

# DEPARTMENT OF HOMELAND SECURITY

## Office of Inspector General

Challenges Remain in Securing the Nation's  
Cyber Infrastructure



*Office of Inspector General*

**U.S. Department of Homeland Security**  
Washington, DC 20528



**Homeland  
Security**

June 5, 2007

### Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the strengths and weaknesses of the National Cyber Security Division's implementation of its mission to coordinate security of the nation's cyber infrastructure. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, technical scans, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner  
Inspector General

# Table of Contents/Abbreviations

---

|  |           |
|--|-----------|
| Executive Summary .....  | 1         |
| Background.....  | 2         |
| Results of Audit .....   | 4         |
| <b>Progress Made In Securing Cyberspace .....</b>  | <b>4</b>  |
| <b>Better Management of Strategic Plan Is Needed .....</b>   | <b>5</b>  |
| Establish Priorities to Ensure Critical Tasks Are Completed .....  | 5         |
| NCSD Needs to Improve the Monitoring of Its Milestones .....   | 6         |
| Recommendations .....  | 7         |
| Management Comments and OIG Analysis.....  | 8         |
| Better Defined Performance Measures Are Needed .....   | 8         |
| Recommendation .....   | 10        |
| Management Comments and OIG Analysis.....  | 10        |
| Expanded Incident Reporting Analysis Will Improve Identification and Response<br>to Cyber Incidents .....  | 11        |
| Recommendations .....  | 13        |
| Management Comments and OIG Analysis.....  | 13        |
| <b>Improved Information Sharing and Communications Will Enhance Cyber<br/>Infrastructure Security.....</b> | <b>14</b> |
| Recommendations.....   | 17        |
| Management Comments and OIG Analysis .....   | 18        |
| <b>Revised Certification and Accreditation Will Satisfy FISMA Requirements.....</b>                        | <b>19</b> |
| Recommendations.....   | 21        |
| Management Comments and OIG Analysis .....   | 22        |

## Appendices

|   |    |
|---|----|
| Appendix A: Purpose, Scope, and Methodology .....           | 24 |
| Appendix B: Management Comments to the Draft Report .....   | 26 |
| Appendix C: NCSD Major Functions and Responsibilities ..... | 35 |
| Appendix D: Federal Agency Incident Categories .....        | 37 |
| Appendix E: Major Contributors to this Report .....         | 38 |
| Appendix F: Report Distribution.....                        | 39 |

# Table of Contents/Abbreviations

---

## Abbreviations

|         |   |
|---------|---|
| CS&C    | Cyber Security and Communications               |
| CS&T    | Cyber Security and Telecommunications           |
| DHS     | Department of Homeland Security                 |
| FISMA   | Federal Information Security Management Act     |
| IT      | Information Technology                          |
| NCSD    | National Cyber Security Division                |
| NIST    | National Institute of Standards and Technology  |
| OIG     | Office of Inspector General                     |
| OMB     | Office of Management and Budget                 |
| PART    | Program Assessment Rating Tool                  |
| US-CERT | United States Computer Emergency Readiness Team |

## **Executive Summary**

We audited the National Cyber Security Division to determine whether: (1) it is working collaboratively with the public, private, and international entities to secure cyberspace and cyber assets; (2) it is effectively managing the implementation of *The National Strategy to Secure Cyberspace*; and (3) security controls were effectively implemented on two mission support systems (Einstein and Cybercop Portal).

Since our last review in 2004, the National Cyber Security Division has taken actions to further implement *The National Strategy to Secure Cyberspace*. For example, the division has established a fully operational incident handling center (United States Computer Emergency Readiness Team). The National Cyber Security Division has put into action programs that promote cyber security awareness among the public and private sectors; improve vendor software development and reduce vulnerabilities; develop and promote sound practices and standards that enhance cyber security; promote a global culture of security through international outreach awareness; promote and facilitate the development of adequately trained information technology professionals; and plan, coordinate, and conduct cyber exercises with the public and private sectors to improve cyber security readiness, protection, and incident response capabilities. The National Cyber Security Division has established working groups and participated with public and private sector organizations to share information and protect cyberspace and cyber assets.

While the National Cyber Security Division has made progress in meeting its mission, it can improve its efforts to secure the nation's cyber infrastructure. Specifically, the division has not (1) established priorities to ensure that its mission-critical tasks supporting its programs are completed timely; (2) developed enhanced performance measures that can be used to evaluate the effectiveness in meeting its mission; (3) fully developed its information sharing and communications programs with the private sector; (4) developed and implemented enhanced procedures to ensure that all known cyber incidents from across the federal government are being reported; and (5) ensured that its support systems comply with all *Federal Information Security Management Act* requirements, including testing of contingency plans.

We are making 14 recommendations to the Assistant Secretary for Cyber Security and Communications (CS&C). CS&C has already begun to take actions to implement 13 of the recommendations. CS&C's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

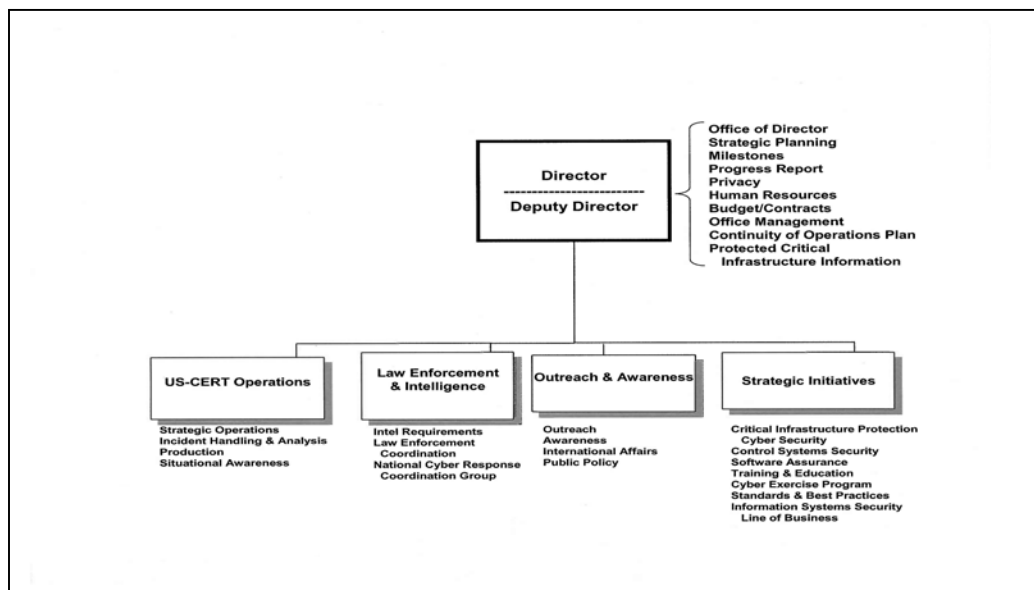
---

## Background

The Department of Homeland Security (DHS) established the National Cyber Security Division (NCSA) in June 2003 to serve as a national focal point for addressing cyber security issues and to coordinate implementation of the cyber security strategy in the United States. NCSA's mission is to work collaboratively with public, private, and international entities to secure cyberspace and cyber assets, and to implement the actions and recommendations of *The National Strategy to Secure Cyberspace*.<sup>1</sup>

In September 2006, the first Assistant Secretary for Cyber Security and Telecommunications (CS&T) was appointed within the Preparedness Directorate, which includes NCSA.<sup>2</sup> NCSA reports to the Assistant Secretary and is headed by the Office of the Director and comprises four branches: United States Computer Emergency Readiness Team (US-CERT) Operations, Law Enforcement and Intelligence, Outreach and Awareness, and Strategic Initiatives. In October 2006, a new NCSA Acting Director was named and who later became the Director in January 2007. As of December 2006, NCSA had a staff of 107 (31 federal employees, 4 detailees, and 72 contractors). See Figure 1 for an organization chart and Appendix C for the major functions and responsibilities of each branch.

Figure 1 – NCSA Organization Chart



---

<sup>1</sup> The White House issued *The National Strategy to Secure Cyberspace* in February 2003.

<sup>2</sup> On March 31, 2007, CS&T was renamed Office of Cyber Security and Communications and the Preparedness Directorate was renamed the National Protection and Programs Directorate.

---

US-CERT is the operational arm of NCS&D and is charged with protecting the nation's Internet infrastructure by coordinating defense against and response to cyber attacks. In addition, US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber trend and analysis information, and coordinating incident response activities. US-CERT interacts with federal agencies, the information technology (IT) industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

NCS&D has worked collaboratively with the private and public sector partners to develop the IT Sector-Specific Plan. The final draft of this document was completed in December 2006. The IT Sector-Specific Plan provides a foundation for sector planning activities to manage risk and to improve situational awareness, response, recovery, and reconstitution of the nation's IT infrastructure. These improvements, which can be accomplished through the public and private sectors, will enhance national capabilities. The IT Sector-Specific Plan identifies near-term (less than 1 year) and long-term (1 to 3 years) actions that require collaborative efforts between and among the private sector, state and local governments, non-governmental organizations, and the federal government.

CS&T produced a strategy report, in December 2006, for the DHS Secretary that provides a comprehensive overview of its organization. The report lists stakeholders' expectations, CS&T's capabilities, current initiatives, gaps between stakeholder expectations and the organization's capabilities and programs, strategic priorities, and actions to support the mission over the next 2 years.

In July 2004, we reported that NCS&D had begun to implement the actions and recommendations detailed in *The National Strategy to Secure Cyberspace*.<sup>3</sup> We noted that NCS&D faced a number of challenges to address long-term cyber threats and vulnerabilities to the nation's critical infrastructure. Specifically, we found that NCS&D had not:

- Prioritized its initiatives to address the recommendations in *The National Strategy to Secure Cyberspace*.
- Identified the resources needed to ensure that it could identify, analyze, and reduce long-term cyber threats and vulnerabilities.
- Developed strategic implementation plans, including performance measures and milestones, focusing on the division's priorities, initiatives, and tasks.

---

<sup>3</sup> *Progress and Challenges in Securing the Nation's Cyberspace* (OIG-04-29, July 2004).

- 
- Instituted a formal communications process within DHS, as well as the public, private, and international sectors.
  - Initiated and implemented a process to oversee and coordinate efforts to develop best practices and create cyber security policies with other government agencies and the private sector.

NCSD has taken corrective actions to develop strategic implementation plans, institute a formal communications process, and oversee and coordinate efforts to develop best practices and security policies. However, other recommendations remain open and are addressed in this report.

## Results of Audit

### Progress Made In Securing Cyberspace

NCSD has made progress in its cyberspace security efforts. Specifically, NCSD established a fully operational, incident-handling center (US-CERT) to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of the nation's cyber infrastructure. In addition, NCSD has established working groups and participated with public and private sector organizations to share information and protect cyberspace and cyber assets.

NCSD also has put into action programs to address the recommendations in *The National Strategy to Secure Cyberspace*. For example:

- The Outreach and Awareness program was established to promote cyber security awareness among and within the public and private sectors, maintain relationships with governmental cyber security professionals to coordinate and share information about cyber security initiatives, and develop partnerships to promote coordination and collaboration on cyber security activities.
- The Software Assurance program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve capabilities to develop and deploy trustworthy software products.
- The Standards and Best Practices program promotes and sponsors the development of standards, guidance documents, metrics, and tools that raise awareness and encourage the implementation of cyber security practices and processes.
- The International Affairs program was established for NCSD to engage in international outreach activities to build awareness about the global cyber risk, share information about the role and activities of

**Challenges Remain in Securing the Nation's Cyber Infrastructure**



---

computer security incident response teams, and build relationships among governments toward global cooperation on cyber security.

- The Training and Education program promotes and facilitates the development of adequately trained information technology professionals to support the Nation's cyber security needs via effective training, education, and certification programs.
- The Cyber Exercise program plans, coordinates, and conducts cyber exercises with the public and private sectors as a mechanism for NCSD to improve cyber security readiness, protection, and incident response capabilities.

The implementation of these programs helps NCSD fulfill its mission to partner with the public and private sectors to prevent, minimize, prepare for, and respond to threats to critical IT infrastructure. However, as discussed in the following sections, improvements are needed in NCSD's efforts to implement *The National Strategy to Secure Cyberspace*.

### **Better Management of Strategic Plan Is Needed**

NCSD has not effectively managed its strategic plan to ensure that critical tasks are completed timely. Specifically, NCSD has not prioritized key activities for the division or established effective performance measures to monitor the division's progress in accomplishing its mission and goals. In addition, NCSD needs to improve its incident reporting analysis in order to identify and reduce underreporting by federal agencies. Until NCSD implements its critical strategic initiatives, including the reporting of all cyber incidents and monitoring its progress with effective performance measures, the division cannot ensure that it can partner successfully with the public and private sector to prevent, minimize, prepare for, and respond to threats to critical IT infrastructure.

#### **Establish Priorities to Ensure Critical Tasks Are Completed**

NCSD has undertaken steps to address the recommendations proposed in *The National Strategy to Secure Cyberspace*. However, in addressing the recommendations, NCSD has not prioritized specific initiatives, taking into consideration the required resources to ensure the timely completion of its initiatives. As a result, many of NCSD's initiatives are not complete and the progress to date has been limited.

While NCSD has begun many initiatives to address the recommendations proposed in *The National Strategy to Secure Cyberspace*, many of its efforts lacked specific timeframes for completion. NCSD personnel said that each of

---

the actions outlined in the division's draft Strategic Plan, dated May 2006, and all of the program plans developed by its branches that support it, are a "priority." We determined that these actions had not been prioritized based on NCSD management goals or available resources.

Certain critical programs that were established to implement recommendations from *The National Strategy to Secure Cyberspace* will not be completed for another 2 or more years. For example, the Control Systems Security Program, the goal of which is to guide a cohesive effort between government and industry and reduce the risk to critical infrastructure control systems, is not expected to complete its roll out until FY 2009. Additionally, the computer forensics laboratory, that will train government security personnel to become specialized in multiple forensic areas, is not expected to be fully operational until FY 2009, but will begin initial training in the fall of 2007.

In addition, some members of the National Cyber Response Coordination Group, the IT-Information Sharing and Analysis Center, and the IT-Sector Coordinating Council expressed their concerns that NCSD has too many priorities for the available resources provided to the division. Some group members also expressed concerns that NCSD was not working on initiatives that are currently needed. For example, members cited the need for smaller cyber exercises in addition to the larger scaled one previously held or the creation of operational recovery plans in the event of a major cyber incident. Group members believed that these concerns became more critical with the issuance in December 2006 of the IT-Sector Specific Plan. This plan listed over 70 short and long-term actions, many needing NCSD assistance, which need to be completed within the next 3 years. In addition, the CS&T Strategy report, issued in December 2006, identified strategic priorities and actions that are to be accomplished within the next 2 years. Taken in total, the number of existing and new actions required of NCSD is significant and could overextend the capabilities of the division if not prioritized and properly resourced.

### **NCSD Needs to Improve the Monitoring of Its Milestones**

NCSD's monitoring of its program initiatives needs improvement. NCSD has not established a process to monitor and manage effectively the division's current milestones and deliverables. As a result, it is difficult for management to monitor efforts of the division in completing its initiatives and determining whether they are on schedule, ahead of schedule, or behind schedule.

NCSD has not consolidated tracking all of the division's milestones and deliverables. NCSD produced a draft Strategic Plan in May 2006, which details its actions and milestones to accomplish the division's goals. To

---

support the Strategic Plan, NCS D staff developed ten program plans that include milestones for major deliverables and actions. Program plans list the overview of the program, goals, milestones, performance measures, resources, and challenges. In addition, NCS D management uses quarterly Program Assessment Rating Tool (PART) reports to track milestones that have been completed during the quarter. PART is a diagnostic tool that the Office of Management and Budget (OMB) uses to assess the performance of programs and to drive improvement in program performance. OMB defines three categories of performance measures: (1) outcome-the intended result of carrying out a program or activity (value added), (2) output-the level of activity that will be provided over a period of time, and (3) efficiency-the ratio of the outcome or output to the input of any program. The PART report only identifies tasks or milestones that have been met. It does not identify or explain delays.

The Strategic Plan and the individual program plans do not associate resource requirements to the achievement of deliverables and milestones. In addition, four of the ten program plans reviewed did not contain information as to interim milestones. For example, some milestones were listed as “ongoing,” “FY 2007,” “FY06-FY10,” or “FY06-FY10 Planned.” These types of milestones do not allow NCS D management to monitor effectively the incremental progress of its initiatives and evaluate whether the program goals have been achieved. Interim milestone dates are often needed to manage incremental progress for activities that can take years to complete in their entirety. We also found instances where some milestones were reported in the program plans as complete, but were not reported on the PART report.

The sophistication and effectiveness of cyber attacks have steadily advanced in recent years. Therefore, to improve its ability to address these threats, it is imperative that NCS D prioritize its initiatives based upon available resources and criticality as determined by management. Without establishing priorities, NCS D cannot ensure that critical initiatives and milestones are accomplished on schedule and in a timely manner. Improving the monitoring of its milestones will allow NCS D the ability to better guide and track the division’s activities in implementing the recommendations outlined in *The National Strategy to Secure Cyberspace*.

## **Recommendations**

We recommend that the Assistant Secretary for CS&C direct the NCS D Director to:

**Recommendation #1:** Establish priorities and milestones (short term and long term) for critical tasks using input from the CS&T Strategy Summary report,

---

IT-Sector Specific Plan, and *The National Strategy to Secure Cyberspace*. Milestones should be based on available funding and resources.

**Recommendation #2:** Consolidate the tracking of all current and future initiatives and milestones, and review at least quarterly.

## **Management Comments and OIG Analysis**

CS&C concurred with recommendation 1. CS&C plans to address its strategic priorities through short and long term actions over the course of the next 2 years and beyond. NCS D's implementation plan and detailed program plans, which are mapped to CS&C's priorities, contain its goals and priorities. To improve performance management within its new organizational structure, CS&C is in the process of defining additional performance measures and milestones that tie into NCS D's mission, priorities, processes, and available resources. In addition, CS&C has scheduled its first quarterly review to evaluate NCS D's progress in terms of priorities developed by the Assistant Secretary for CS&C, current funding, and anticipated funding for Fiscal Year 2008.

We agree that the steps that CS&C has taken, and plans to take, satisfy this recommendation.

CS&C did not concur with the finding that resulted in recommendation 2. In disagreeing with the finding that NCS D needs to improve the monitoring of its milestones, CS&C indicated that NCS D monitors its milestones and performance based upon its strategic plan and updates its program plans each quarter. In addressing our recommendation, NCS D is revising its strategic plan with a comprehensive implementation plan and updated program plans to track actions, milestones, and resources. NCS D will report quarterly to CS&C on accomplishments and deliverables mapped to programmatic actions, milestones and resource allocations, identifying anticipated potential shortfalls and remedial actions.

We believe that the steps that NCS D has taken, and plans to take, satisfy this recommendation to consolidate the tracking of all current and future initiatives and milestones and review them quarterly.

### **Better Defined Performance Measures Are Needed**

NCS D has not developed effective performance measures needed to monitor the division's success in accomplishing its mission and goals. Without such measures, NCS D will have difficulty in determining how effective its

---

initiatives are in achieving significant results in strengthening the nation's cyber security.

Performance measures are the indicators or metrics that are used to gauge program performance. Furthermore, performance measures should address the direct products and services delivered by a program (outputs), and the results of those products and services (outcomes). Outcomes are important, as they often describe the intended result or consequence that will occur from carrying out a program or activity. For example, an outcome goal might be to reduce the time it takes to disseminate cyber threat warning by FY 2008. Therefore, outcomes are of direct importance to beneficiaries and the public. While performance measures must distinguish between outcomes and outputs, there must be a reasonable connection between them, with outputs supporting (i.e., leading to) outcomes in a logical fashion.

NCSD has developed performance measures based on OMB's PART metrics: output, outcome, and efficiency. NCSD branches report to OMB the status of their metrics on a quarterly basis. To monitor branch progress, NCSD identified three performance measures:

- Number of cyber security products delivered to key stakeholders (output).
- Percent of targeted stakeholders who participate in or obtain cyber security products and services (outcome).
- Percent of completion of key milestones and accomplishments (efficiency).

We determined that NCSD has not developed sufficient outcome performance measures to ensure that its programs are achieving the intended results and impact, i.e., secure cyberspace and reduce security vulnerabilities. For instance, NCSD developed performance measures that emphasize "quantity" (number of newsletters issued, number of people attending conferences or workshops), but has not developed measures to evaluate the "quality" of its products and services. For example, outcomes that measure the effect newsletters or conferences have on the cyber community, the number of vulnerabilities reduced, or the usefulness of the information or service to the public have not been established.

In addition, since one of NCSD's performance measures is the percent of completion of key milestones, it is important that target completion dates be established for all milestones and deliverables in order to monitor the performance and progress of the branches. For example, some of the milestones in the individual program plans were listed as "ongoing" or "FY06-FY10." Additionally, one of the goals of the Outreach and Awareness

---

branch is to maintain relationships with governmental cyber security professionals in order to share information about cyber security initiatives, and develop partnerships to promote collaboration on cyber security preparedness issues. Performance measures and milestones that would evaluate its success have not been developed.

According to OMB guidance, performance measures are developed to monitor a program's accomplishments and determine whether results are being achieved. Establishing performance measures also keeps program partners focused on the key goals of a particular initiative. Performance measures must reflect a program's mission and priorities, be few in number, and should reflect direct outcomes. In some cases where the outcome of a program may not be realized for many years, a program should define specific short- and medium-term steps or milestones to accomplish the long-term outcome performance goals. Appropriate performance goals should include performance measures and targets, outcomes, and annual and long-term measures and targets.

## **Recommendation**

We recommend that the Assistant Secretary for CS&C direct the NCSA Director to:

**Recommendation #3:** Develop additional performance measures for each branch that can be used to review and periodically evaluate the outcome or success of the division's programs.

## **Management Comments and OIG Analysis**

CS&C did not concur with the finding that resulted in recommendation 3. In disagreeing with the finding that better defined performance measures are needed, CS&C indicated that NCSA developed and began collecting internal program level measures to improve the ability to assess overall programmatic progress in the third quarter of Fiscal Year 2006. In addressing our recommendation, NCSA recently developed revised PART measures to cover all of its programs. NCSA is regularly evaluating its metrics and strives to improve them.

We believe that the steps that NCSA has taken, and plans to take, satisfy this recommendation to develop additional performance measures.

---

## **Expanded Incident Reporting Analysis Will Improve Identification and Response to Cyber Incidents**

US-CERT is not performing detailed analysis to ensure that all incidents are being received from all federal agencies.<sup>4</sup> Less than complete reporting hampers the government's ability to know whether an incident is isolated at one agency or is part of a larger event (widespread propagation of an Internet worm) and thus complicates and delays appropriate response, such as distributing security patches or other compensating controls.

Security incidents are reported to US-CERT either through OMB-mandated incident reports from federal agencies or incident reports submitted voluntarily by state, local, and tribal governments, as well as private sector organizations. In addition, US-CERT monitors real-time network traffic from selected Internet access points to detect suspicious activities for those federal agencies that are participating in the Einstein program. The Einstein program is an initiative that builds cyber-related situational awareness across the participating federal agencies. Specifically, the Einstein program employs an automated tool to monitor government agencies' network traffic to facilitate the identification and response to cyber threats and attacks, improve network security, increase the resiliency of critical electronically delivered government services, and enhance the survivability of the Internet. The Einstein program helps agencies identify baseline network traffic patterns, configuration problems, unauthorized network traffic, network backdoors, routing anomalies, and network scanning activities.

Federal agencies are required to follow US-CERT's Concept of Operations for Federal Cyber Security Incident Handling when analyzing and reporting security incidents. US-CERT leveraged National Institute of Standards and Technology (NIST) guidance to identify incident and event categories and reporting timeframes for federal civilian agencies when submitting security incidents to US-CERT (see Appendix D).

In OMB's 2004 and 2005 reports to Congress, the accuracy, timeliness, and completeness of incident reporting was identified as a concern.<sup>5</sup> In addition, OMB cited that the number of incidents reported indicated sporadic reporting by some agencies and unusually low levels of reported malicious activity at other agencies.

---

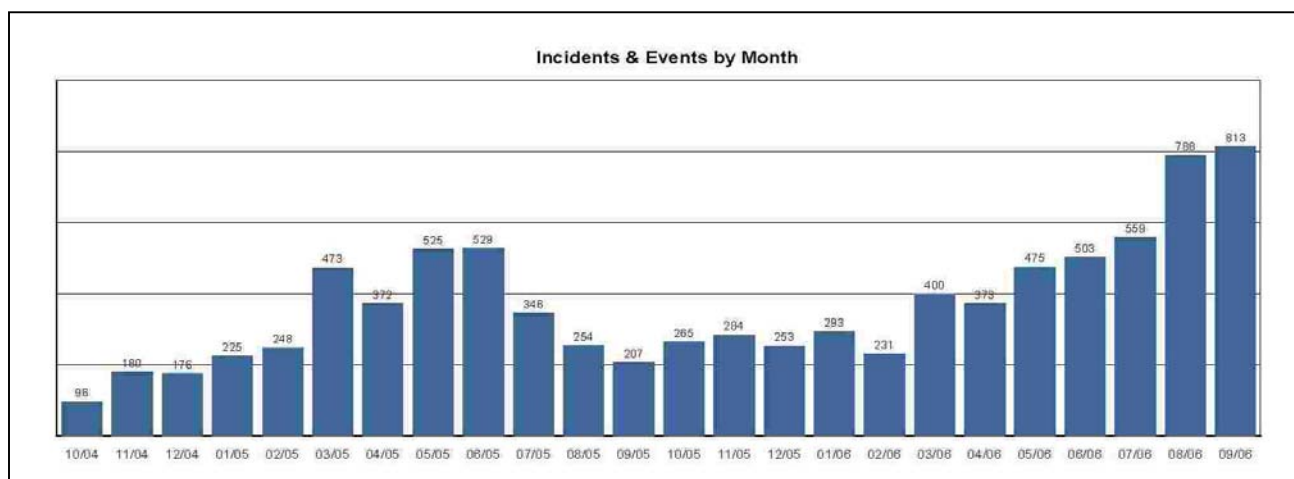
<sup>4</sup> An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Examples of the incidents are (1) denial of service attacks, (2) malicious codes, (3) unauthorized access, and (4) improper usage.

<sup>5</sup> *Federal Information Security Management Act (FISMA) 2004 Report to Congress*, dated March 1, 2005, and *FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, dated March 1, 2006.

Security incidents reported by federal agencies are analyzed for emerging threats and ranked by severity. US-CERT does not determine whether all security incidents and events are being reported by all federal agencies. Furthermore, US-CERT has not developed a process to use potential cyber incidents identified by Einstein along with other analyses to identify possible incident underreporting.

We obtained a summary report prepared by US-CERT for the period of October 1, 2004, to September 30, 2006. The number of incidents reported to US-CERT by federal agencies has increased each of the last 2 years (FY 2005: 3,631; FY 2006: 5,237). See Figure 2 below for the number of incidents and events reported during this period.

**Figure 2-Total Incidents and Events by Month**



There is a wide variation in the number of incidents and events reported to US-CERT by federal agencies of comparable size. For example, over the 2-year period, one agency with more than 56,000 employees reported 726 incidents, whereas another comparable agency with more than 67,000 employees reported only 17 incidents. In an effort to address this problem, OMB reported to Congress in FY 2005 that DHS had begun deploying Einstein's automated tool to monitor network traffic at three agencies and had funding to install it at an additional six agencies.<sup>6</sup> OMB further reported that the use of this and similar tools should considerably improve the government's ability to identify and respond to potential incidents in a timely manner. While DHS is the lead federal agency in securing the nation's cyberspace, it is not one of the federal agencies using Einstein department-wide to monitor its network traffic.

<sup>6</sup> As of December 2006, eight agencies were participating in the Einstein program.



---

As a service to federal agencies, US-CERT summarizes all security incidents and events, and issues a high-level snapshot report (quarterly and annually) to the White House and federal agencies. According to US-CERT personnel, these reports can be used by agencies to compare their individual security incidents and events with those reported by other agencies.

NCSA management said that while the Federal Information Security Management Act (FISMA) requires federal agencies to report all incidents to US-CERT, NCSA has not been given the authority to enforce individual agency reporting. To rectify sporadic incident reporting by federal agencies, NCSA staff have discussed the issue with OMB. NCSA has also met with the Chief Information Officers Council to make them aware of the need and benefits of reporting all incidents to US-CERT and have performed outreach to agencies that are reporting few if any incidents. NCSA management said that the annual FISMA reviews performed by the agency Inspectors General are used to identify and report instances of underreporting.

An effective incident response capability is critical to a government-wide security program as well as individual agency programs. In order for US-CERT to successfully perform its duties, it must have an accurate depiction of incidents across all agency bureaus and operating divisions. Additionally, incident reports can provide Chief Information Officers and other agency senior managers with valuable input for risk assessments, help prioritize security improvements, and illustrate risk and related trends.

## **Recommendations**

We recommend that the Assistant Secretary for CS&C direct the NCSA Director to:

**Recommendation #4:** Develop and implement procedures to review and analyze agencies' incidents submissions to identify underreporting of incidents by federal agencies.

**Recommendation #5:** Work with OMB and federal agencies to eliminate underreporting of cyber security incidents to US-CERT and complete the deployment of Einstein to all federal agencies.

## **Management Comments and OIG Analysis**

CS&C did not concur with recommendation 4. While NCSA continues to work collaboratively with OMB and federal agencies to encourage more robust reporting, compliance with FISMA regulations and underreporting issues fall outside the scope and authority of US-CERT.

---

While we agree that OMB is responsible for directing federal agencies to report all cyber incidents to US-CERT under FISMA guidance, we believe that NCSD, as the lead in securing cyberspace for the federal government, should develop and implement procedures to identify underreporting of incidents. The identification of underreporting would be based on analysis and situational monitoring currently being performed by US-CERT. The procedures we are recommending could be used in conjunction with recommendation 5 (eliminating underreporting of cyber security incidents), which CS&C agreed to implement.

CS&C concurred with recommendation 5. NCSD continues to work collaboratively with OMB and federal agencies to encourage more robust reporting but does not have the authority to mandate reporting. NCSD is working to expand the Einstein program to additional federal agencies. The program is planning an aggressive rollout of additional Einstein installations by the end of Fiscal Year 2008.

We agree that the steps that CS&C has taken, and plans to take, satisfy this recommendation.

## **Recommendation**

We recommend that the DHS Chief Information Officer:

**Recommendation #6:** Participate in the Einstein program in order to detect and identify potential security incidents.

## **Management Comments and OIG Analysis**

CS&C concurred with recommendation 6. NCSD is working closely with the Office of the Chief Information Officer to deploy Einstein across the department. A memorandum of agreement has been drafted between the parties and they will continue to collaborate.

We agree that the steps that management has taken, and plans to take, satisfy this recommendation.

## **Improved Information Sharing and Communications Will Enhance Cyber Infrastructure Security**

NCSD needs to improve its information sharing and communications programs with its private sector partners. Some private sector partners expressed concern over the focus and clarity of NCSD's communications.

**Challenges Remain in Securing the Nation's Cyber Infrastructure**

---

Concern was also expressed with the sharing of classified information with the private sector. Without the public and private sectors working together in identifying and sharing critical cyber information, there is little assurance that all critical data is made available to key personnel in order to prevent or recover from a major cyber incident.

### **Communications with Private Sector**

NCSD interacts with the IT sector (comprised of the producers and providers of hardware, software, and IT services) through working groups and incident response organizations. NCSD also collaborates with groups from the public and private sectors to facilitate the collection and sharing of computer security information and incidents.

While members of the groups interviewed said that there have been improvements at NCSD in the past year, including the sharing of threats and vulnerabilities and better interaction with NCSD staff, many in the private sector remain resistant to sharing information with the federal government. Group members expressed concern with the number of NCSD's ongoing priorities (noted in our previous finding), communications with the private sector, and the sharing of information.

NCSD helped to create the National Cyber Response Coordination Group, the principal interagency forum to coordinate intra-governmental and public/private preparedness efforts to respond to and recover from large-scale cyber attacks. NCSD established the Government Forum of Incident Response and Security Teams, a group of technical and tactical practitioners of security response teams responsible for securing government information technology systems. NCSD also interacts with the IT-Sector Coordinating Council and the IT-Information Sharing and Analysis Center. The IT-Information Sharing and Analysis Center is recognized by DHS as the information sharing organization for private industry within the IT sector.

Some of the IT information sharing organization members expressed concern that NCSD is not focusing its communications program toward the right people. While there has been an extensive amount of outreach and communications with the public and private sector cyber stakeholders, some members believe that there is a lack of communications by NCSD with senior executives at key IT sector companies. The members believe that NCSD senior management should meet with the executives individually to convince them of the value of cyber security improvements and collaboration with the federal government.

---

Members in the private sector also had concerns when receiving information requests from NCSA. At times, it was unclear what specific information DHS wanted, why the information was needed, what NCSA would do with it, and how the information would be protected. Per group members, there remains a hesitancy to share information by the private sector due to a lack of trust of the government.

Communications with the private sector is a challenge for NCSA. NCSA's message to the private sector concerning the need for stronger cyber security and information sharing must be communicated to many people at different levels within organizations who are responsible for securing their own portion of cyberspace. Without the support of senior management in the private sector, there is little assurance that employees at these companies will implement the security improvements needed to secure their cyber assets. Further, without a clear understanding by the private sector of how information is used and secured, there is little assurance that NCSA will obtain the necessary information needed to protect the cyber infrastructure.

### **Sharing of Classified and Sensitive Information**

Some private sector partners also expressed concern over sharing of classified information. Specifically, incident and vulnerability information that the private sector believes that they need to secure their own cyber assets is deemed classified, and thus prevents the sharing of critical information. In addition, some members of the private sector said that they are not provided with clear guidance on how sensitive (For Official Use Only [FOUO]) or classified information that they do receive can be shared with other people within their organizations.

US-CERT personnel said that classified information is received from many sources including the intelligence community, Department of Defense, and law enforcement agencies. US-CERT personnel will send an unclassified/FOUO version only to those organizations or individuals that they believe need the information.

The originating organization of classified information is responsible for determining the classification of the documents being sent to US-CERT. Per US-CERT personnel, the originator is to include an unclassified portion or version so that the critical information can be distributed to the appropriate organizations. At times, US-CERT personnel must request the unclassified version from the originator if it was not sent originally. In addition, US-CERT must ask the originator of the information for their approval before sending the information out to the recipients.

---

According to NCSA, US-CERT's capability to disseminate unclassified information to its public and private sector constituents continues to evolve as NCSA works more closely with the originating organizations to improve the process. In many cases, the originator of the classified information will not allow NCSA to share unclassified versions of the information with the private sector. The marking of unclassified documents as FOUO limits NCSA's ability to share information with the private sector.

In an attempt to keep the private sector informed on cyber matters, NCSA staff has held meetings with several Information Sharing and Analysis Centers, participated in daily IT-Information Sharing and Analysis Center Operations Center conference calls, and are available for individual inquiries concerning the sharing of classified or sensitive information. NCSA has also discussed classified information with cleared private sector individuals.

Homeland Security Presidential Directive 7 requires DHS and federal agencies to collaborate with the private sector to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. *The National Strategy to Secure Cyberspace* also calls for the removal of impediments to information sharing between the public and private sectors.

It is essential that people and organizations receive and are able to share critical information in order to take the appropriate steps to reduce the effects of a cyber incident. In its December 2006 Strategy report, CS&T acknowledged that information sharing, including the sharing of classified information, is a gap between stakeholder expectations and DHS' capabilities and programs.

## Recommendations

We recommend that the Assistant Secretary for CS&C direct the NCSA Director to:

**Recommendation #7:** Develop clearer communications with key personnel and organizations in the private sector to explain the processes being used to capture, share, use, and secure cyber information.

**Recommendation #8:** Expand its communications program with a focus on key private sector executives to encourage corporations to more actively participate in the information sharing program and to better secure its systems.

**Recommendation #9:** Develop and implement formal procedures for receiving, reviewing, and distributing sensitive and classified information.

---

The procedures should include the types of information that can be shared, and the timing of receiving an unclassified (or reduced level) and redacted version or portion of the information that can be shared with cyber partners in the private sector. These procedures should be reviewed and agreed to by all organizations providing sensitive and classified information.

## **Management Comments and OIG Analysis**

CS&C concurred with recommendation 7. NCSA will continue to build and maintain strong working relationships with the IT sector. In October 2006, US-CERT, in collaboration with the IT-Information Sharing and Analysis Center, developed a draft Concept of Operations for private industry cyber security incident handling that addresses information sharing, communication, and coordination with the private sector, including how the public and private sectors will work together and how information will be shared. In addition, the NCSA Internet Disruption Working Group completed a draft of the information sharing assessment in January 2007 and findings will be briefed to the Internet community at the next Internet Disruption Working Group forum. CS&C will continue to enhance analysis and information aggregation functions to provide timely and actionable dissemination of information.

We agree that the steps that CS&C has taken, and plans to take, satisfy this recommendation.

CS&C concurred with recommendation 8. CS&C agreed that more can and should be done to expand communications to key private sector stakeholders. The Assistant Secretary for CS&C created a permanent External Affairs position within the CS&C front office working closely with NCSA to engage with private sector executives in a variety of forums. Recent activities include meetings with key private sector representatives and major industry groups.

We agree that the steps that CS&C has taken, and plans to take, satisfy this recommendation.

CS&C concurred with recommendation 9. CS&C agreed that more should be done to improve information sharing with public and private sector organizations. US-CERT is working with its intelligence community partners to develop procedures for sharing of information between organizations. In addition, NCSA and its partners have shared classified information with cleared private sector stakeholders and continue to make every effort to develop unclassified versions of key documents to ensure broad dissemination of actionable information.

---

We agree that the steps that CS&C has taken, and plans to take, begin to satisfy this recommendation.

## **Revised Certification and Accreditation Will Satisfy FISMA Requirements**

NCSD's certification and accreditation documentation requires updating in order to satisfy FISMA requirements. We noted deficiencies with the security artifacts<sup>7</sup> contained in the accreditation packages for two NCSD systems, Einstein and Cybercop Portal, which were authorized to operate in FY 2006.<sup>8</sup> Lacking key information, agency officials cannot make credible risk-based decisions on whether to authorize systems to operate or ensure that systems are adequately secure. Both systems were authorized to operate for 1 year; therefore they are scheduled to be recertified and accredited in 2007.

NCSD has implemented adequate security controls over the systems reviewed. However, some security documents were missing key information that is required to meet applicable OMB, NIST, and DHS guidelines.<sup>9</sup>

### **Einstein Documentation**

NCSD uses data captured from its Einstein system sensors to analyze suspicious network traffic from across the federal government network infrastructure. A number of improvements are needed in the system documentation. Specifically:

- The system security plan does not identify each of the systems that are connected to Einstein or contain an accurate description of the hardware installed. Agency officials require this detailed information in order to make credible, risk-based decisions on whether adequate controls have been implemented and to determine whether to authorize the system to operate.

---

<sup>7</sup> DHS requires 11 artifacts be developed during the certification and accreditation process. The 11 artifacts are: Authority To Operate letter, system security plan, risk assessment, security test and evaluation, security assessment report, contingency plan, contingency plan test results, e-authentication determination, Federal Information Processing Standards Publication 199 determination, privacy threshold analysis, and annual self assessment.

<sup>8</sup> The Cybercop Portal is a secure Internet-based information sharing mechanism for more than 8,700 law enforcement members involved in the field of electronic crimes investigations. The law enforcement community, including investigators from private industry, e.g., banks and the network security community, is tied together and supported by this secure, Internet-based, collaboration portal. Members represent all 50 states, effectively all government agencies, and more than 40 countries.

<sup>9</sup> According to OMB policy, certification and accreditation requires documentation of security planning, including risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements.

- 
- Einstein’s contingency plan does not address backup and recovery procedures necessary to restore operations in the event of an emergency or system failure.
  - NCSD has not tested the contingency plan to ensure that business and computer operations can be maintained or restored, possibly at an alternate location, in the event of an emergency, system failure, or disaster.
  - The risk assessment does not evaluate the likelihood of vulnerabilities identified that may be exploited or the potential impact and magnitude of harm to the system by exploiting the vulnerabilities identified.
  - Physical controls implemented at the contractor's location were not evaluated when completing the NIST 800-26 self-assessment to ensure that physical access to computer resources is restricted to authorized personnel.

### **Cybercop Portal Documentation**

NCSD supports the Cybercop Portal, which is used by law enforcement entities at all levels of government to communicate and share information. A number of improvements are needed in the system’s security documentation. Specifically:

- The risk assessment does not stipulate the use of security testing to identify vulnerabilities or analyze the effectiveness of controls implemented.
- The system test and evaluation plan does not include procedures to assess the effectiveness of controls implemented.
- NCSD has not performed annual security testing to evaluate the system controls implemented.
- The contingency plan has not been tested to determine whether specific aspects of the plan such as the data backup and recovery procedures remain valid.
- Security awareness training was not provided to contractors who are responsible for maintaining the system.

### **Vulnerability Assessments of Einstein and Cybercop Portal**

Overall, NCSD has implemented adequate security controls over each of the two systems reviewed. To assess system security, we (1) interviewed information technology personnel responsible for Einstein and Cybercop Portal; (2) performed vulnerability scans at NCSD headquarters, contractor



---

sites, and the Einstein collection systems at one federal agency; (3) manually reviewed selected routers, switches, and firewalls for Einstein system; and, (4) performed vulnerability scans on selected servers and firewalls, and password analysis for the Cybercop Portal. Our testing did not include an assessment of the Cybercop Portal application software.

No high-risk vulnerabilities were detected on the Cybercop Portal devices tested. We found only two medium-security vulnerabilities on the Einstein system. When devices are not properly configured, the vulnerabilities could be exploited to gain inappropriate access to sensitive information. Subsequent to the completion of our audit work, NCSA personnel indicated that appropriate actions have been taken to address the vulnerabilities. As fieldwork had already been completed, we did not verify whether the vulnerabilities had been addressed.

FISMA requires federal agencies to provide adequate controls for the data and information systems under their controls by (1) periodically assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction; (2) performing annual security testing to evaluate the effectiveness of security controls implemented; (3) providing security awareness training to inform personnel, including contractors and other users; and (4) planning and developing procedures to ensure the continuity of operations for the systems and data that support the operations and assets of the agency.

Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions. Testing of contingency plans is performed to validate specific aspects of the plan, policies, procedures, systems, and facilities that will be used in the event of an emergency. Testing the plan identifies planning gaps and is also a training exercise to prepare recovery personnel for plan activation, which can improve plan effectiveness and overall agency preparedness.

## **Recommendations**

We recommend that the Assistant Secretary for CS&C direct the NCSA Director to develop and implement procedures for all systems to:

**Recommendation #10:** Ensure that certification and accreditation documents contain complete and accurate information to reflect the security postures of the system. In addition, security documents should be reviewed periodically and revised if necessary to ensure that agency officials are provided with the most accurate information to make credible, risk-based decisions on whether to authorize a system to operate.

---

**Recommendation #11:** Test contingency plans, at least annually, to ensure business and computer operations can be maintained or restored in the event of an emergency, system failure, or disaster.

**Recommendation #12:** Perform security testing annually to evaluate the effectiveness of controls implemented.

**Recommendation #13:** Provide security awareness training to all contractors.

**Recommendation #14:** Remedy all vulnerabilities identified for which risks have not been assumed.

## **Management Comments and OIG Analysis**

CS&C concurred with recommendation 10. NCSD has a dedicated full-time Information Systems Security Officer to ensure that US-CERT systems, including Einstein and Cybercop Portal, meet FISMA requirements and continue to maintain the proper authority to operate. Based on feedback from our review, US-CERT is in the process of updating documentation for the 2007 Einstein and Cybercop Portal re-accreditations.

We agree that the steps that CS&C plans to take satisfy this recommendation.

CS&C concurred with recommendation 11. US-CERT has successfully implemented a backup system for Einstein. In March 2007, Einstein's back-up system was successfully tested, with additional testing planned in upcoming months. Additionally, US-CERT has requested resources to build and maintain an alternate site location for the Einstein program. A Continuity of Operations Plan has been developed and is operational for the Cybercop Portal to include off-site backup capability.

We agree that the steps that CS&C has taken, and plans to take, begin to satisfy this recommendation. However, CS&C did not specifically address whether it has or will test the Cybercop Portal's off-site backup capability. We maintain that contingency plans should be tested for all systems, at least annually.

CS&C concurred with recommendation 12. US-CERT performs security testing annually in compliance with DHS policy. US-CERT is currently submitting documentation and conducting testing so that an additional one-year authority to operate the Einstein system may be granted. For the Cybercop Portal, annual security testing is performed in accordance with standard certification and accreditation procedures. The administrator of the

---

Cybercop Portal conducts additional security testing to evaluate the effectiveness of the controls implemented.

We agree that the steps that CS&C has taken, and plans to take, satisfy this recommendation.

CS&C concurred with recommendation 13. NCS D provides and complies with all security awareness training required by DHS for all staff, including contractors. CS&C conducted its latest security awareness training for all its components on April 25, 2007.

We agree that the steps that CS&C has taken satisfy this recommendation.

CS&C concurred with recommendation 14. NCS D and US-CERT have been proactive in addressing identified vulnerabilities within Einstein and have resolved the necessary items.

We agree that the steps that CS&C has taken begin to satisfy this recommendation. However, while CS&C addressed the vulnerabilities we identified during the audit, it did not specifically address whether it will remedy all vulnerabilities identified for which risks have not been assumed as a result of future security testing.

## Purpose, Scope, and Methodology

Our objective was to determine whether NCSA is working collaboratively with the public, private, and international entities to secure cyberspace and cyber assets and has effectively managed the implementation of *The National Strategy to Secure Cyberspace*. Specifically, we determined whether: (1) NCSA has adequately addressed the actions and recommendations in *The National Strategy to Secure Cyberspace*; (2) implementation plans are meeting NCSA's strategic goals and priorities; (3) US-CERT is adequately performing its mission; (4) partnerships and coordination with other government agencies and the private sector are effective in securing cyberspace and cyber assets; and, (5) operational systems are in compliance with *Federal Information Security Management Act* requirements.

To accomplish our audit, we interviewed selected NCSA personnel and contractors at its headquarters and contractor facilities. We interviewed selected members of the Government Forum of Incident Response and Security Teams, IT-Information Sharing and Analysis Center, IT-Sector Coordinating Council, and the National Cyber Response Coordination Group to obtain their perspective on how well NCSA is managing its mission and working with its cyber partners. These groups were selected since the members work with NCSA on a regular basis. We asked for feedback about NCSA's priorities, communications and information sharing, frustrations, and positive aspects of NCSA.

During the audit, we reviewed applicable security policies, procedures, and other appropriate documentation. In addition, we evaluated the quality of the certification process for two of its mission support systems (Einstein and Cybercop Portal) and determined whether the systems were accredited per OMB and DHS guidance. We further tested security controls over the two systems to ensure that effective controls have been implemented to protect the information stored and processed by the systems. We used network vulnerability assessment software (Tenable Network Security's Nessus Vulnerability Scanner, Internet Security Systems' Internet Scanner) to detect and analyze vulnerabilities on devices for the two systems at NCSA headquarters, one federal agency, and contractor sites. Upon completion of the assessments, we provided NCSA with the technical reports detailing vulnerabilities detected and remediation actions needed.

We conducted our audit between October 2006 and January 2007 under the authority of the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix E.

## **Appendix A**

### **Purpose, Scope, and Methodology**

---

The principal OIG points of contact for the audit are Frank W. Deffer, Assistant Inspector General, IT Audits at (202) 254-4100 and Edward G. Coleman, Director, Information Security Audit Division at (202) 254-5444.

**Appendix B**  
**Management Comments to the Draft Report**


Office of the Under Secretary for  
National Protection and Programs  
U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

April 24, 2007

MEMORANDUM TO: Richard L. Skinner  
Inspector General

FROM: George W. Foresman  4/30/07  
Under Secretary

SUBJECT: *Response to Office of Inspector General's Challenges Remain in  
Securing the Nation's Cyber Infrastructure Draft Audit Report*

This responds to the March 19, 2007, memorandum requesting the Directorate for National Protection and Programs' comments to the Office of the Inspector General Draft Audit Report, *Challenges Remain in Securing the Nation's Cyber Infrastructure*. First, we sincerely appreciate the opportunity to respond to the draft report. The attached document provides comments on the 14 recommendations directed to the National Protection and Programs Directorate. Questions concerning specific comments should be addressed to Duane Johnson 202-447-3230.

Please accept our thanks for the opportunity to respond to the draft report and to work with the Office of the Inspector General during this engagement. As the National Protection and Programs Directorate works toward refining its programs, the Office of the Inspector General's independent analysis of program performance greatly benefits our ability to continuously improve our activities. We look forward to continuing this partnership in the future.

Attachment

cc: Greg Garcia  
Steven Pecinovsky

## Appendix B Management Comments to the Draft Report

4/23/2007

**Office of Cyber Security and Communications**  
**Response to Department of Homeland Security Office of Inspector General**  
***Challenges Remain in Securing the Nation's Cyber Infrastructure***  
**Draft of March 2007**

The Office of Cyber Security and Communications (CS&C) is pleased to have the opportunity to respond to the Department of Homeland Security (DHS) Office of Inspector General (OIG) draft report entitled, *Challenges Remain in Securing the Nation's Cyber Infrastructure* (Report). We appreciate OIG's independent evaluation of the National Cyber Security Division (NCSD), and have taken seriously the suggestions for improvement.

Since the last OIG audit was concluded in July 2004,<sup>1</sup> NCSD has made significant progress implementing the National cyber security priorities outlined in the *National Strategy to Secure Cyberspace* (February 2003) toward its mission of working collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.

This Report provides a fair assessment of much of the progress to date, recognizing the considerable breadth inherent in our cyber security responsibilities. While CS&C concurs with many of the findings and recommendations, we believe further clarification would be beneficial and appreciate the opportunity to expand upon the fourteen areas targeted in the Report, as discussed below.

**1. Establish priorities and milestones (short term and long term) for critical tasks using input from the CS&T Strategy Summary report and IT-Sector Specific Plan. Milestones should be based on available funding and resources.**

CS&C concurs with the need to establish short and long term priorities and milestones for critical tasks. Upon taking office in the fall of 2006, Assistant Secretary Garcia conducted a comprehensive assessment of CS&C programs, personnel, and processes. As part of this effort, he met with government and industry leaders to hear about their needs and challenges, as well as their ideas regarding CS&C priorities. The result of this comprehensive assessment was the identification of three strategic priorities: Prepare and Deter; Respond; and, Build Awareness. Over the course of the next two years and beyond, CS&C will address these priorities through near- and long-term actions.

NCSD goals and priorities map to CS&C priorities with an NCSD implementation plan and detailed program plans, with updated prioritized actions and milestones as well as current and anticipated resources for the next five years. In an effort to continue to improve performance management within the new organizational structure, CS&C is in the process of defining additional performance measures and milestones that tie into NCSD's mission, priorities, processes, and available personnel and budget. CS&C has scheduled its first quarterly review of its components, including NCSD, evaluating

<sup>1</sup> *Progress and Challenges in Securing the Nation's Cyberspace*, OIG-04-29 (July 2004).

4/23/2007

progress in terms of priorities developed by the CS&C Assistant Secretary, current funding, and anticipated funding for Fiscal Year 2008. As part of this effort, NCSD also provides weekly status updates to the Assistant Secretary and contributes to CS&C's bi-weekly report to the Department's leadership on priority actions.

The OIG Report also suggests the IT SSP milestones be taken into account within NCSD programs. As noted above, CS&C has clearly delineated priorities for NCSD, which align with the Department of Homeland Security Goals and the *National Strategy to Secure Cyberspace*; taking into account available and anticipated funding. As the government lead for the IT Sector, NCSD played a key role in developing the IT SSP in collaboration with the public and private sectors. In this regard, NCSD worked closely with government and industry representatives to develop mutually agreed upon goals, and assure the IT Sector Specific Plan complemented the Federal government's priorities and milestones for the Nation's cyber security assets.

**2. Centralize the tracking of all current and future initiatives and milestones, and review at least quarterly.**

CS&C non-concurs with this finding. NCSD monitors its milestones and performance based upon its strategic plan. As noted above, NCSD is also revising its strategic plan with a comprehensive implementation plan and revised program plans: tracking actions, milestones and resources. In the interim, each NCSD program continues to map progress with milestones and associated metrics in their current program plans that are reviewed quarterly at the NCSD branch level.

Each quarter, NCSD programs update their program plans and metrics tracking documents, which identify completed milestones and report on various measures. Program managers and senior leadership use this process to review proposed future milestones and deliverables. The quarterly tracking also flows into the quarterly Office of Management and Budget (OMB) Program Assessment Rating Tool (PART) reporting process. In addition, NCSD's internal efficiency metric measures the percentage of milestones completed on time. Program managers must substantiate reasons for falling short of milestones and meet with senior leadership to adjudicate follow-up action at the branch level.

NCSD will report quarterly to CS&C on accomplishments and deliverables mapping to programmatic actions, milestones and resource allocations, identifying anticipated potential shortfalls and remedial actions.

**3. Develop additional performance measures for each branch that can be used to review and periodically evaluate the outcome or success of the division's programs.**

CS&C non-concurs with this finding. Since NCSD was established in June 2003, the organization has tackled a vast array of challenges and responsibilities in a systematic way to ensure performance is evaluated against its cyber mission. In addition, since the

2



## Appendix B Management Comments to the Draft Report

4/23/2007

issuance of the Government Accountability Office report on Critical Infrastructure Protection in May of 2005,<sup>2</sup> NCSO has drafted a metrics implementation plan that provides the process, guidance, and template by which internal NCSO programmatic goals and milestone metrics will be collected and evaluated. These internal metrics are aligned with the NCSO strategic plan milestones to measure progress, and gauge areas for improvement at the activity level.

NCSO internal performance measures have been developed and collected through the PART process and other internal performance measurement reporting processes. Below is a sample of the major programmatic measures:

- Number of emergency response conference calls involving 90% of Cabinet agencies to mitigate damages from catastrophic disaster. (Manmade or otherwise).
- Publish 95% of critical IT vulnerabilities to prevent major IT failures of critical computing infrastructure (approximately 15,000 out of 144,000 vulnerabilities published yearly).
- Through the Einstein program, provide the ability to share cyber threats in real-time for 80% of the Cabinet departments and agencies; and disseminate cyber threat alerts based on United States Computer Emergency Readiness Team (US-CERT) analysis across the Government Forum of Incident Response and Security Teams (G-FIRST) community.
- Collect and catalog 10,000 Malicious Code artifacts annually (reflect software code for the most damaging computer attacks) for use by the G-FIRST community to protect Federal civilian government computer systems.
- Number of interagency or working groups, conferences, workshops, speeches, briefings, which are held, delivered, or chaired by NCSO; and developed and delivered methodologies, guidance, frameworks and major reports/plans.
- Targeted public, private, and international stakeholders who participate in or obtain cyber security products and services.
- The degree to which programmatic goals and milestones are being met.

NCSO has taken into account previous findings and recommendations from DHS OIG and Government Accountability Office reports to develop and implement performance measures to improve the ability to assess overall programmatic progress. As indicated above, NCSO has developed proposed revised PART measures to cover the breadth of its programs. In addition, NCSO developed and implemented internal program level measures (examples above) that began in the third quarter Fiscal Year 2006. These performance measures ensure NCSO's effectiveness in product delivery focused on protecting the Nation's cyber assets through the implementation of an integrated cyber risk management program and a National Cyber Security Response System to detect, respond to, and recover from cyber attacks and disruptions. Finally, even with metrics in place, NCSO is regularly evaluating its metrics and strives to improve them.

<sup>2</sup> *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (May 26, 2005). NCSO has also addressed findings in the DHS Office of Inspector General Report, *Progress and Challenges in Securing the Nation's Cyberspace*, OIG-04-29 (July 2004).

4/23/2007

**4. Develop and implement procedures to review and analyze agencies' incidents submissions to identify underreporting of incidents by federal agencies.**

CS&C non-concurs with this finding and recommendation. The NCSD's US-CERT receives incident reports from agencies and provides quarterly and annual trend reports to the individual agencies and the White House, as required by Federal Information Security Management Act (FISMA).<sup>3</sup>

While less than complete reporting may well hamper comprehensive analysis of an incident, NCSD does not concur with recommendation number four, or some of the assertions in the Report discussing expanded incident reporting analysis. The OMB, not US-CERT, is responsible for directing the twenty four Federal agencies subject to FISMA to report all cyber incidents to US-CERT under FISMA guidance.

The US-CERT Operations Incident Handling Center provides a 24 hour a day, seven day a week watch center that conducts daily analysis and situational monitoring. The Center identifies trends and provides information on incidents and other events, as they are detected and unfold, to increase situational awareness and understanding of the current operating environment. FISMA policy requires all Federal agencies to notify US-CERT of any data breaches, unauthorized access, or suspicious activity, including the loss of personally identifiable information (PII). Incidents reported to US-CERT are handled in accordance with the nature of the incident. Incidents requiring law enforcement or intelligence community support are routed appropriately. Additionally, incident data is analyzed along with Einstein data, malicious code submissions, and vulnerabilities to correlate cyber security events. The resulting analysis is disseminated through US-CERT's operational products, including, but not limited to Federal Information Notices, Critical Infrastructure Information Notices, Situational Awareness Reports, Technical Information Papers, and Quarterly Trends and Analysis Reports.<sup>4</sup>

NCSD and US-CERT have developed strong relationships with a number of agencies resulting in successful response collaborations in compliance with OMB guidance, FISMA, and the US-CERT Concept of Operations (CONOPS). While NCSD continues

---

<sup>3</sup> Federal Information Security Management Act (FISMA), 44 U.S.C. Section 3541 et. seq., provides the framework for securing Federal government's information technology. Section 3546 states the Federal information security incident center [designated by OMB as US-CERT], will perform certain functions such as: technical timely assistance to agency information system operators; compiling and analyzing information about incidents that threaten information security; informing operators of agency information systems about current and potential information security threats and vulnerabilities; and consultation with NIST, agencies or offices operating or exercising control national security systems (including National Security Agency.) See also, OMB Memo, M-04-25, August 2004, which expressly requires Federal civilian agencies to implement FISMA and to "ensure the operation of a central federal information security incident center" which is US-CERT.

<sup>4</sup> The trend reports provided to the agencies provide a summary of the incidents reported to US-CERT during the reporting period.

## Appendix B Management Comments to the Draft Report

4/23/2007

to work collaboratively with OMB and the agencies to encourage more robust reporting, compliance with FISMA regulations and underreporting issues fall outside the scope and authority of US-CERT. Contrary to the Report, NCSD staff has not requested the authority to challenge the number of incidents being reported.<sup>5</sup> OMB has retained the statutory authority to hold agencies accountable for non-compliance with administrative directives and policies. These types of activities are beyond the scope and technical expertise of US-CERT.

### **5. Work with OMB and federal agencies to eliminate underreporting of cyber security incidents to US-CERT. Complete the deployment of Einstein to all federal agencies.**

CS&C concurs with this recommendation. As noted above in connection with recommendation number four, NCSD continues to work collaboratively with OMB and Federal agencies to encourage more robust reporting, and does not have the authority to mandate reporting. Einstein has proven effective in reducing time for the Federal Government to gather and share critical data on computer security risks from days to hours.<sup>6</sup>

With regard to the Einstein deployment among all Federal agencies, CS&C concurs with this recommendation. NCSD is working assiduously to expand the Einstein program. Einstein is currently deployed at ten Federal agencies with a goal to deploy it to all Cabinet level and critical independent Federal agencies. Two additional agencies are expected to have Einstein in place by the end of Fiscal Year 2007. The program is planning an aggressive roll out of additional Einstein installations by the end of Fiscal Year 2008.

### **6. DHS Chief Information Officer (CIO): Participation in the Einstein program in order to detect and identify potential security incidents.**

CS&C concurs and NCSD/US-CERT is working closely with the DHS Chief Information Officer (CIO) regarding the deployment of Einstein across the Department. US-CERT and the DHS CIO have taken steps together to facilitate the deployment of Einstein across DHS, including the drafting of a Memorandum of Agreement between the parties and will continue to collaborate. Einstein is deployed within US-CERT.

---

<sup>5</sup> Report, p.12.

<sup>6</sup> The US-CERT Einstein program supports Federal agencies' efforts to protect their computer networks. Einstein provides the first situational awareness picture of the Federal Government's Internet facing networks. It enables the rapid detection of cyber attacks affecting agencies and provides Federal agencies with early incident detection.

4/23/2007

**7. Develop clearer communications with key personnel and organizations in the private sector to explain the processes being used to capture, share, use, and secure cyber information.**

CS&C concurs with this recommendation. With the increasing sophistication of cyber attacks and the ever-present demand for communications capabilities during incident response, CS&C concurs with this recommendation and NCSO will continue to build and maintain strong working relationships with the IT Sector.

CS&C is promoting enhanced public/private information sharing involving cyber attacks, threats, and vulnerabilities through a variety of efforts including development of a US-CERT CONOPS with the private sector and collaboration with the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). In October 2006, US-CERT, in collaboration with the IT-ISAC, developed a draft CONOPS for Private Industry Cyber Security Incident Handling that addresses information sharing, communication, and coordination with the private sector. The CONOPS clearly articulates how the public and private sectors will work together and how information will be shared. NCSO is also collaborating with HITRAC and IT Sector partners to enhance cyber and IT Sector risk assessment efforts. These efforts will help to ensure that threat products accurately reflect the latest cyber security expertise and issues, and also that products are designed to meet Critical Infrastructure/Key Resource stakeholder needs, enabling them to take effective protective actions, and respond to and recover from incidents.

The NCSO Internet Disruption Working Group (IDWG) conducted an information sharing assessment study to better understand the information sharing landscape involving Internet incidents. The IDWG completed a draft of the information sharing assessment in January 2007, and findings will be briefed to the Internet community at the next IDWG Forum. The briefing will also outline resources and time needed to implement recommendations.

CS&C recognizes that in order to build true information sharing partnership, information must flow both ways and will continue to enhance analysis and information aggregation functions to provide timely and actionable dissemination of information.

**8. Expand its communications program with a focus on key private sector executives to encourage corporations to more actively participate in the information sharing program and to better secure its systems.**

CS&C concurs that more can and should be done to expand communications to key private sector stakeholders. Since the arrival of Assistant Secretary Garcia in the fall of 2006, emphasis has been placed on actively engaging the private sector. He created a permanent External Affairs position within the CS&C Front Office working closely with NCSO to engage with private sector executives in a variety of forums. Recent activities include meetings with key private sector representatives and major industry groups.

6

## Appendix B Management Comments to the Draft Report

4/23/2007

**9. Develop and implement formal procedures for receiving, reviewing, and distributing sensitive and classified information. The procedures should include the types of information that can be shared, and the timing of receiving an unclassified (or reduced level) and redacted version or portion of the information that can be shared with cyber partners in the private sector. These procedures should be reviewed and agreed to by all organizations providing sensitive and classified information.**

CS&C concurs with this finding that more should be done to improve information sharing with public and private sector organizations. This is a government-wide challenge that is currently being led by the Office of the Director of National Intelligence's "Information Sharing Environment" initiative, in which DHS is participating.

NCSO complies with all existing Federal and DHS directives regarding sensitive and classified information. US-CERT is working with its intelligence community partners to develop "tear-line" procedures for sharing of information between organizations. In addition, NCSO and its partners have shared classified information with cleared private sector stakeholders and continue to make every effort to develop unclassified versions of key documents to ensure broad dissemination of actionable information.

**10. Ensure that certification and accreditation documents contain complete and accurate information to reflect the security postures of the system. In addition, security documents should be reviewed periodically and revised if necessary to ensure that agency officials are provided with the most accurate information to make credible, risk-based decisions on whether to authorize a system to operate.**

CS&C concurs. NCSO has a dedicated, full-time Information Systems Security Officer (ISSO) on site along with a Certification and Accreditation (C&A) team to ensure that US-CERT systems, including Einstein and the Cybercop Portal, meet FISMA requirements and continue to maintain the proper authority to operate. Additionally, the documents are validated by the DHS CIO and Information Systems Security Manager (ISSM) at the directorate and department level. The Cybercop Portal C&A process for Fiscal Year 2006 was the first certification of the portal since it was the first year DHS provided funding for development of the portal. Based on feedback from the OIG's review, US-CERT is in the process of updating documentation for the 2007 Einstein and Cybercop Portal re-accreditation..

**11. Test contingency plans, at least annually, to ensure business and computer operations can be maintained or restored in the event of an emergency, system failure, or disaster.**

7

## Appendix B Management Comments to the Draft Report

---

4/23/2007

CS&C concurs with this recommendation. Einstein was initially implemented as a “pilot” program to test the capability and did not address contingency capabilities. However, since the program rapidly expanded to full operational capability in Fiscal Year 2006, US-CERT has been working to implement Continuity of Operations Plan (COOP) capabilities. In this regard, US-CERT has successfully implemented a backup system for Einstein, which allows for a restoration of operations in the event of an emergency. In March 2007, Einstein’s back up system tested successfully, with additional testing planned in upcoming months. Additionally, US-CERT has requested resources to build and maintain an alternate site location for the Einstein program.

A COOP has been developed and is operational for the Cybercop Portal to include off-site back-up capability in the event of an emergency, system failure, or disaster to the primary facility. This COOP plan is provided for and delineated in the current contract DHS maintains with the administrator of the portal.

### **12. Perform security testing annually to evaluate the effectiveness of controls implemented.**

CS&C concurs with this recommendation. US-CERT performs security testing annually in compliance with Department of Homeland Security policy. Einstein was granted a one-year Authority To Operate (ATO) in June 2006. US-CERT is currently submitting documentation and conducting testing so that an additional one-year ATO may be granted by the DHS CIO. For the Cybercop Portal, annual security testing is performed in accordance with standard C&A procedures. The administrator of the Cybercop portal, conducts additional security testing to evaluate the effectiveness of the controls implemented.

### **13. Provide security awareness training to all contractors.**

CS&C concurs. NCSO provides and complies with all security awareness training required by the DHS to all staff, including contractors. CS&C is conducting its next security awareness training for all components on April 25, 2007.

### **14. Remedy all vulnerabilities identified for which risks have not been assumed.**

Based on this Report’s preliminary findings, CS&C concurs. NCSO/US-CERT has been proactive in addressing identified vulnerabilities within Einstein and has resolved the necessary items.

8

## Appendix C

### NCSD Major Functions and Responsibilities

---

#### **NCSD Director**

The NCSD Director is responsible for issues related to the operation of the NCSD, such as human resources, policy, and budget, as well as participation in international initiatives. The director develops the overall strategic direction and priorities for the division, in line with CS&C goals and objectives. The director is responsible for managing US-CERT—which is a partnership between NCSD and the public and private sectors to make cyber security a coordinated, national effort; increase public awareness of cyber threats and vulnerabilities; and improve computer security preparedness and response to cyber threats.

#### **US-CERT Operations Branch**

NCSD's US-CERT Operations branch focuses on situational awareness, analytical cells, and federal coordination. US-CERT is charged with protecting the nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. A key component of US-CERT is the National Cyber Security Response System (Response System), which provides a nationwide, real-time collaborative information-sharing network to enable communication and collaboration among DHS and federal, state, local, and international government and law enforcement entities. Components of the Response System include the following:

- The US-CERT Operations Center serves as a 24-hour-a-day/7-day-a week, real-time focal point for cyber security, conducting daily conference calls with U.S.-based watch and warning centers to share classified and unclassified security information.
- The US-CERT Portal provides a Web-based collaborative system that allows US-CERT to share sensitive cyber-related information with members of government and industry.
- The US-CERT Control Systems Security Center serves as an operational and strategic component of US-CERT's capability to address the complex security issues associated with the use of control systems.
- The US-CERT public web site provides government, the private sector, and the public with information they need to improve their ability to protect their information systems and infrastructures.
- The National Cyber Alert System is to deliver targeted, timely, and actionable information to Americans to allow them to secure their computer systems.
- The National Cyber Response Coordination Group brings together officials from federal agencies to coordinate public/private cyber preparedness and incident response.
- The Government Forum of Incident Response and Security Teams is a community of government response teams that are responsible for securing government information technology systems. This forum works to understand and handle computer security incidents and to encourage proactive and preventative security practices.

#### **Outreach and Awareness Branch**

NCSD's Outreach and Awareness branch is responsible for outreach, awareness, and messaging. The branch promotes cyber security awareness among the general public and within key communities, maintains relationships with governmental cyber security professionals to coordinate and share information about cyber security initiatives, and develops partnerships to promote public/private coordination and collaboration on cyber security issues.

The branch is organized into three functional areas: Stakeholder Outreach, Communications and Messaging, and Coordination. The Stakeholder Outreach team serves to build and maintain relationships among and between industry, government, and academia in order to raise cyber security awareness and secure cyberspace. The Communications and Messaging team focuses on coordination of internal and external communications.

## Appendix C

### NCSA Major Functions and Responsibilities

---

The Coordination team works to ensure collaboration on events and activities across NCSA and with other DHS entities, including the public affairs, legislative affairs, and private-sector offices and others, as appropriate. The team works to foster the department's role as a focal point and coordinator for securing cyberspace and implementing *The National Strategy to Secure Cyberspace*. The International Affairs program engages in international outreach activities to build awareness about the global cyber risk, secure the critical information infrastructure, establish information sharing relationships, communications mechanisms, and collaborative arrangements, and institute collaborative arrangements for addressing critical information infrastructure protection issues.

#### **Law Enforcement and Intelligence Branch**

The Law Enforcement and Intelligence branch of NCSA has two primary responsibilities: managing the National Cyber Response Coordination Group and facilitating the coordination of law enforcement and intelligence cyber-related efforts for NCSA. This branch serves as a liaison to the law enforcement and intelligence communities and provides a mechanism for information sharing among the components concerned with cyber issues of law enforcement, intelligence, and the private sector. This information sharing includes all levels of information (classified, law enforcement sensitive, and unclassified).

#### **Strategic Initiatives Branch**

NCSA's Strategic Initiatives branch is organized into seven programs with different responsibilities, as follows:

- The Critical Infrastructure Protection Cyber Security program is responsible for developing a critical infrastructure protection plan for the IT Sector, including the Internet, that will identify critical assets and vulnerabilities, map interdependencies, and promote cyber awareness throughout other sector specific plans.
- The Control Systems Security program is responsible for facilitating control system incident management and security awareness, establishing an assessment capability for vulnerability reduction and incident response, creating a self-sustaining security culture within the control systems community, focusing attention on the protection of legacy control systems, and making strategic recommendations for the future of control systems and security products.
- The Software Assurance program presents a framework for promoting and coordinating efforts to improve the security, reliability, and safety of software.
- The Training and Education program is responsible for promoting the development of an adequate number of effective cyber security professionals, enhancing cyber security capabilities within the federal workforce by identifying the skills and abilities necessary for specific job tasks, and working with other organizations to develop content standards for training products and for certifications.
- The Cyber Exercise program is charged with improving the nation's ability to respond to cyber incidents by creating, sponsoring, and learning from international, national, regional, and interagency exercises. The team is responsible for planning and coordinating cyber security exercises with internal and external DHS stakeholders.
- The Standards and Best Practices/Research and Development Requirements program works to encourage technology innovation efforts. The team is responsible for identifying cyber security research and development requirements and cyber security standards issues, and for assembling and distributing information on best practices.
- The Information Systems Security Line of Business program provides leadership and direction for improving information systems security services across the federal government. The program works to achieve more consistent security management processes and controls across government through the reuse of proven best practices, and by promoting savings through reduced duplication and economies of scale for common hardware, software, and shared services.



## Appendix D

### Federal Agency Incident Categories

| Category | Name                             | Description  | Reporting Timeframe   |
|----------|----------------------------------|--|---|
| CAT 0    | Exercise/Network Defense Testing | This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.   | Not Applicable; this category is for each agency's internal use during exercises.   |
| CAT 1    | Unauthorized Access              | In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource   | Within one (1) hour of discovery/detection.   |
| CAT 2    | Denial of Service                | An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the Denial of Service.  | Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity. |
| CAT 3    | Malicious Code                   | <i>Successful</i> installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus software. | Daily<br>Note: Within one (1) hour of discovery/detection if widespread across agency.  |
| CAT 4    | Improper Usage                   | A person violates acceptable computing use policies.   | Weekly  |
| CAT 5    | Scans/Probes/Attempted Access    | This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.   | Monthly<br>Note: If system is classified, report within one (1) hour of discovery.  |
| CAT 6    | Investigation                    | <i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.  | Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.                   |

## **Appendix E**

### **Major Contributors to this Report**

---

#### **Information Security Audits Division**

Edward G. Coleman, Director  
Jeff Arman, Audit Manager  
Chiu-Tong Tsang, Audit Team Leader  
Jason Bakelar, Information Technology Specialist  
Charles Twitty, Auditor

Tarsha Ross, Referencer

#### **Advanced Technology Division**

David Hawkins, Senior Security Engineer

## Appendix F Report Distribution

---

### **Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
General Counsel  
Executive Secretary  
Assistant Secretary for Policy  
Assistant Secretary for Public Affairs  
Assistant Secretary for Legislative and Intergovernmental Affairs  
Under Secretary for National Protection and Programs  
Assistant Secretary for Office of Cyber Security and Communications  
Chief Information Officer  
Deputy Chief Information Officer  
Chief Information Security Officer  
Director, Compliance and Oversight Program  
Director, National Cyber Security Division  
Director, DHS GAO/OIG Liaison Office  
Chief Information Officer Audit Liaison  
National Protection and Programs Audit Liaison  
National Protection and Programs Information Systems Security Manager  
Director, OIG Information Security Audit Division  
Chief Privacy Officer

### **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) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at [www.dhs.gov/oig](http://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 the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov). The OIG seeks to protect the identity of each writer and caller.