

DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

**Progress and Challenges in Securing
the Nation's Cyberspace**



Office of Information Technology

OIG-04-29

July 2004



**Homeland
Security**

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, investigative, and special reports prepared by the OIG as part of its DHS oversight responsibility to identify and prevent fraud, waste, abuse, and mismanagement.

This report assesses the strengths and weaknesses of the program or operation under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

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

A handwritten signature in black ink, appearing to read "Clark Kent Ervin".

Clark Kent Ervin
Inspector General

Contents

Introduction.....	3
Results in Brief	3
Background.....	5
Progress	8
Challenges.....	10
Recommendations.....	15
Management Comments and OIG Evaluation	16

Appendices

Appendix A: Purpose, Scope, and Methodology	21
Appendix B: Management’s Response	22
Appendix C: Major Contributors to this Report.....	28
Appendix D: Report Distribution	29

Abbreviations

CERT®/CC	CERT® Coordination Center
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
FedCIRC	Federal Computer Incident Response Center
FTE	Full-Time Equivalent
GFIRST	Government Forum of Incident Response and Security Teams
HSOC	Homeland Security Operations Center
IAIP	Information Analysis and Infrastructure Protection
IIMG	Interagency Incident Management Group
IT	Information Technology
NCSD	National Cyber Security Division
OIG	Office of Inspector General
US-CERT	United States Computer Emergency Readiness Team

Introduction

The speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. More and more people are capable of launching significant assaults against the nation's infrastructure and cyberspace because of the increasing sophistication of computer attack tools. As noted by the CERT[®] Coordination Center (CERT[®]/CC), identified computer security vulnerabilities that an attacker can exploit have increased dramatically, with the number of vulnerabilities quadrupling from 1,090 in 2000 to 4,129 in 2002. Industry experts agree that cyber terrorism, in which computer systems become targets, is one of the nation's top five security threats and will likely remain so for years to come.¹

Due to the significance of cyber threats on the United States and their possible consequences, the security of cyber systems is one of the Department of Homeland Security's (DHS) highest priorities. The objectives of our audit were to determine whether DHS' efforts to implement the White House's cyber strategy - *The National Strategy to Secure Cyberspace*² - and to protect the nation's critical infrastructure from a major cyber terrorist attack are adequate and effective. We performed our work at the National Cyber Security Division (NCSA) from December 2003 through February 2004. See Appendix A for a discussion of our purpose, scope, and methodology.

Results in Brief

DHS has begun to implement the actions and recommendations detailed in *The National Strategy to Secure Cyberspace*. With the establishment of NCSA in June 2003, DHS made notable progress in protecting the nation's critical infrastructure from cyber vulnerabilities, threats, and attacks. Major accomplishments include:

- Creation of the United States Computer Emergency Readiness Team (US-CERT). Formed as a partnership between NCSA and the private

¹ *SC Magazine*, December 2002.

² The White House issued *The National Strategy to Secure Cyberspace* in February 2003.

sector, US-CERT serves as the national focal point for computer security efforts.

- Establishment of the National Cyber Alert System, managed by US-CERT, as the means to relay cyber security information to all computer users.
- Participation by NCSA in Dartmouth College's cyber focused communications and coordination exercise (LiveWire).³
- Sponsorship by NCSA of the National Cyber Security Summit to promote information sharing and partnerships with the private sector in securing cyberspace.⁴
- Formation of three new organizations to strengthen federal information technology (IT) defenses and coordinate responses to system threats.⁵

Though NCSA has undertaken some major initiatives, it still faces a number of challenges to address long-term cyber threats and vulnerabilities to the nation's critical infrastructure. Specifically, NCSA has not:

- Prioritized its initiatives to address the recommendations in *The National Strategy to Secure Cyberspace*.
- Identified the resources needed to ensure that it can 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.
- Instituted a formal communications process within DHS, as well as the public, private, and international sectors.

³ Conducted in October 2003, LiveWire was a national communications and coordination exercise designed to test current preparedness, business processes, and communications paths by imitating a variety of cyber attacks and demonstrating interdependencies between the cyber infrastructure and other critical infrastructures.

⁴ As a result of the summit, five task forces, sponsored by the private sector, were formed and reported their findings and recommendations on key security issues facing the United States.

⁵ The three organizations formed were the Government Forum of Incident Response and Security Teams (GFIRST), the Federal Chief Information Security Officers (CISO) Forum, and the Cyber Interagency Incident Management Group (IIMG).

-
- 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.
 - Reviewed or updated the actions and recommendations in *The National Strategy to Secure Cyberspace*.

NCSD must address these issues to reduce the risk that the critical infrastructure may fail due to cyber attacks.

In response to our draft report, IAIP agreed with and has already taken steps to implement each of the recommendations. However, IAIP also said that some of our recommendations have been rendered obsolete or overcome by new circumstances. Based on our assessment of IAIP's specific comments, none of the recommendations have been fully implemented, and therefore, the conditions noted in the report continue to exist. IAIP's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

Critical infrastructures, economy, and national security in the United States are dependent on IT and telecommunications systems. The consequences of a cyber attack on our critical information networks and infrastructures, which are composed of public and private institutions in many different sectors under the guidance of federal lead departments and agencies (illustrated in Figure 1 below), can have a significant negative effect on the United States. The resulting widespread disruption of essential services after a cyber attack could delay the notification of emergency services, damage our economy, and put public safety at risk.

Figure 1

Critical Infrastructure Lead Agencies

Lead Agencies	Sectors
Department of Agriculture	Agriculture Food (meat, poultry, and egg products)
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health Healthcare Food (except meat, poultry, and egg products)
Department of Homeland Security	Information Technology Telecommunications Chemical Transportation Systems Postal and Shipping Emergency Services
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water Water Treatment Systems

In response to the September 11, 2001, terrorist attacks, *The National Strategy for Homeland Security*⁶ was developed to mobilize and organize national homeland security functions to secure the United States from future attacks. *The National Strategy for Homeland Security* organizes homeland security functions into six critical mission areas, including protecting critical infrastructure and key assets. Eight major initiatives come under the area of protecting critical infrastructure and key assets, including the need to secure cyberspace.

As the first step in the long-term effort to secure the nation’s information infrastructure and to provide a framework for protecting cyberspace,⁷ the White House issued *The National Strategy to Secure Cyberspace* in February 2003. This blueprint is an integral part of DHS’ overall mission to protect the nation’s information systems. It highlights actions and recommendations that the federal

⁶ The White House issued *The National Strategy for Homeland Security* in July 2002.

⁷ For the purposes of this audit, cyberspace refers to the interconnected information systems and networks that comprise the Nation’s infrastructure.

government and the private sector should take to address the nation's five cyberspace priorities:

- **Priority I** - A National Cyberspace Security Response System
- **Priority II** - A National Cyberspace Security Threat and Vulnerability Reduction Program
- **Priority III** - A National Cyberspace Security Awareness and Training Program
- **Priority IV** - Securing Governments' Cyberspace
- **Priority V** - National Security and International Cyberspace Security Cooperation

DHS plays a central role in executing *The National Strategy to Secure Cyberspace*. In addition to implementing the actions directly assigned to it, DHS serves as the primary point of contact for the public and private sectors on issues related to cyberspace security. In cooperation with the White House, DHS coordinates and supports implementation of non-federal tasks, such as getting home users and small businesses to secure their connections to cyberspace.

Due to the significance of cyber threats to the nation, the security of cyber systems is one of the highest priorities within DHS. In March 2003, DHS merged several organizational components, which it had inherited, and combined them under its newly formed Information Analysis and Infrastructure Protection (IAIP) Directorate.⁸ IAIP has the responsibility to: (1) identify and assess a broad range of intelligence information concerning current and future threats against the United States; (2) map identified threats against nationwide vulnerabilities; (3) issue timely warnings and advisories for the full spectrum of terrorist threats against the homeland, including physical and cyber events; (4) take appropriate preventive or protective actions to mitigate identified risks and assist in response and recovery efforts; and, (5) carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States.

⁸ The following organizational components were brought together to form DHS' IAIP Directorate: Critical Infrastructure Assurance Office, Federal Computer Incident Response Center (FedCIRC), National Communications System, National Infrastructure Protection Center, and National Infrastructure Simulation and Analysis Center and Energy Security and Assurance Program.

IAIP created NCSD in June 2003 to implement the actions and recommendations described in *The National Strategy to Secure Cyberspace*, as well as to be the national focal point to address cyber security issues in the United States. Its mission includes: (1) identifying, analyzing, and reducing cyber threats and vulnerabilities; (2) disseminating cyber threat warning information; (3) coordinating cyber incident response; and, (4) providing technical assistance in continuity of operations and recovery from cyber incidents.

DHS Is Making Progress

With the creation of NCSD, DHS raised the nation's awareness of the possibility of cyber terrorist attacks and the need to protect critical infrastructures from such attacks. NCSD has undertaken several initiatives to address the actions and recommendations in *The National Strategy to Secure Cyberspace*, including:

- Creation of US-CERT.⁹ In partnership with CERT[®]/CC at Carnegie Mellon University, US-CERT serves as the national focal and coordination point for computer security efforts. US-CERT is charged with analyzing and reducing cyber threats and vulnerabilities; disseminating cyber threat warning information; and, coordinating incident response. The creation of US-CERT satisfies the first recommendation associated with Priority I in *The National Strategy to Secure Cyberspace*. Priority I calls for the creation of a single point of contact for the federal government's interaction with industry and other partners for continual functions, including cyberspace analysis, warning, information sharing, major incident response, and national recovery efforts.
- Implementation of the National Cyber Alert System.¹⁰ This alert system is the nation's first cohesive cyber security system to identify, analyze, and prioritize emerging vulnerabilities and threats. Through security alerts, tips, and bulletins, the system disseminates information on cyber security issues and provides free computer security update and warnings to all computer users who sign up on US-CERT's web site.¹¹ Cyber security alerts are issued when vulnerabilities are identified or exploited. Bi-weekly cyber security tips provide information on best computer

⁹ US-CERT was created in September 2003.

¹⁰ The National Cyber Security Alert System was implemented in January 2004.

¹¹ As of February 9, 2004, over 250,000 users have subscribed to the system. Also, as of March 24, 2004, 6 cyber alerts, 5 security tips and 5 security bulletins have been issued.

security practices, as well as “how-to” information, for all users in both a technical and non-technical format. Security bulletins, also bi-weekly, provide summaries about security issues, notification of new vulnerabilities, potential impact, and actions required to mitigate risk. With the implementation of the National Cyber Alert System, NCSD addresses recommendations that fall under Priority III in *The National Strategy to Secure Cyberspace*.

- Participation in Dartmouth College’s cyber focused communications and coordination exercise (LiveWire). Conducted in October 2003, LiveWire was a large scale exercise designed to test the coordination of private and public sector incident management, response, and recovery capabilities. The results of the exercise are being used as a foundation for DHS’ response capabilities to a cyber attack, and to plan for LiveWire II, which began in February 2004. As recommended under Priority I in *The National Strategy to Secure Cyberspace*, DHS uses exercises to evaluate the impact of cyber attacks on government-wide processes and to test the coordination of public and private sector incident management, response, and recovery capabilities.
- Hosting the National Cyber Security Summit.¹² This summit was designed to strengthen partnerships between NCSD and the private sector, and focused on addressing key security issues facing the United States. Five private sector task forces were formed during the summit: Awareness for Home Users and Small Businesses; Cyber Security Early Warning, Best Practices and Standards; Corporate Governance, Best Practices and Standards; Technical Standards and Common Criteria; and Security Across the Software Development Life Cycle: Secure Software. These task forces will recommend strategies to address the national cyberspace priorities outlined in *The National Strategy to Secure Cyberspace*.
- Establishment of three new organizations to strengthen federal IT defenses, coordinate responses to systems threats, and improve information sharing. Facilitated by NCSD, the three organizations - GFIRST, Federal CISO Forum, and Cyber IIMG - are composed of management officials from the federal government. GFIRST was established to share operational incident response data, tools,

¹² The National Cyber Security Summit was hosted by NCSD in December 2003.

technologies, and techniques between security practitioners across the federal government. The Federal CISO Forum was launched to provide a trusted environment for agencies to share positive and negative experiences with technology and applications. Through the Cyber IIMG, NCSO formed a group to address cyber attack attribution issues, as well as a working group to discuss threat scenarios and mitigation tactics and techniques. As recommended under Priority I in *The National Strategy to Secure Cyberspace*, these organizations will work together to remove impediments to information sharing about cyber security and infrastructure vulnerabilities within the federal government.

In addition, NCSO is establishing programs with the National Science Foundation, the National Security Agency, and other federal agencies to educate, train, and certify students and professionals on information assurance and cyber security. NCSO plans to launch a US-CERT cyber exchange partnership program during 2004. This program will provide public and private organizations active in cyber security watch, warning, and response activities with a trusted forum to exchange and coordinate information and events. Also, NCSO is participating in international forums to promote the international aspects of protecting critical infrastructures from cyber terrorism. These activities directly address priorities established in *The National Strategy to Secure Cyberspace*.

Challenges Remain In Developing a U.S. Cyber Protection Program

Despite the progress made, DHS faces significant challenges in developing and implementing a program to protect our national cyber infrastructure. DHS has experienced delays in establishing its structure, which includes defining its budget and staffing requirements, and faces a number of additional challenges in instituting the enhanced cyber threat analysis organization that is needed to address long-term threats and vulnerabilities to the nation's critical infrastructure.

Prioritize Initiatives and Establish Milestones

NCSO has not prioritized its initiatives or established individual milestones and benchmarks. There is little assurance that NCSO can successfully address the actions and recommendations in *The National Strategy to Secure Cyberspace* in a timely manner if milestones are not established. Milestones are needed to monitor the implementation of the actions and recommendations. Additionally, NCSO cannot substantiate its budget and staffing needs, validate its organizational structure, develop performance measures, or coordinate and oversee efforts to

mitigate long-term cyber security vulnerabilities and threats if these initiatives are not prioritized.

Because its goals and initiatives have not yet been prioritized, NCSD's branch chiefs assign staff to so-called mission critical tasks and activities, without official input or oversight from management. The director of NCSD, who did not report to DHS until mid-October 2003, first began conducting weekly staff meetings to discuss priorities in February 2004.

Resource Requirements Identification

NCSD has not identified its long-term budget or resource requirements based on the priorities that must be established to carry out its mission. During a four month period, NCSD drafted three different organizational structures. Each was a refinement that permitted NCSD to align its areas of focus with its available resources and tasks. The finalization of its organizational structure is necessary for NCSD to establish its long-term budget and staffing requirements, develop strategic plans, implement performance measures, and oversee efforts to address the recommendations in *The National Strategy to Secure Cyberspace*.

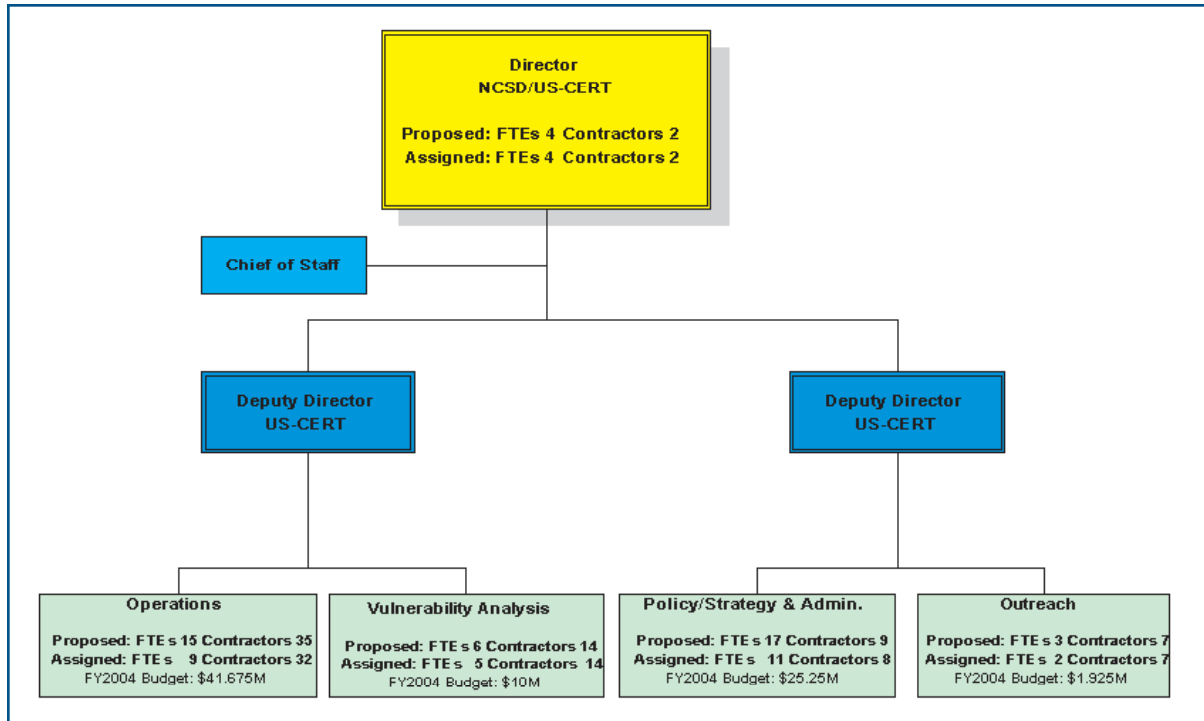
IAIP provided NCSD with a budget of \$78.85 million and 29 full-time equivalent (FTE) staff for fiscal year 2004. NCSD also relies heavily on contractors to address many of its initiatives and tasks. According to NCSD management officials, additional resources will be needed as the division's priorities and structure become better defined. As of February 23, 2004, NCSD had a staff of 84 (21 FTEs and 63 contractors).

NCSD has estimated that a staff of 112 (45 FTEs and 67 contractors), and a proposed budget of \$79.62 million will be needed to accomplish the goals IAIP has proposed for FY 2004.¹³ Though NCSD's 2004 estimates are not based on the division's priorities or initiatives, efforts are under way to justify staffing and budget increases based on the priorities established in *The National Strategy to Secure Cyberspace*, such as the assessment of threats and vulnerabilities to federal cyber systems. Remediation plans then can be developed to secure the government's cyberspace.

¹³ See Figure 2 for NCSD's proposed staffing and budget as of February 23, 2004.

Figure 2

NCSO Organization (as of February 23, 2004)



Strategic Plans and Performance Measures

NCSO has not developed a strategic plan, with specific goals, objectives, and milestones, to implement its initiatives and to ensure that processes coincide with the national priorities and recommendations in *The National Strategy to Secure Cyberspace*. An approved strategic implementation plan helps ensure that processes are established and that NCSO is focusing on the critical tasks necessary to secure the nation’s critical cyber infrastructure. Additionally, performance measures are needed to allow management to assess NCSO’s progress in addressing priorities and attaining strategic goals and milestones. NCSO cannot track in an efficient and effective manner its or other public and private organizations’ progress in implementing *The National Strategy to Secure Cyberspace* if performance measures are not developed and monitored.

Only one branch within NCSO, Vulnerability Analysis, has drafted a plan formally to document its strategic and performance goals and objectives. The

plan, however, has not been reviewed or approved by NCSO management. NCSO needs to ensure that each branch develops and implements strategic plans and processes that are focused on the priorities and processes that will enable it to accomplish its mission. In addition, the performance measures that will be used to evaluate NCSO's progress in building an effective organization capable of mitigating long-term cyber threats and vulnerabilities should be addressed within each branch's strategic plan.

In February 2002, the Office of Management and Budget reported to Congress that the lack of performance measures was one of six common government-wide security weaknesses. As documented in *The National Strategy to Secure Cyberspace*, each federal department and agency will be accountable for its performance on cyber security efforts and be responsible for employing performance measures to evaluate progress in implementing the recommendations in *The National Strategy to Secure Cyberspace*. Also, the performance measures utilized should allow agencies to make resource allocation decisions and adjust priorities accordingly.

Improve Formal Communications

NCSO has not instituted a formal communications process within DHS, or within the government, private, intelligence, or international communities. In addition, NCSO has not determined how best to communicate US-CERT's mission, roles, and responsibilities to its partners. The communications process is critical to ensuring that the assistance DHS is providing to secure cyber systems and infrastructures will be utilized by the public and private sectors, and to encouraging the sharing of critical cyber threat and vulnerability information. This includes any pertinent intelligence information, so that NCSO has the information it needs to accomplish its mission. Priority I of *The National Strategy to Secure Cyberspace* calls for DHS to raise awareness and remove impediments to information sharing regarding cyber security and infrastructure vulnerabilities between the public and private sectors, too. DHS cannot address this recommendation effectively without a formal communications process.

NCSO and the Homeland Security Operations Center (HSOC) communicate and share cyber threat information on a daily basis. This process is an effective way to ensure that NCSO receives all cyber-related threat information that comes into HSOC. NCSO communicates with DHS' Chief Information Security Officer (CISO) and other federal agencies, too, including the intelligence and law enforcement communities on a regular basis. Many of these communications,

however, are on an ad hoc basis, relying on personal relationships NCS D personnel have developed with people over the years. The reliance on personal relationships for key communications is risky and could result in NCS D's not receiving or sharing critical cyber security information if those contacts are not available or if the person initiating the contact no longer works for NCS D or DHS.

In interviews with government and private sector partners, we learned that NCS D's mission, structure, and roles and responsibilities are not adequately communicated to its partners in the public and private sectors. Several partners interviewed suggested that the government's communication mechanisms need to be improved, e.g., use of advertising has not been used to reach the public at large.

Effectively Oversee and Provide Guidance

NCS D has not developed a formal process to oversee or provide guidance on cyberspace security issues to DHS, other federal, state, and local governments, and the private sector. According to NCS D management officials, oversight responsibilities were not formally established or specifically addressed with the creation of the division.

The National Strategy to Secure Cyberspace is but a first step in a long-term effort to secure the nation's information infrastructure. The federal government is to continue broad partnerships in the public and private sectors to develop, implement, and refine *The National Strategy to Secure Cyberspace*. DHS has been assigned the central role in its implementation. It is responsible for overseeing federal department and agency plans and programs to execute the initiatives assigned; coordinating and supporting the implementation of recommended non-federal tasks; providing the guidance to address the tasks assigned; and, periodically refining *The National Strategy to Secure Cyberspace*.

Through its Outreach Branch, NCS D is coordinating with other government agencies and private sector organizations; multi-state, IT, and sector Information Sharing and Analysis Centers; and DHS' Office of the Chief Information Officer on critical infrastructure protection issues. It is not, however, actively overseeing the performance of those entities. Meanwhile, NCS D is relying on the National Institute of Standards and Technology to establish guidance for cyber security. Effective oversight and guidance by DHS is needed to ensure that all federal, state, and local government agencies, as well as the private sector, are properly securing their own critical infrastructures.

Recommendations

We recommend that the Under Secretary for IAIP direct the Assistant Secretary for Infrastructure Protection:

Recommendation #1:

Prioritize NCSD's initiatives and establish milestones based on the funding available. A plan for ensuring the completion of priorities needs to be developed and tied to specific milestone completion dates.

Recommendation #2:

Finalize NCSD's organizational structure, with supporting budget and staffing levels for each branch. To do this, NCSD should obtain IAIP management's approval of the budget and resources needed to carry out its mission and implement *The National Strategy to Secure Cyberspace*. Approved budget resources and staffing can then be allocated to each branch.

Recommendation #3:

Ensure that NCSD and each branch develop strategic implementation plans identifying milestones and completion dates that coincide with the division's priorities, the roles and responsibilities of its staff, and the tasks needed to implement *The National Strategy to Secure Cyberspace*. Management should approve these plans and use them to monitor and evaluate NCSD's progress in accomplishing its initiatives, priorities, and tasks.

Recommendation #4:

Develop performance measures that can be used to determine the progress DHS and all other responsible organizations (public and private sector) are making in addressing the actions and recommendations in *The National Strategy to Secure Cyberspace*. The performance measures should be reviewed periodically to ensure that they are being met.

Recommendation #5:

Define and communicate the roles and responsibilities of the division, its branches, and its staff. Develop a plan to improve NCSD's communications

with its public and private sector partners, including home users, on its structure, mission, and roles as well as responsibilities regarding cyber security awareness and protection.

Recommendation #6:

Develop and document a process to communicate and share information obtained on cyber vulnerabilities, threats, and incidents with key federal, state and local government intelligence and law enforcement agencies.

Recommendation #7:

Initiate and implement a process to oversee DHS and other federal, state, and local government efforts to protect their respective critical infrastructures from cyber vulnerabilities and threats.

Recommendation #8:

Develop and issue necessary guidance and directives on protecting critical infrastructures from cyber vulnerabilities and threats and improving security.

Recommendation #9:

Review and refine periodically the actions and recommendations in *The National Strategy to Secure Cyberspace*.

Management Comments and OIG Evaluation

We obtained written comments (Appendix B) on a draft of this report from IAIP. Generally, IAIP agreed with the report's findings and recommendations and said that significant advancements in addressing all of the recommendations have been made. However, IAIP also said that some of our recommendations have been rendered obsolete or overcome by new circumstances. Based on our assessment of IAIP's specific comments, none of the recommendations have been fully implemented, and therefore, the conditions noted in the report continue to exist. Below is a summary of IAIP's response to each recommendation and our assessment of the response.

Recommendation #1: Prioritize NCSD’s initiatives and establish milestones based on the funding available. A plan for ensuring the completion of priorities needs to be developed and tied to specific milestone completion dates.

IAIP agreed that the formulation of milestones is an important step to achieve results and to execute a plan. In March and early April 2004, NCSD created detailed internal milestones, including completion dates and priorities. This information was tied to budget figures and submitted to the United States House of Representatives Select Committee on Homeland Security in May 2004. Correspondingly, each branch within NCSD has been engaged in updating their respective milestones and in correlating those milestones to manpower needs and funding requirements for fiscal years 2004, 2005, and 2006.

We accept IAIP’s response that milestones have been established based on funding available. NCSD still needs to develop a plan to ensure that milestones are prioritized and the timelines for completing milestones are being met. NCSD should provide us with a copy of the plan.

Recommendation #2: Finalize NCSD’s organizational structure, with supporting budget and staffing levels for each branch. To do this, NCSD should obtain IAIP management’s approval of the budget and resources needed to carry out its mission and implement *The National Strategy to Secure Cyberspace*. Approved budget resources and staffing can then be allocated to each branch.

IAIP agreed with our recommendation. On March 18, 2004, NCSD finalized and implemented the division’s organizational structure. NCSD will continually assess its organizational structure for operational efficiency and expects to release a revised version of the organizational structure in the third quarter of 2004. An initial budget and staffing plan has also been developed, and the current budget justification cycle is being utilized to refine and to accurately reflect the organizational structure for the FY 2005 and FY 2006 budget submission.

We agree that the steps that NCSD has taken, and plans to take, satisfies this recommendation.

Recommendation #3: Ensure that NCS D and each branch develop strategic implementation plans identifying milestones and completion dates that coincide with the division’s priorities, the roles and responsibilities of its staff, and the tasks needed to implement *The National Strategy to Secure Cyberspace*. Management should approve these plans and use them to monitor and evaluate NCS D’s progress in accomplishing its initiatives, priorities, and tasks.

IAIP accepted and is implementing this recommendation.

We accept IAIP’s response to our recommendation. NCS D should provide us with specific dates when it expects their strategic implementation plans will be completed and approved.

Recommendation #4: Develop performance measures that can be used to determine the progress DHS and all other responsible organizations (public and private sector) are making in addressing the actions and recommendations in *The National Strategy to Secure Cyberspace*. The performance measures should be reviewed periodically to ensure that they are being met.

IAIP is currently working with each of the Department’s directorates and divisions to develop performance measures and metrics. NCS D agreed to work within the framework of performance measures and metrics for the overall infrastructure protection program. When complete, these performance measures and metrics will provide a basis for continuous measurement and improvement across DHS.

We agree that NCS D has taken steps to address the intent of this recommendation. NCS D should also develop performance measures for the public and private sector organizations that are responsible for addressing the actions and recommendations in *The National Strategy to Secure Cyberspace*. NCS D should provide us with a copy of the performance measures and timeline for periodically reviewing the performance measures to ensure that they are being met.

Recommendation #5: Define and communicate the roles and responsibilities of the division, its branches, and its staff. Develop a plan to improve NCS D’s communications with its public and private sector partners, including home users, on its structure, mission, and roles as well as responsibilities regarding cyber security awareness and protection.

IAIP agreed and recognized the importance of defining and communicating the roles and responsibilities of NCSO to its branches and staff. IAIP agreed that the goal for increased public awareness of the roles and responsibilities of NCSO is a critical component to accomplish its mission. NCSO designed the US-CERT, launched the National Cyber Alert System, and has undertaken a number of programs geared toward sharing information and developing working partnerships with the public and private sectors. NCSO also has submitted a detailed outreach plan for calendar year 2004 that outlines a public outreach campaign for communications.

We agree that the steps NCSO has taken, and plans to take, satisfy the intent of this recommendation. NCSO should provide us with a copy of the outreach plan.

Recommendation #6: Develop and document a process to communicate and share information obtained on cyber vulnerabilities, threats, and incidents with key federal, state and local government intelligence, and law enforcement agencies.

IAIP agreed with our recommendation. NCSO is reviewing draft standard operating procedures on how its operations group handles, assesses, and coordinates emerging cyber related events. These procedures will continually evolve and mature over time.

We agree that the steps NCSO has taken satisfy the intent of this recommendation. NCSO should provide us with a copy of the approved standard operating procedures.

Recommendation #7: Initiate and implement a process to oversee DHS and other federal, state, and local government efforts to protect their respective critical infrastructures from cyber vulnerabilities and threats.

IAIP accepted this recommendation and has active programs already being implemented to address the recommendation.

We accept IAIP's response. NCSO should create a timeline to track the implementation of these active programs.

Recommendation #8: Develop and issue necessary guidance and directives on protecting critical infrastructures from cyber vulnerabilities and threats and improving security.

IAIP agreed with our recommendation. NCSD has issued guidance on protecting critical infrastructures from cyber threats and on the general improvement of security.

We accept IAIP's response. NCSD should create a timeline for issuing directives on protecting critical infrastructures for both the public and private sectors.

Recommendation #9: Review and refine periodically the actions and recommendations in *The National Strategy to Secure Cyberspace*.

IAIP agreed with the intent of this recommendation. NCSD monitors many of its initiatives, and will improve its evaluation and analysis process, in the context of the actions and recommendations in *The National Strategy to Secure Cyberspace*, as well as the other strategic documents.

We agree that the steps NCSD has taken, and plans to take, satisfies the intent of this recommendation.

Purpose, Scope, and Methodology

The objective of our audit was to determine whether DHS' efforts to protect the nation's critical infrastructure from a major cyber terrorist attack are adequate and effective. Our audit focused on NCSD, within DHS' IAIP directorate. We determined whether: (1) NCSD's organizational structure was established to fulfill its assigned roles and responsibilities; (2) NCSD has developed effective implementation plans; and, (3) NCSD is performing its oversight responsibilities as outlined in *The National Strategy to Secure Cyberspace*.

We conducted our audit between December 2003 and February 2004 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards. To fulfill our audit objective, we interviewed IAIP officials; NCSD's Director, Deputy Directors, branch chiefs and staff; and other federal and non-government officials who work in coordination with NCSD. We reviewed *The National Strategy for Homeland Security*, the Homeland Security Act of 2002, *The National Strategy to Secure Cyberspace*, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, and Homeland Security Presidential Directive 7. We used these documents as criteria for DHS' roles and responsibilities in identifying, preventing, responding to, and recovering from cyber attacks. Also, we reviewed documentation pertaining to IAIP and NCSD, including presentations, press releases, congressional testimony, organizational charts, websites, and various news articles. In addition, we assessed NCSD's progress in implementing the actions and recommendations from *The National Strategy to Secure Cyberspace*.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology, (202) 254-4100, and Edward G. Coleman, Director, Information Security, (202) 254-5444. Major OIG contributors to the audit are identified in Appendix C.

U.S. Department of Homeland Security
Washington, DC 20407



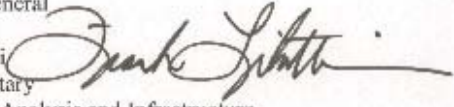
Homeland
Security

July 1, 2004

MEMORANDUM FOR:

Clark Kent Ervin
Inspector General

FROM:

Frank Libutti 
Under Secretary
Information Analysis and Infrastructure
Protection Directorate

SUBJECT:

OIG Draft Report - *Progress and Challenges in Securing
the Nation's Cyberspace* (OIG-IT-03-005)

The purpose of this memorandum is to provide the Information Analysis and Infrastructure Protection Directorate's (IAIP) response to your draft report regarding the National Cyber Security Division's (NCSD) efforts to implement *The National Strategy to Secure Cyberspace* ("*The National Strategy*"). Thank you for the opportunity to comment on your report prior to its publication.

NCSD believes the report to be a fair assessment of the state of the national cyber security program and of NCSD, as of February 2004. As noted in the report, since its formation in June 2003, NCSD made significant strides in implementing *The National Strategy* although much work remained. Since February 2004, NCSD has continued to make considerable progress in implementing *The National Strategy*, and has made significant advancement in addressing all nine of your recommendations. Our comments below speak to this and are intended to provide you with an update on the initiatives underway at NCSD. Please note that due to the passage of time between the field work on this job and issuance of the report, some recommendations have been rendered obsolete because they have already been implemented, and other recommendations have been overcome by new circumstances. (Specific comments on the report's recommendations are contained in the Attachment to this memo and technical comments have been forwarded separately.)

As an overall comment, the report does not completely outline all of NCSD's initiatives and accomplishments. For example, the report does not acknowledge the substantial efforts expended to create a National Cyberspace Security Response System- the first priority within *The National Strategy*. The report asserts that this priority was satisfied through NCSD's creation of US-CERT and the partnership with CERT/CC. It does not acknowledge, however, the number of programs underway within US-CERT designed to create the 24x7x365 operational capabilities necessary to analyze and coordinate cyber events.

As another example of how the report does not detail NCSD accomplishments, the report cites NCSD's National Cyber Alert System as the means through which NCSD disseminates information on cyber security issues. The National Cyber Alert System is only one of many means at NCSD's disposal to engage the public and private sectors on cyber security issues. The primary vehicles through which DHS communicates cyber threat information to the private sector are as follows: (1) the US-CERT public website at www.us-cert.gov, (2) the National Cyber Alert System (3) HSI/US-CERT Portal, (4) the Information Sharing and Analysis Centers (ISACs) in each of the critical infrastructure sectors, and (5) direct interaction with 24x7 Computer Emergency Response Teams (CERT Teams).¹ NCSD also produces a daily cyber briefing based upon open-source research that is widely distributed through email and another key accomplishment- the HSI/US-CERT portal.

Although staff expressed this in interviews, it bears repeating that the rapid and dynamic environment in which DHS operates should be noted in the report. As with any newly-formed organization, the rate of change- both organizationally and programmatically- is significant and presents unique challenges not facing other government organizations. As a result, some programs within DHS, including several of the cyber security programs discussed in the OIG report, are executed quickly to show immediate value and tactical progress and are later modified over time to address more strategic issues. The OIG report makes no mention of this type of execution.

IAIP authorizes the public release of these comments and evaluations. Again, we appreciate the opportunity to comment on this report. If you have any questions regarding our comments, please contact John Daley, IAIP Audit Liaison, at 202-282-8381.

Attachment

¹ Actually, in discussing the formation of GFI/ST, the Federal CISO Forum, and the Cyber IIMG, a helpful fact to include would be that these groups collaborate securely through the HSI/US-CERT portal.

Attachment

Specific Comments on the Recommendations contained in OIG-IT-03-005 (Progress and Challenges in Securing the Nation's Cyberspace).

1. *Prioritize NCSD's initiatives and establish milestones based on the funding available. A plan for ensuring the completion of priorities needs to be developed and tied to specific milestone completion dates.*¹

NCSD agrees that the formulation of milestones is an important step to achieve results and to execute a plan. Similarly, NCSD created detailed internal milestones- including completion dates and priorities- in March and early April of 2004. This information was tied to budget figures and submitted to the United States House of Representatives Select Committee on Homeland Security in May 2004.

The need to continually review and reassess is critical to the implementation of milestones in relation to the dynamic environment in which NCSD operates. Correspondingly, each branch within NCSD has been engaged in continually updating their respective milestones and in correlating those milestones to both manpower needs and funding requirements for fiscal year FY04, FY05, and FY06.

2. *Finalize NCSD's organizational structure with supporting budget and staffing levels for each branch. To do this, NCSD should obtain the approval of the budget and resources needed to carry out its mission and to implement The National Strategy to Secure Cyberspace from LAMP management. Approved budget resources and staffing can then be allocated to each branch.*

On March 18, 2004, NCSD finalized and implemented the division's organizational structure, a revised version of the one referenced on page 10 of the Progress Report.² NCSD's organizational structure is continually assessed for operational efficiency and NCSD expects to release a revised version of the organizational structure in Q3 2004. Efficiency in growing any organization mandates active review of current organizational charts and continual fine tuning.

NCSD has developed an initial budget and staffing plan which is continually reviewed and refined. Furthermore, NCSD has utilized the current budget justification cycle to refine and to more accurately reflect the organizational structure in the FY05 and FY06 budget submission.

3. *Ensure that NCSD and each branch develop strategic implementation plans identifying milestones and completion dates that coincide with the division's priorities, the roles and responsibilities of its staff, and the tasks needed to implement The National Strategy to Secure Cyberspace. Management should approve these plans and use them to monitor and to evaluate NCSD's progress in accomplishing its initiatives, priorities, and tasks.*

¹ On page 9 of the Progress Report, the Inspector General states that the Director of NCSD first commenced weekly meetings to discuss priorities in February 2004, when in fact weekly meetings with the Director regarding priorities commenced shortly after the Director's arrival in December of 2003.

² On page 9 of the Progress Report, the Inspector General states "NCSD drafted three different organization structures." This claim is factually inaccurate.

NCSD accepts and is implementing this recommendation.

4. Develop performance measures that can be used to determine the progress DHS and all other responsible organizations (public and private sector) are making in addressing the actions and recommendations in The National Strategy to Secure Cyberspace. The performance measures should be reviewed periodically to ensure that they are being met.

DHS is currently working across the Department and within each of the Directorates and Divisions to develop performance measures and metrics. NCSD is currently working within the framework of performance measures and metrics for the overall infrastructure protection program. When complete, these performance measures and metrics will provide a basis for continuous measurement and improvement across all of the branches of NCSD, across all of the Divisions in the Office of Infrastructure Protection, and across all of the Directorates that comprise DHS.

5. Define and communicate the roles and responsibilities of the division, its branches, and its staff. Develop a plan to improve NCSD's communications with its public and private sector partners including home users on its structure, mission, and roles as well as responsibilities regarding cyber security awareness and protection.

NCSD agrees that defining and communicating the roles and responsibilities of NCSD to its branches and staff is an important mission requirement.

NCSD designed the US-CERT, a partnership effort aimed directly at the public and private sectors. Pursuant to this public/private partnership, on January 28, 2004, US-CERT launched its National Cyber Alert System for both technical and non-technical audiences. The National Cyber Alert System is designed to notify recipients of severe cyber security events such as a new vulnerability or exploit and to mitigate against the threat in coordination with guidance on the recommended measures. Additionally, NCSD hosted the National Cyber Security Summit in December 2003 which was designed to improve communications between the public and private sectors. As these programs mature and develop, NCSD will review and augment as necessary.

Since April, NCSD has established working relationships with The National Cyber Security Alliance, Educause, the MS-ISAC, the National Association of State Chief Information Officers (NASCIO) and others to establish a series of programs geared towards home users, small businesses, state and local government, K-12 and higher education that focus specifically on their needs and level of understanding. DHS also provides cyber security tips to home users and small businesses through the National Cyber Security Alliance StaySafeOnline campaign to educate all users about basic security practices and to increase overall awareness. DHS is currently developing cyber security tool kits in partnership with the Alliance that can be disseminated to both home users and small businesses.

With respect to communicating within the public sector, NCSD would like to highlight the substantial progress made when it created Cyber Interagency Incident Management Group (Cyber IIMG), Chief Information Security Officers Forum (CISO Forum), and Government Forum of Incident Response and Security Teams (GFIRST). These groups already have

increased horizontal information sharing across somewhat stove-piped organizations and improved the overall cyber preparedness of the U.S. Government. These forums directly address Priority IV of *The National Strategy: Securing Government's Cyberspace* and they facilitate information sharing and cooperation that contribute to a variety of efforts throughout the Strategy.

The goal for increased public awareness of the roles and responsibilities of NCSD is a critical component to mission accomplishment. NCSD has attempted to issue a number of press releases and to engage public discourse on key initiatives or around certain key events. NCSD also has submitted a detailed outreach plan for calendar year 2004 that outlines a public outreach campaign for communications.

6. *Develop and document a process to communicate and share information obtained on cyber vulnerabilities, threats, and incidents with key federal, state and local government intelligence and law enforcement agencies.*

NCSD is reviewing draft-standard operating procedures on how its operations group handles, assesses and coordinates emerging cyber related events. These procedures will continually evolve and mature over time.

7. *Initiate and implement a process to oversee DHS and other federal, state, and local government efforts to protect their respective critical infrastructures from cyber vulnerabilities and threats.*

NCSD accepts this recommendation and has active programs already being implemented to address the recommendation. Several programs include but are not limited to the following: US-CERT, the Cyber Interagency Incident Management Group (C-IIMG), the Government Forum for Incident Response and Security Teams (GFIRST), the Chief Information Security Operators Forum (CISO) Forum, the National Cyber Alert System, Cyber component of DHS' Homeland Security Presidential Directive 7 ("HSPD 7") and Interagency Security Planning Effort, partnership with Multi-State Information Sharing and Analysis Center (MS-ISAC), the Homeland Security Information Network (HSIN)/US-CERT Portal, the US-CERT Control System Center, a US-CERT Control System Center test bed initiative in partnership with INEEL National Labs, a national web cast initiative, and partnership with National Association of State Chief Information Officers (NASCIO).

8. *Develop and issue necessary guidance and directives on protecting critical infrastructures from cyber vulnerabilities and threats and improving security.*

From time-to-time, NCSD issues appropriate guidance on protecting critical infrastructures from cyber threats and on the general improvement of security as a part of and in addition to the aforementioned programs listed in response to recommendation 7. For example, NCSD has issued cyber guidance to sector specific agencies as part of DHS' HSPD 7 initiative and sector specific plan development. In addition, NCSD has initiated a series of web casts to provide Americans with information and guidance on cyber security preparedness and response. Lastly, The National Cyber Alert System has issued several alerts and best practices guides to the public.

9. *Periodically review and refine the actions and recommendations in The National Strategy to Secure Cyberspace.*

NCSD monitors many of its initiatives in the context of the actions and recommendations in *The National Strategy* as well as the other strategic documents. For example, in preparing internal milestones and budget, NCSD leveraged *The National Strategy* to organize the accomplishments necessary to achieve the broader goals contained in the strategy. NCSD periodically measures progress against the action and recommendations and is maturing processes necessary to track progress toward the action and recommendations contained in *The National Strategy* across both private and public sectors.

In late March 2004, NCSD prepared a draft progress report designed to detail Federal agency progress in implementing *The National Strategy*. Much of the content from this report formed the basis of NCSD's response to a written request for information from the United States House of Representatives Select Committee on Homeland Security. This was drafted in April 2004 and delivered to Congress in May of 2004.

NCSD will continue to improve its evaluation and analysis of its performance against the actions and recommendations of *The National Strategy* as well as the other strategic documents referenced above.

Office of Information Technology
Information Security Audits Division

Edward G. Coleman, Director
Barbara Bartuska, Audit Manager
Jeff Arman, Audit Manager
Chelsea Pickens, Senior IT Auditor
Foxhall Parker, IT Auditor
Meghan Sanborn, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
DHS OIG Liaison
DHS Public Affairs

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.

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 Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.