo and passengers. Project Matrix Step 1 lists those nationally critical cyber systems, including the Automated Commercial Environment (ACE), that support this function. In accordance with HSPD-7, DHS should place a higher protection priority on nationally critical systems, such as ACE, than it places on systems that do not support a nationally critical function.

Within the department, the CISO has responsibility for Project Matrix. In November 2003, the DHS CISO obtained Project Matrix contract support at a cost of approximately $1.97 million. Step 1 of Project Matrix was to produce a rank ordered list of critical functions and services. In November 2005, the DHS CISO cancelled the Project Matrix support contract after obtaining only 15 of 18 (79%) Project Matrix Step 1 reports from DHS components.[1] Further, in August 2007, the DHS CISO eliminated the section of the *DHS 4300A Sensitive Systems Handbook* that detailed the responsibilities of the Office of the DHS Chief Information Officer, and the DHS CISO related to HSPD-7 and Critical Infrastructure Protection.

The DHS CISO said that he canceled the contract and removed the section from the handbook because Project Matrix was not mentioned as a requirement in HSPD-7.

[1] The Office of Inspector General, Science and Technology Directorate, and the National Cyber Security Division did not submit Project Matrix Step 1 reports.

However, when these responsibilities were removed from DHS guidance, no DHS office was given the responsibility to identify and prioritize internal critical infrastructure assets.

According to HSPD-7,

> All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources.

DHS could improve its ability to identify and prioritize its internal cyber critical infrastructure by assigning an office with this responsibility. The absence of this assigned responsibility hinders DHS' ability to ensure that its most critical assets are prioritized for protection.

Better Coordination Needed on DHS HSPD-7 Related Efforts

The effectiveness of HSPD-7 implementation could be improved if staff from the Office of Security and the CIO synchronized their respective efforts to provide prioritized protection for internal cyber critical infrastructure. Specifically, the Office of Security is not adequately coordinating HSPD-7 related activities with the CIO.

In compliance with HSPD-7, DHS issued the Government Facilities Sector Plan.[2] However, CIO staff said that they were unaware that this plan was issued. This occurred because the Chief Security Officer, as the DHS representative to this government coordinating council, did not distribute the Government Facilities Sector plan to the CIO. Further, Office of Security staff did not invite CIO staff to a planning meeting to discuss the impact that cyber security has on the Government Facilities Sector.

According to HSPD-7,

> Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them.

Ineffective coordination could cause plans for protecting internal cyber critical infrastructure to be incomplete. For example, Office of Security is responsible for physical security of facilities. The physical security provided may need to be reassessed if the facility contains DHS internal cyber critical infrastructure.

[2] *Government Facilities – Critical Infrastructure and Key Resources as input to the National Infrastructure Protection Plan*, May 2007.

Recommendations

We recommend that the Undersecretary for Management take the following actions for activities related to the management of internal cyber critical infrastructure:

Recommendation #1: Assign responsibility and provide the necessary resources to determine protection priorities for the Department's internal cyber critical infrastructure.

Recommendation #2: Develop a process to coordinate the DHS internal cyber critical infrastructure protection activities among the Line of Business Chiefs.

Management Comments and OIG Analysis

We obtained written comments on a draft of the report from the Deputy Undersecretary for Management. We have included a copy of the comments in Appendix A. The Deputy Undersecretary concurred with both recommendations; however, she suggested that they should be reworded for clarity. We reviewed the Deputy Undersecretary for Management's suggestions and made changes where appropriate.

****

We conducted our audit from August 2007 to March 2008 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government audit standards.

Appendix A
Management Response

Under Secretary for Management
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

MAR 0 6 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Elaine C. Duke
Deputy Under Secretary for Management

SUBJECT: *Letter Report: DHS Needs to Prioritize Its Cyber Assets*

Thank you for your memorandum dated January 31, 2008, regarding Office of the Inspector General draft letter report entitled, *DHS Needs to Prioritize Its Cyber Assets*. Your memorandum noted the following two recommendations:

- "Assign responsibility and provide the necessary resources to determine protection priorities for its internal cyber critical infrastructure."
- "Develop a process to coordinate the DHS internal cyber critical infrastructure protection activities of the Management Directorate offices."

I agree with both recommendations. However, I suggest they be worded as follows for clarification:

- "Assign responsibility and provide the necessary resources to determine protection priorities for the Department's internal critical infrastructure, including critical cyber infrastructure."
- "Develop a process to coordinate the DHS internal critical infrastructure protection activities among the Line of Business Chiefs."

The Chief Administrative Officer is assigned the responsibility to manage the business continuity and mission assurance functions and will have the lead for implementing these recommendations.

Appendix B
Major Contributors to This Report

Roger Dressler, Director, Department of Homeland Security, Information Technology Audits

Kevin Burke, Audit Manager, Department of Homeland Security, Information Technology Audits

Matthew Worner, Program Analyst, Department of Homeland Security, Information Technology Audits

Domingo Alvarez, Senior IT Auditor, Department of Homeland Security, Information Technology Audits

Beverly Dale, Senior IT Auditor, Department of Homeland Security, Information Technology Audits

Syrita Morgan, Management and Program Assistant, Department of Homeland Security, Information Technology Audits

Samer El-Hage, Management and Program Assistant, Department of Homeland Security, Information Technology Audits

Tarsha Cary, Referencer

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Under Secretary, Management
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Chief Information Officer
Chief Information Security Officer
DHS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**
  DHS Office of Inspector General/MAIL STOP 2600, Attention:
  Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.