Department of Homeland Security
Office of Inspector General

Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure

(Redacted)

OIG-11-89

June 2011

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

Homeland
Security

June 10, 2011

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 progress that DHS' National Protection and Programs Directorate (NPPD) has made in implementing the actions and recommendations outlined in *The National Strategy to Secure Cyberspace*, the National Infrastructure Protection Plan, and the Comprehensive National Cybersecurity Initiative. This report also includes an assessment of security controls on two systems containing critical cyber infrastructure information. This report is based on a review of internal policies and procedures; interviews with management officials, employees within Office of Cybersecurity and Communications, and system administrators and contractor personnel within the Office of Infrastructure Protection; physical security assessments; system security vulnerability assessments; direct observations, and a review of applicable documentation.

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. We trust 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.

Frank W. Deffer
Assistant Inspector General, IT Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

ACAMS	Automated Critical Asset Management System
CII	Critical Infrastructure Information
CIKR	critical infrastructure and key resources
CNCI	Comprehensive National Cybersecurity Initiative
CS&C	Cybersecurity and Communications
DC2	Data Center 2
DHS	Department of Homeland Security
DOE	Department of Energy
FY	fiscal year
HSPD	Homeland Security Presidential Directive
IICS	Infrastructure Information Collection System
IP	Infrastructure Protection
ISAC	Information Sharing and Analysis Center
IT	information technology
LENS	Linking Encrypted Network System
NCS	National Communications System
NCSD	National Cyber Security Division
NIPP	National Infrastructure Protection Plan

NIST	National Institute of Science and Technology
NPPD	National Protection and Programs Directorate
OEC	Office of Emergency Communications
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCII	Protected Critical Infrastructure Information
PCIIMS	PCII Management System
SQL	Structured Query Language
US-CERT	United States Computer Emergency Readiness Team

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

Cybersecurity risks pose some of the most serious economic and national security challenges our Nation faces. DHS is the principal focal point for the security of cyberspace and the national effort to protect critical infrastructure and key resources. Under the department's NPPD, the Office of Cybersecurity and Communications is responsible for enhancing the security, resiliency, and reliability of the Nation's cyber and communications infrastructure. The Office of Infrastructure Protection leads the national effort to mitigate terrorism risk to, strengthen the protection of, and enhance the all-hazard resilience of the Nation's critical infrastructure.

We evaluated the department's progress in addressing the open actions and recommendations in *The National Strategy to Secure Cyberspace*, the National Infrastructure Protection Plan, and the Comprehensive National Cybersecurity Initiative. We also determined whether effective physical and system security controls have been implemented on two of the systems that contain the Nation's critical cyber infrastructure and asset information.

DHS has made progress in working and sharing information with federal, state, and local governments and the public sector; raising cybersecurity awareness; and implementing educational programs that focus on cybersecurity. However, significant work remains to address the open actions and recommendations and attain the goals outlined in the *Strategy*, National Infrastructure Protection Plan, and Comprehensive National Cybersecurity Initiative. Overall, robust planning and the development of performance measures are needed to reduce cyber risks, threats, and vulnerabilities, in addition to deterring harm to critical infrastructures. Furthermore, a properly trained workforce and the mitigation of configuration and account access vulnerabilities are necessary to ensure the confidentiality, integrity, and availability of the department's critical infrastructure and asset data and the systems used to

capture, store, and protect that information from unauthorized access and misuse.

This report makes 10 recommendations. Management has already begun to take the actions to implement the recommendations. The response from the Under Secretary, NPPD, is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber-optic cables that allow our Nation's critical infrastructures to work. The cyber infrastructure includes electronic information and communications systems and services and the data contained therein. The internet is part of our cyber infrastructure. The internet has been identified as a key resource, comprising domestic and international assets within both the information technology (IT) and communications sectors, and is used by all sectors to varying degrees. These sectors include energy, transportation, finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense, and food and agriculture.

A network of networks supports the operation of all sectors of our economy. Attacks on our Nation's information networks can have serious consequences, such as disrupting critical operations, causing loss of revenue and intellectual property, or causing loss of life. A network of networks supports the operation of all sectors of our economy. Countering such attacks requires the development of new risk mitigation capabilities if we are to—

- Reduce vulnerabilities.
- Deter those with the capabilities and intent to harm our Nation's critical infrastructures.
- Ensure the confidentiality, integrity, and availability of our information and communications systems, and the critical infrastructure data contained on these systems.

Recognizing the challenges and opportunities inherent in securing cyberspace, the President identified cybersecurity and the establishment of related performance metrics as key management priorities of his administration. Cybersecurity involves the protective measures needed to secure cyberspace and the cyber infrastructure. It also involves the restoration of the systems and the data contained therein to ensure confidentiality, integrity, and availability.

The underlying guidance for securing cyberspace and critical cyber infrastructures includes the following:

- *The National Strategy to Secure Cyberspace* – Issued in February 2003, the *Strategy* was developed to help reduce our Nation's vulnerability to debilitating attacks against our critical information infrastructures and the physical assets that support them. The *Strategy* provides an initial framework for both organizing and prioritizing federal agencies' roles in securing cyberspace. The *Strategy* is focused on improving the national response to cyber incidents, reducing threats and vulnerabilities to potential exploits, preventing cyber attacks against critical U.S. infrastructure, and improving the international management of and response to such risks and harm.

- National Infrastructure Protection Plan (NIPP) – Updated and reissued in 2009, the NIPP provides the unifying structure to integrate existing and future critical infrastructure and key resources (CIKR). It addresses the protection of the cyber elements of CIKR in an integrated manner rather than as a separate consideration. Our Nation's economy and national security are highly dependent on the global cyber infrastructure, which has created an interconnected and interdependent global network. The global network links the physical and cyber elements of CIKR. Cyber interdependence presents a unique challenge for all sectors.

- Comprehensive National Cybersecurity Initiative (CNCI) – Launched by the White House in January 2008 in National Security Presidential Directive 54/Homeland Security Presidential Directive (HSPD) 23, the CNCI consists of a number of mutually reinforcing initiatives designed to help secure the U.S. in cyberspace. Its goals include (1) enhancing shared situational awareness of network vulnerabilities, threats, and events in the federal government and acting quickly to reduce our current vulnerabilities and prevent intrusions; (2) enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technology; and (3) strengthening the future cybersecurity environment by expanding cyber education, coordinating and redirecting research and development efforts across the federal government, and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

DHS serves as the federal agencies' lead in assessing, mitigating, and responding to cyber risks in collaboration with federal, state, and local governments, the private sector, academia, and international partners. The department is also responsible for federal outreach to state, local, and nongovernmental organizations, including the private sector, academia, and the public. Additionally, DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance CIKR protection. These efforts include developing and implementing comprehensive, multitiered risk management programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance, guidelines, and protocols; and recommending risk management and performance criteria and metrics within and across sectors. Furthermore, pursuant to HSPD 7, *Critical Infrastructure Identification, Prioritization, and Protection*, DHS is the focal point for coordinating best practices and supporting protective programs to secure cyberspace across and within government agencies.

Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society. Several of the responsibilities for addressing the challenges to secure cyberspace, cyber assets, and our Nation's IT infrastructure, in accordance with the actions and recommendations outlined in the *Strategy*, NIPP, and CNCI, fall within the Office of Cybersecurity and Communications (CS&C), under NPPD.[1] CS&C is composed of three major programs: the National Cyber Security Division (NCSD), National Communications System (NCS), and Office of Emergency Communications (OEC).

Systems used to capture and store critical infrastructure data are operated under the direction of NPPD's Office of Infrastructure Protection (IP). During audit planning, we selected two of the

[1] The IT infrastructure consists of critical functions—sets of processes that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (research and development, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs into IT products and services.

systems that contain the Nation's critical infrastructure information, including the results of cyber and physical infrastructure security site reviews, for review. The systems we evaluated are the Linking Encrypted Network System (LENS), which houses the Infrastructure Information Collection System (IICS) database, and the Automated Critical Asset Management System (ACAMS).

LENS is operated and maintained by Department of Energy (DOE) personnel located at Argonne National Laboratory. LENS provides a number of tools/components that support Office of IP activities. These activities include site assistance visits and the Buffer Zone Protection Program. LENS is a web-based portal with an integrated database engine, which is available to DHS users (upon request) to support programmatic activities. LENS provides a wealth of information (i.e., trip scheduling, reports, background packages, maps) quickly to users.

ACAMS is an Office of IP system. The system, hosted at DHS' Data Center 2 (DC2) location, consists of a web-enabled information services portal that assists state and local governments in CIKR protection. Specifically, ACAMS provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel to collect and use CIKR asset data, assess CIKR asset vulnerabilities, develop all-hazard incident response and recovery plans, and build public/private partnerships. ACAMS users utilize the ACAMS database to gather, analyze, and store data on inventoried CIKR sites. This in turn provides state and local jurisdictions with a structured and practical approach to aid them in developing their statewide Critical Infrastructure Programs. ACAMS further secures CIKR assets by providing a program that assists in the collection and management of asset-specific information. This information is gathered, analyzed, and used to prevent, deter, respond to, and mitigate cyber risks, threats, and incidents.

Several actions have been taken since we last reported on DHS' progress to secure cyberspace and Nation's cyber infrastructure in June 2007.[2] In addition to the issuance of the NIPP, creation of the

[2] *Challenges Remain in Securing the Nation's Cyber Infrastructure* (OIG-07-48), June 2007.

CNCI, and completion of the Cyberspace Policy Review,[3] these actions include DHS' launch of its first ever Quadrennial Homeland Security Review and "Bottom-Up" reviews.

- The Quadrennial Homeland Security Review reflects the most comprehensive assessment and analysis of homeland security to date and offers a vision for a secure homeland. The report, issued in February 2010, specifies key mission priorities, outlines goals for each of those mission areas, and lays the groundwork for subsequent analysis and recommendations. One of the core missions outlined in the report is safeguarding and securing cyberspace by creating a safe, secure, and resilient cyber environment and promoting cybersecurity knowledge and innovation.

- The Bottom-Up Review was an unprecedented department-wide assessment of DHS, begun in November 2009, to align the department's programmatic activities and organizational structure with the mission sets and goals identified in the Quadrennial Homeland Security Review. The results of the review were issued in July 2010.

Both the Quadrennial Homeland Security Review and Bottom-Up Review reiterate DHS' commitment to secure cyberspace and protect critical infrastructures.

Results of Audit

Progress Made in Securing Cyberspace and Critical Infrastructures

CS&C is actively involved in DHS' efforts to better integrate, consolidate, and focus cybersecurity and infrastructure resilience operations as outlined in the *Strategy*, NIPP, and CNCI. To do this, it has focused efforts on outreach and awareness activities by establishing and building relationships with CIKR, public, private, and international partners; promoting cybersecurity awareness programs; and supporting workforce and public education programs. Specific efforts are detailed below.

[3] Shortly after taking office, President Obama directed a 60-day comprehensive review to assess U.S. policies and structures for cybersecurity, known as the Cyberspace Policy Review. Upon completion of the review, a report, *Assuring a Trusted and Resilient Information and Communications Infrastructure,* was issued in May 2009.

To prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm critical infrastructure and assets, CS&C is working and sharing information with the public and private sectors, as well as international partners. For example:

- NCSD, which serves as the national focal point for cybersecurity, is working with many government and industry leaders, including the IT Sector Coordinating Council, Cross-Sector Cyber Security Working Group, and Multi-State Information Sharing and Analysis Centers (ISAC). The United States Computer Emergency Readiness Team (US-CERT), under NCSD, maintains strong operational relationships with many trusted international partners, including Brazil, Canada, Finland, Germany, Japan, Korea, and foreign fusion centers.

- NCS, responsible for coordinating with the telecommunications and IT industries and for the protection, restoration, and sustainment of national cyber and IT resources, leads the Wireless Priority Service and Government Emergency Telecommunications Service programs. All branches within NCS work with the Communications ISAC. NCS facilitates information sharing between government and industry through the Network Security Information Exchanges program, which meets bimonthly. Meetings with international partners, including Australia, Canada, and the United Kingdom, occur annually.

- OEC is the lead on the Public Safety Broadband program and is involved with the Communications Planning Advisory Committee for industry information planning; the National Security Telecommunications Advisory Committee, a public safety forum that coordinates with internet service providers; and the Communications ISAC.

CS&C also promotes public awareness through outreach programs. For example, CS&C is working with the National Association of Counties to raise awareness of cybersecurity issues and has developed programs with the Multi-State ISAC and the National Association of State Chief Information Officers. In addition, CS&C is developing several other programs with the National Lieutenant Governors Association, the U.S. Conference of Mayors, and the National League of Cities. NCSD has developed a partnership with the U.S. Chamber of Commerce to offer six specific education and awareness summits to be held around the country. The State, Local, and Tribal Engagement branch within NCSD is focused on outreach to state, local, and tribal governments. October is designated as National Cybersecurity Awareness Month, and NCSD conducts briefings around the country to raise the public's awareness of cybersecurity risks and how to protect their computer systems from potential exploits.[4]

In alignment with actions and recommendations outlined in the *Strategy* and CNCI, CS&C supports DHS' efforts to take cybersecurity to the next level by supporting workforce and public education programs. CS&C coleads, through NCSD's Global Cyber Security Management branch, the department's efforts to address CNCI Initiative #8 – Expand cyber education. The Global Cyber Security Management branch is focused on establishing cybersecurity education and training partnerships to share investment, analyze requirements to synchronize cyber roles and skill standards, and develop a competency assessment methodology. The Cyber Education and Workforce Development group within NCSD cosponsors the National Security Agency's Centers of Excellence. NCSD's National Cybersecurity Education Strategy group coleads the National Initiative for Cybersecurity Education, which focuses on working closely with students at all levels. NCSD also supports the Centers for Academic Excellence and Scholarship for Service programs. In addition, NCSD provides control systems training for federal, state, and local agencies, international partners, and private industry participants, and community-based cyber training through the University of Texas at San Antonio.[5]

Further, CS&C supports a series of continuous efforts designed to secure federal government information systems by reducing security vulnerabilities, protecting sensitive data from intrusions, and anticipating future threats. For example, during fiscal year (FY) 2010, NCSD completed 58 cybersecurity assessments and 50 control system reviews as part of its CIKR mission. US-CERT operates the National Cybersecurity Protection System, known as Einstein, which provides for the automated collection, correlation, analysis, and sharing of potential treats and security information across the federal government to improve our Nation's situational awareness of cybersecurity. US-CERT is also actively involved in the National Security Alliance and participates in the StaySafeOnline campaign.[6] Additionally, US-CERT regularly posts tips, best practices, and cybersecurity links online, conducts briefings for organizations, and supports National Cybersecurity Awareness Month.

[4] One of the main objectives of National Cybersecurity Awareness Month is to educate people about how to secure personal information online.
[5] A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems.
[6] The StaySafeOnline campaign (www.staysafeonline.org) provides the public with guidance to help stay safe online at work, home, and school, and strengthen our collective cybersecurity efforts.

CS&C Has Not Developed a Strategic Implementation Plan or Performance Measures To Address Cybersecurity Risks

Although progress has been made in building relationships with the public and private sectors, raising cybersecurity awareness, and implementing education and outreach programs, much work remains to protect cyberspace and the Nation's critical infrastructures from vulnerabilities and exploits. CS&C has yet to develop a strategic implementation plan, including performance measures and milestones, to document how it will address the open actions and recommendations in the *Strategy*, NIPP, or CNCI, or meet its mission to safeguard and secure cyberspace.

CS&C Has Not Developed a Strategic Implementation Plan To Achieve Its Cybersecurity Mission

CS&C has not developed a strategic implementation plan that outlines its responsibilities or establishes specific objectives and milestones for enhancing cybersecurity or protecting critical infrastructures. An approved strategic implementation plan would help ensure that CS&C's programs and processes align with its mission and national priorities to secure the Nation's critical cyber infrastructure, as outlined in the Quadrennial Homeland Security Review. Furthermore, CS&C has not developed a strategy to address open actions and recommendations in the *Strategy* or to achieve the goals outlined in the NIPP and CNCI.

According to the *Government Performance Results Act of 199*3, as amended, a strategic plan should identify the major functions and operations of an agency and include general goals and objectives and a description of how those goals and objectives should be achieved. A strategic plan should cover at least 5 years.

As NCSD, NCS, and OEC have not yet developed or finalized their strategic plans, CS&C cannot integrate those plans to develop one comprehensive strategic implementation plan. NCSD currently has a draft strategic plan, but as of December 14, 2010, the plan had not been approved by management. NCSD's strategic plan is based on Mission 4: Safeguarding and Securing Cyberspace, as outlined in the Quadrennial Homeland Security Review report. According to NCSD, an implementation plan will also be developed to specifically address NIPP or CNCI activities. NCS management officials told us that they look to NCSD to address the actions and recommendations in the *Strategy*; a strategic plan for addressing the goals outlined in the NIPP or

CNCI is not being developed. An OEC official said that he is in the process of defining his program area's roles and responsibilities according to the *Strategy*.

Under both the *Strategy* and NIPP, DHS is responsible for developing a comprehensive national plan for securing key resources and the critical infrastructure of the United States and coordinating overall CIKR protection efforts. DHS is responsible for several of the initiatives documented in the CNCI: Initiative #2 – Deploy an intrusion detection system of sensors across the federal enterprise; Initiative #3 – Pursue deployment of intrusion prevention systems across the federal enterprise; Initiative #5 – Connect current cyber operations centers to enhance situational awareness; and Initiative #12 – Define the federal role for extending cybersecurity into critical infrastructure. As the focal point for cybersecurity within DHS and the Sector-Specific Agency for the IT and Communications Sectors, CS&C is responsible for enhancing the security, resiliency, and reliability of the Nation's cyber and communications infrastructure.

We reported in July 2004 that DHS had yet to develop a strategic plan to address the actions and recommendations in the *Strategy*.[7] Though some of the information in the *Strategy* is out-of-date, the open actions and recommendations align with the actions called for under the NIPP and CNCI. In May 2009, as part of the 60-day comprehensive Cyberspace Policy Review to assess United States policies and structures for cybersecurity, the President determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national cybersecurity strategy.

To develop a comprehensive strategic implementation plan to enhance the security, resiliency, and reliability of the Nation's cyber and communications infrastructure, each program area's responsibilities need to be defined. In addition, CS&C must ensure that each program area develops and implements plans that are focused on the critical priorities that will enable CS&C to accomplish its mission and address long-term cyber threats and vulnerabilities.

[7] *Progress and Challenges in Securing the Nation's Cyberspace* (OIG-04-29), July 2004.

Performance Criteria and Metrics Have Not Been Developed

Performance metrics allow an organization to track progress against priorities, establish accountability, document actual performance, promote effective management, and provide a feedback mechanism for decision makers. CS&C has not developed objective, quantifiable performance measures to determine whether it is meeting its mission to secure cyberspace and protect critical infrastructures. Additionally, CS&C is not able to track its progress efficiently and effectively in addressing the actions outlined in the *Strategy* or achieving the goals outlined in the NIPP. Performance metrics allow an organization to track progress against priorities, establish accountability, document actual performance, promote effective management, and provide a feedback mechanism for decision makers.

Only one of CS&C's program areas, NCSD, has drafted performance measures that are aligned with its mission, as outlined in the Quadrennial Homeland Security and Bottom-Up reviews. Performance measures are needed to assess CS&C's progress in addressing national priorities and attaining strategic goals and milestones. Establishing performance metrics is one of the near-term actions outlined the Cyberspace Policy Review. Under the *Strategy*, each agency is to be held accountable for its cybersecurity efforts and be responsible for employing performance measures to evaluate progress in addressing the recommendations in the *Strategy*. As outlined in the NIPP, performance criteria and metrics are needed to assess efforts to lead, integrate, and coordinate the overall national effort to enhance CIKR protection.

Performance measures indicate what a program is accomplishing and whether results are being achieved. In addition, measures help management determine how to allocate resources and evaluate the effectiveness of current efforts. The Office of Management and Budget (OMB) requires each agency to prepare an annual performance plan covering each program activity included in an agency's budget. A performance plan should include the following:

- Goals that define the level of performance to be achieved by a program activity.
- Goals that are objective, quantifiable, and measurable.
- Performance indicators to measure or assess the relevant output, service levels, and outcomes of each program activity.

- A basis for comparing actual program results with established performance goals.

Conclusion

Without a strategic implementation plan, CS&C cannot prioritize its key activities or evaluate its progress in accomplishing its mission and goals, nor can it determine whether it is meeting its responsibilities outlined in the *Strategy*, NIPP, and CNCI. The use of performance metrics is a critical step in the risk management process to enable DHS and Sector-Specific Agencies to assess improvements in CIKR protection and resiliency at the national and sector levels objectively and qualitatively. Once CS&C has defined its responsibilities, priorities, and goals, it will be able to develop objective, quantifiable performance criteria and metrics to evaluate its progress and better support DHS' efforts to secure cyberspace and protect CIKR.

Recommendations

We recommend that the Assistant Secretary, Office of CS&C:

Recommendation #1: Define its program areas' responsibilities, priorities, and goals based on cybersecurity policy and the results of the Cyberspace Policy Review, Quadrennial Homeland Security Review, and Bottom-Up Review.

Recommendation #2: Ensure that each program area develops and implements strategic plans that are focused on the critical tasks necessary to support DHS' efforts to safeguard and secure cyberspace and protect critical infrastructures, with an emphasis on the IT and communications sectors.

Recommendation #3: Develop a comprehensive strategic implementation plan that defines its mission and priorities, identifies milestones, and is aligned with its program areas' responsibilities and plans to support DHS' overall mission to secure cyberspace and protect CIKR.

Recommendation #4: Develop and implement objective performance criteria and measures that can be used to track and evaluate the effectiveness of actions defined in its strategic implementation plan and used by management to assess CS&C's overall progress in attaining its strategic goals and milestones.

Management Comments and OIG Analysis

NPPD concurred with recommendation 1. NPPD management agreed that the responsibilities, priorities, and goals of the Office of CS&C's program areas require clear definition to ensure the most efficient application of resources based on administration and departmental policies. These responsibilities, priorities, and goals will inform a CS&C strategic plan, on target for completion by the end of FY 2011.

<u>OIG Analysis</u>

We agree with management's response to satisfy this recommendation. This recommendation will remain open until the Office of CS&C provides documentation to support that the planned corrective action is completed.

NPPD concurred with recommendation 2. According to NPPD's response, NCSD is completing its strategic plan and, to the extent not already in process, CS&C will ensure that NCS and OEC develop and implement their own strategic plans.

<u>OIG Analysis</u>

We agree with the actions being taken to satisfy the intent of this recommendation. This recommendation will remain open until the Office of CS&C provides documentation to support that the planned corrective actions are completed.

NPPD concurred with recommendation 3. CS&C's development of an overarching strategic implementation plan is a FY 2011 objective, and will be linked to the most recent version of the NPPD strategic plan. The FY 2011 and FY 2012 NPPD strategic plans are in draft form. In the interim, CS&C will execute its strategic plan, while also remaining cognizant of strategic initiatives at the NPPD level. The CS&C strategic plan will be aligned with the NPPD FY 2011 and FY 2012 strategic plans, since it will be informed partly by those draft versions. Additionally, the *Quadrennial Homeland Security Review* Mission 4 strategy will inform CS&C's planning process with respect to its cybersecurity mission. NPPD, the DHS Office of Policy, and other public and private sector stakeholders are currently developing the Mission 4 strategy.

OIG Analysis

We agree with the actions being taken to satisfy the intent of this recommendation. This recommendation will remain open until the Office of CS&C provides documentation to support that the planned corrective actions are completed.

NPPD concurred with recommendation 4. CS&C's objective performance criteria and measures will be developed once the strategic implementation plan is completed.

OIG Analysis

We agree with management's response to satisfy this recommendation. This recommendation will remain open until the Office of CS&C provides documentation to support that the planned corrective action is completed.

Training and System Vulnerabilities May Put Protected Critical Infrastructure Data at Risk

Critical infrastructure data may be at risk due to insufficient training and to system vulnerabilities. Specifically, LENS administrators with access to Protected Critical Infrastructure Information (PCII) completed initial PCII training, but have not taken PCII refresher training.[8] DC2 system administrators for ACAMS have never taken required PCII training. In addition, although we did not identify any high-risk system security vulnerabilities for LENS, we identified access control deficiencies that must be addressed. We also identified significant system configuration and account access deficiencies for ACAMS. Further, although both LENS and ACAMS are authorized to operate, there are discrepancies between the documentation and the system security authorization information maintained for ACAMS.

LENS and ACAMS Administrators and Contractors Are Not PCII Certified

Personnel who manage and operate LENS are not completing annual PCII training. Training records show that all Argonne National Laboratory personnel with access to PCII completed

[8] PCII is CIKR information that critical infrastructure owners and operators in the private sector and at the state and local levels have voluntarily shared with the federal government. The federal government is responsible for properly safeguarding this information, which is exempt from public disclosure.

initial PCII training but had not taken PCII refresher training. Additionally, even though ACAMS personnel within NPPD's Office of IP are PCII certified, the system administration personnel at DC2 had not obtained PCII certification at the time of our audit.

Our review of PCII training certificates for 23 people who have or had access to LENS PCII showed that 20 of the 23 certificates were not current. Three of the 23 users' training certificates were dated in 2006, 15 were dated in 2008, and 2 were dated in 2009. Only 3 of the 23 training certificates were current. According to the LENS System Security Plan, LENS administrators (all Argonne National Laboratory employees) who are required to access or process PCII must complete an access form and initial PCII training. However, the LENS System Security Plan does not require users to complete annual refresher training to maintain PCII certification. Furthermore, DOE does not require LENS personnel to take PCII refresher training annually. LENS system administrators, who potentially have access to PCII in the DHS–owned IICS database, are not in compliance with DHS' PCII requirements.

DHS data center personnel, including contractors, were unable to provide documentation showing that the 33 local system administrators at DC2 with access to the PCII database had ever obtained PCII certification. According to the ACAMS System Security Plan, non-DHS personnel and contractors who work closely on ACAMS are required to take PCII training to ensure they are aware of their role in system and information security.

The *Critical Infrastructure Information Act of 2002* (*CII Act*) established PCII as a category of Sensitive but Unclassified information. DHS is the agency responsible for administering the PCII Program. The PCII Program is unique in that it provides an outlet for critical infrastructure owners to voluntarily submit information to the federal government to which the government would not otherwise have access. Once information has been submitted and validated by the PCII Program Office, federal, state, and local government entities can use it in their efforts to protect the Nation's critical infrastructure.[9] Both LENS and ACAMS capture and store PCII data.

[9] The PCII Program Office operates under the authority of the *CII Act*, Title II, Subtitle B of the *Homeland Security Act of 2002*, as amended. The Secretary of Homeland Security designated the Under Secretary of NPPD as the senior DHS official responsible for directing and administering the PCII Program.

To gain access to PCII, individuals must meet the following requirements: (1) have homeland security responsibilities, (2) have a need-to-know, (3) complete PCII authorized user training, and (4) if non-federal employees, sign a non-disclosure agreement. Before being granted PCII access, a user must be trained in safeguarding and handling requirements, as documented in the PCII Program Procedures Manual, dated April 2009.[10] According to the manual, users are also required to complete annual refresher training to maintain PCII access and privileges. Furthermore, the manual requires any system storing PCII to be configured to restrict access to authorized users with the proper need-to-know.

Most LENS administrators at Argonne National Laboratory completed initial PCII training prior to the implementation of DHS' PCII Management System (PCIIMS), which tracks authorized PCII user status and enforces an annual refresher training requirement. Therefore, the PCII Program Office considered LENS personnel's PCII certificates valid until LENS personnel were able to access PCIIMS. Authorized user certificates did not have an expiration date and refresher training was not enforced prior to DHS' implementation of PCIIMS. In September 2010, LENS personnel began registering in PCIIMS to complete applicable PCII training. However, LENS administrators had yet to meet DHS requirements for PCII refresher training at the time of our audit.

According to DC2 personnel, local administrators with access to the ACAMS database have never taken PCII training because they were not aware of the requirement. The ACAMS Program Office said that, based on guidance provided by the DHS Office of the Chief Information Officer, DC2 personnel were not initially required to complete PCII training because they are responsible for providing hosting services. They do not have access to the ACAMS PCII database or the ACAMS web application. The PCII Program Office has since worked with the Office of the Chief Information Officer to implement PCII training for DC2 personnel as an additional measure of precaution.

Training ensures that users maintain an awareness of PCII program developments and reinforces protective procedures. Individuals

[10] The manual implements the requirements and criteria of the *CII Act* and its implementing regulations at 6 C.F.R. Part 29, as amended.

with access to PCII who obtain and maintain appropriate certification should be able to appropriately handle and protect it and the systems containing PCII from unauthorized access or misuse.

Account Access Controls Can Be Improved To Further Secure IICS

Overall, the system security controls implemented on the IICS component of LENS are effective in protecting the PCII and other sensitive information captured and stored on the system. However, we identified issues regarding account access controls. Although these issues do not pose a significant security risk to the system, LENS personnel should enhance access controls to reduce the risks associated with unauthorized access to the system and data. Restricting user and administrator access limits potential misuse of PCII data contained in LENS. Specifically, we identified the following concerns:

- Eighty-eight of 436 (20%) of the active IICS website users have never logged into the system. DHS requires that user accounts that have never been logged into be deactivated.
- Unused IICS database administrator accounts were not being disabled within the required timeframe. These accounts were configured to be disabled after 90 days of inactivity. Under DHS policy, unused accounts should be deactivated within 45 days.
- A LENS administrator had established a temporary testing account. Per DHS requirements, temporary account access must be rigorously controlled and approved by the respective Chief Information Security Officer. The National Institute of Science and Technology (NIST) recommends that temporary and unnecessary accounts be disabled and/or removed when no longer needed to secure access to sensitive systems and information.

LENS system personnel indicated that the deficiencies identified were due to administrator error. For example, the system administrator who created an automated script to disable unused IICS accounts did not realize that users who had never logged into LENS were excluded from the disabling action. LENS personnel have begun to address the account access issues we identified.

We also evaluated controls that protect LENS data in terms of system account access and security, data security, and user authentication. We interviewed LENS system administrators and manually reviewed database and server configurations. Automated tools were used to test for vulnerabilities and adherence to DHS policy on the database, servers, and the IICS website. Our fieldwork testing did not identify any significant deficiencies on LENS.

Configuration and Access Control Vulnerabilities Put ACAMS Data at Risk

System configuration and account access control deficiencies may put ACAMS and its PCII data at significant risk of inappropriate access, disclosure, and misuse. Because ACAMS contains sensitive CIKR prevention and protection information, the system configuration and access control vulnerabilities need to be addressed to reduce these risks and ensure the confidentiality, integrity, and availability of the system, as well as the critical asset information stored.

Configuration Control Vulnerabilities

We identified the following configuration control vulnerabilities:

- [redacted] is used for network management on the DC2 network. DHS prohibits the use of this protocol, as it may introduce vulnerabilities into the system.
- Two high-risk [redacted], [redacted], are missing on five ACAMS servers. The [redacted] address multiple vulnerabilities, [redacted]. DHS requires that [redacted] in a timely manner to protect against known security vulnerabilities.
- [redacted]. An attacker can use that information to exploit the active website. [redacted], should be restricted to those needed to perform job functions.

[11] [redacted].

- Certain [redacted], prohibited by DHS because they may introduce vulnerabilities into the system, have been identified on the DC2 network.
- The “acams” [redacted] policy does not meet DHS’ minimum [redacted] requirements.
- [redacted] is in use [redacted]. DHS requires that the more secure [redacted] be used for all [redacted] access.
- The [redacted] server is running on [redacted]. DHS requires that [redacted] to run on a [redacted] to avoid attacks [redacted].

Account Access Control Issues

We also identified account access control issues:

- Eighty-three percent (4,005 of 4,807) of the active ACAMS users had not logged into their accounts for more than 45 days prior to the date the list of users was pulled for testing. Four of these accounts had “super user” access, which grants unrestricted administrative access to ACAMS. DHS requires that accounts be deactivated after 45 days of inactivity to restrict access to sensitive information and minimize the potential for system misuse.
- Seventy-two of the 4,807 active ACAMS users have never logged onto the system. Other users had not logged onto the system for almost 5 years—the oldest login dates back to February 1, 2006. DHS requires that accounts be deactivated after 45 days of inactivity, including accounts of users who have never logged into a system.
- Twenty testing, training, demo, or otherwise temporary accounts were identified on the ACAMS website. According to DHS policy, temporary or testing access should be used only when necessary to meet mission needs. Further, temporary access must be rigorously controlled and approved by the respective component’s Chief Information Security Officer.
- Four ACAMS website administrators have duplicate unrestricted access to the system; each administrator has two “super user” accounts. DHS requires that elevated privileges be restricted for systems containing sensitive information.
- Thirty-seven local administrators have privileges on the ACAMS servers. These administrators are not members of

separate groups, such as operating system administrators or database administrators. Per DC2 policy, 35 of the 37 administrators were granted access to the built-in local Windows administrators group. DHS requires that the principles of separation of duties and least privilege be enforced for local server administrators and that system access should be restricted to those who need it to perform their job functions.

- Thirty-three local Windows administrators have been granted access to ACAMS' PCII database. The SQL database settings allow all local Windows administrators access to the PCII database. Under DHS policy, the principle of least privilege should be used when granting system access and privileges.

The need for clearly defined roles and responsibilities, contractor oversight, and communication has culminated in multiple security vulnerabilities that may put ACAMS and its PCII data at risk of potential exploitation. Contractor staff at DC2 is tasked with the network and server-level administrative duties, while NPPD's program office is responsible for implementing controls on the data captured and stored by the system, as well as running the ACAMS website.

During our fieldwork, we observed multiple instances of poor oversight and miscommunication between the two parties who should be partners in securing the system. For example, the program office was not aware that DC2 local administrators with access to the ACAMS PCII database were not PCII certified. ACAMS program office personnel had never visited DC2 until we conducted our testing. Further, the division of responsibilities between DC2 and program management staff is not clearly defined. For example, while ACAMS program office personnel indicated that server and database-level configurations were the responsibility of local DC2 administrators, the local DC2 administrators told us that the configuration issues we identified could not be addressed until the program office provided direction.

Until identified access control and configuration issues are addressed, the ACAMS system and data remain at risk. Restricting user and administrator access limits potential misuse of PCII. The implementation of DHS policy for configuring operating systems, applications, and networks, and [redacted], will help protect the system from common avenues of internal and external attack.

ACAMS personnel have actively begun to address the deficiencies we identified. For example, contractor personnel at DC2 indicated that they had begun [redacted] and mitigate website vulnerabilities. Other security weaknesses will be addressed upon completion of planned system upgrades.

ACAMS' Security Authorization Package Is Not Being Updated

We reviewed ACAMS and LENS security authorization packages to determine whether the systems are in compliance with applicable OMB, NIST, and DHS requirements under the Federal Information Security Management Act of 2002. Although both systems have been authorized to operate, ACAMS' security documentation is not current or aligned with the information documented in DHS' enterprise management tool. We did not identify any significant deficiencies in the LENS system documentation.

The security documentation in DHS' enterprise management tool is based on ACAMS being located at a hosting facility in California. ACAMS was moved from that facility to DC2 in June 2010; however, the System Security Plan was not updated to reflect the current location and physical security controls. Additionally, other documentation, such as the contingency plan and test plan, is based on the prior hosting facility's location and has not been updated.

ACAMS is currently in the process of renewing its security authorization, but updated documentation has not yet been uploaded to DHS' enterprise management tool. The original Authority to Operate for ACAMS expired in September 2010. ACAMS has received two 90-day extension letters. The first letter, dated September 10, 2010, expired on December 13, 2010. The second extension letter was not signed until January 6, 2011. Between December 13, 2010, and January 6, 2011, ACAMS was not operating under a valid Authority to Operate or an extension.

According to the ACAMS Project Officer, the first 90-day extension was granted because there were issues with migrating the system to the DC2 location and the security documentation could not be updated timely. The delay in issuing the second extension letter was attributed to delays in management review. The second extension was granted because additional time was needed to update documentation based on new guidance issued by DHS' Office of the Chief Information Security Officer. According to the ACAMS technical lead, there would not have been enough time to revise the security documentation to meet the December 13, 2010, deadline due to the substantive changes needed based on new documentation and associated completion guidance.

DHS requires components to authorize systems at initial operating capability and every 3 years thereafter, or whenever a major change occurs, whichever occurs first. Respective component Chief Information Security Officers are to ensure that systems are properly authorized to ensure that the appropriate security controls have been evaluated and that the data stored on the system is protected.

Conclusion

Proper management of DHS IT systems is essential to ensure the confidentiality, integrity, and availability of critical infrastructure information. Configuration and account access vulnerabilities identified on the LENS and ACAMS systems must be mitigated to manage and secure the systems and PCII data from the risks associated with internal and external threats, unauthorized access, and misuse. Authorized system administrators, users, and contractor personnel need to be appropriately trained to ensure that PCII data and systems containing the data are adequately safeguarded. ACAMS security documentation needs to be updated to ensure that system information is accurate, the appropriate security controls have been evaluated, and the data stored on the system is protected.

Recommendations

We recommend that the Assistant Secretary, Office of IP:

Recommendation #5: Identify systems personnel, users, and contractors who have access to LENS or ACAMS PCII data to ensure that those personnel have obtained initial PCII certification and/or required refresher training to ensure appropriate handling and safeguarding of PCII.

Recommendation #6: Develop a process to track system personnel and contractors who have access to LENS and ACAMS PCII data, and periodically review whether they still need access and have completed required PCII refresher training.

Recommendation #7: Address LENS IICS account access issues identified to further reduce the risks associated with unauthorized system and data access and comply with DHS policy.

Recommendation #8: Implement steps to further define the roles and responsibilities of the ACAMS program office personnel and the system administrators at DC2 and improve oversight of contractor operations.

Recommendation #9: Address identified ACAMS configuration and account access issues to reduce system risks and comply with DHS system requirements, and implement steps to prevent future problems in these areas to ensure the confidentiality, integrity, and availability of critical infrastructure information.

Recommendation #10: Ensure that ACAMS security documentation is appropriately updated and uploaded to DHS' enterprise management tool.

Management Comments and OIG Analysis

NPPD concurred with recommendation 5. According to NPPD's response, paramount to the continued success of the PCII Program is the proper safeguarding and handling of the CII voluntarily shared with the federal government. Accordingly, the PCII Program has developed comprehensive processes and procedures for the access, safeguarding, and handling of PCII to include robust authorized user training. These processes and procedures implement the requirements in the *CII Act of 2002*; Procedures for Handling Critical Infrastructure Information, Final Rule, dated September 1, 2006; and the PCII Program Procedures Manual dated April 2009.

NPPD has verified PCII certification of LENS and ACAMS system administrators, security personnel requiring access to PCII data at DC2, and Argonne National Lab personnel who view, manage, and respond to incident response activities.

DC2 personnel do not use or require operational access to the ACAMS data and therefore were not PCII certified. During the OIG audit, it was determined that DC2 personnel responding to data spills might, in fact, require access to the PCII data, and as a preemptive measure, DC2 and the PCII Program Office have identified and required personnel to become PCII certified. The

PCII Program has verified that all identified DC2 personnel have completed the required training through PCIIMS. The PCII Program verified there was no data compromise and that DC2 personnel never accessed PCII data.

PCIIMS, implemented in December 2009, serves as the system of record for access to PCII data and delivers PCII training and tracks the status of PCII authorized users. PCIIMS provides the PCII Program with a streamlined, web-based user registration and training delivery system, which enables robust training and management of authorized users. PCIIMS enables the Program to implement and track annual refresher training and reaffirm authorized users' continued need for access to PCII.

<u>OIG Analysis</u>

We agree with the actions being taken to satisfy the intent of this recommendation. This recommendation will remain open until the Office of IP provides documentation to support that the corrective actions are completed.

NPPD concurred with recommendation 6. According to NPPD's response, PCIIMS provides the PCII Program with a streamlined, web-based authorized user registration and training delivery system, which enables robust training and management of authorized users. PCIIMS enables the Program to implement and track annual refresher training and reaffirm authorized users' continued need for access to PCII.

PCIIMS also provides mechanisms to verify individual PCII authorized user status and to implement an annual refresher training requirement. Annual refresher training provides verification of the continued need for access to PCII and a reminder to authorized users of the requirements for safeguarding PCII. The system provides automatic notification to authorized users when annual refresher training is required and enables removal of any individual who does not comply with the annual requirement or no longer requires access to PCII.

<u>OIG Analysis</u>

The use of PCIIMS to track whether individuals who need access to LENS and ACAMS PCII data have completed required PCII refresher training partially addresses the intent of this recommendation. However, management did not address whether they will implement a process to periodically review whether individuals still need access to PCII. This recommendation will remain open until the Office of IP provides documentation to support that corrective actions are being taken to address this recommendation and that a review process will be implemented.

NPPD concurred with recommendation 7. NPPD will continue to collaborate with Argonne National Laboratory on this issue.

OIG Analysis

Argonne National Laboratory provided us with documentation showing that the account access issues we identified had been addressed. The documentation provided satisfies the intent of this recommendation. We consider this recommendation resolved and closed.

NPPD concurred with recommendation 8. NPPD will with work DC2 to supplement the service agreement with a roles-and-responsibilities document to define clearly the respective roles and responsibilities of each party by the end of July 2011.

OIG Analysis

We agree with the actions being taken to satisfy the intent of this recommendation. This recommendation will remain open until the Office of IP provides documentation to support that the corrective actions are completed.

NPPD concurred with recommendation 9. NPPD has addressed these issues through the release of ACAMS 3.0.1 in November 2010 and ACAMS 3.1 in April 2011. NPPD stated that it has provided documentation to the OIG advising how these releases address the recommendations.

OIG Analysis

NPPD's response does not meet the intent of our recommendation. We have not received the documentation or management's corrective actions to address this recommendation. This recommendation will remain open until the Office of IP provides documentation to support that corrective actions have been completed.

NPPD concurred with recommendation 10. The system accreditation documentation for ACAMS was undergoing revision at the time of the OIG's review, and as such, the updated documentation was not approved for upload into the enterprise management tool. As of April 2011, ACAMS documentation associated with the accreditation package was finalized and uploaded.

OIG Analysis

We agree with the actions taken to satisfy the intent of this recommendation. This recommendation will remain open until the Office of IP provides documentation to support that corrective action is completed.

Appendix A
Purpose, Scope, and Methodology

The objective of our audit was to evaluate DHS' progress in addressing the actions and recommendations outlined in *The National Strategy to Secure Cyberspace*, NIPP, and CNCI. We also determined whether effective physical and system security controls have been implemented on LENS and ACAMS, two of the systems containing the Nation's critical infrastructure and asset information.

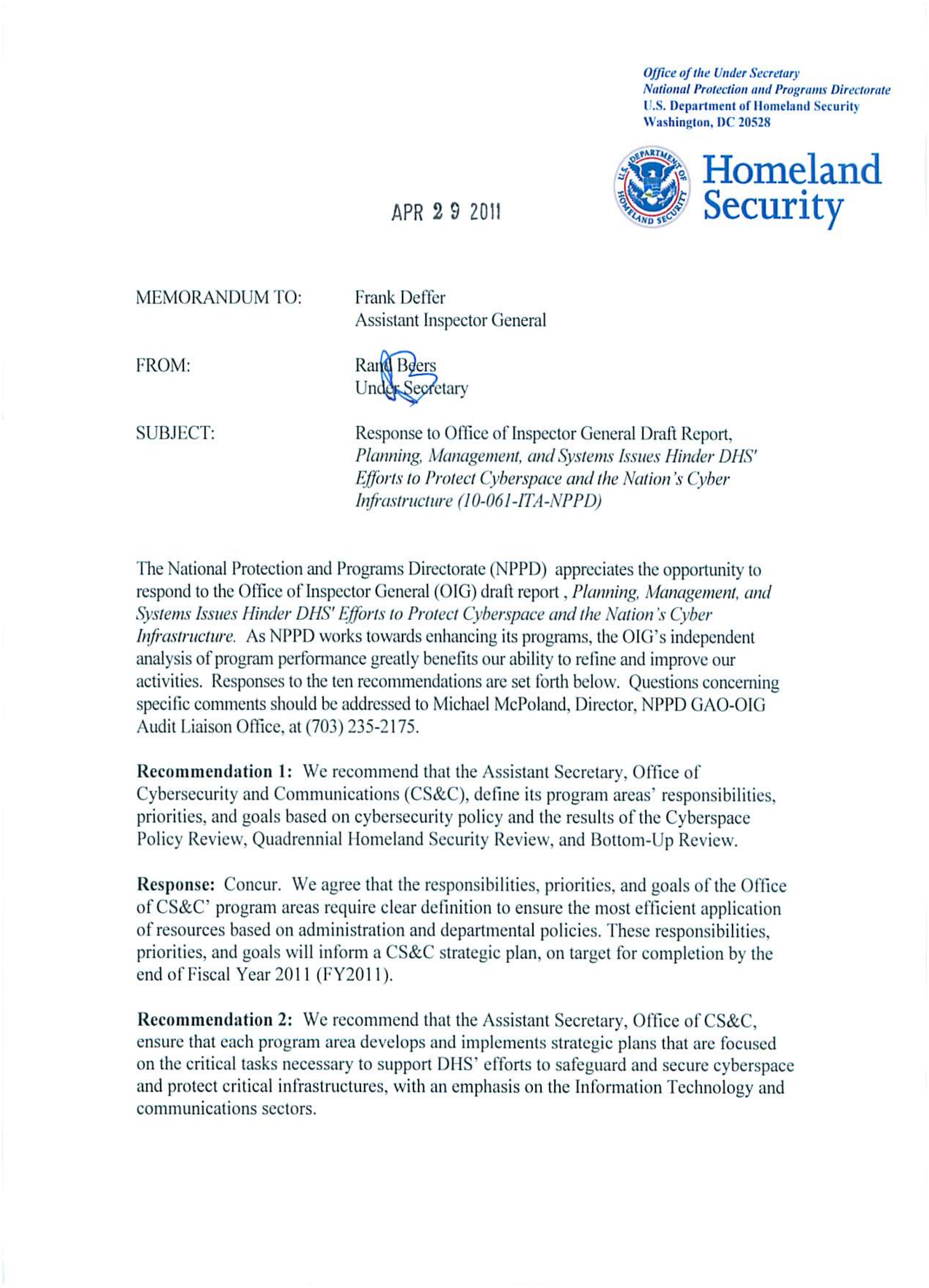
Our audit focused on the actions and recommendations, requirements, and goals outlined in the *Strategy*, NIPP, and CNCI. We also focused on the requirements in HSPD 7 - *Critical Infrastructure Identification, Prioritization, and Protection*; the *Government Performance Results Act of 1993*, as amended; the PCII Program Procedures Manual; Federal Information Security Management Act of 2002; DHS' *Sensitive System Policy Handbook 4300A*; DHS' Windows Server 2003 Configuration Guidance; DHS' Windows SQL Server Secure Baseline Configuration Guide; DHS' Oracle Secure Baseline Configuration Guide; and NIST Special Publication 800-53 - *Recommended Security Controls for Federal Information Systems*. Additionally, we evaluated the results of the Cyberspace Policy Review, Quadrennial Homeland Security Review, and Bottom-Up Review.

We interviewed selected management officials and branch and program management personnel in NCSD, NCS, and OEC. We also interviewed the Development Team Lead/Infrastructure Information Collection Division; Chief, Strategy, Plans and Outreach; Deputy Director, Protective Security Coordination Division; private sector security clearance officials; and personnel in the PCII Program Office. For LENS, we interviewed the Infrastructure Assurance Center IT manager, Oracle database administrator, system administrators, and network specialists. For ACAMS, we interviewed the ACAMS and DC2 Information Systems Security Officers, Facility Security Officer, project lead, project officer, data center services manager, business services representative, system administrators, and network security specialists.

We performed a crosswalk of the NIPP and CNCI to the actions and recommendations in the *Strategy*, analyzed performance measures and standard operating procedures, assessed CS&C's research and development activities, reviewed detailed training documentation, and evaluated LENS and ACAMS security documentation. We conducted physical security assessments at the LENS and ACAMS contractor facilities. In addition, we performed security control vulnerability assessments of LENS and ACAMS to determine the effectiveness of the system security controls implemented. Furthermore, we obtained and analyzed user lists to identify issues that might put the system at risk and manually reviewed database and server configurations. We also evaluated separation of duties, system logs, account access controls, and user authentication.

Fieldwork was performed at NPPD headquarters in Arlington, Virginia, and at contractor facilities in Chicago, Illinois, and Clarksville, Virginia. We conducted this performance audit between September 2010 and January 2011 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. Major OIG contributors to the audit are identified in Appendix C.

The principal OIG point of contact for the audit is Frank W. Deffer, Assistant Inspector General, IT Audits, at (202) 254-4100.



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

Homeland
Security

APR 29 2011

MEMORANDUM TO: Frank Deffer
Assistant Inspector General

FROM: Rand Beers
Under Secretary

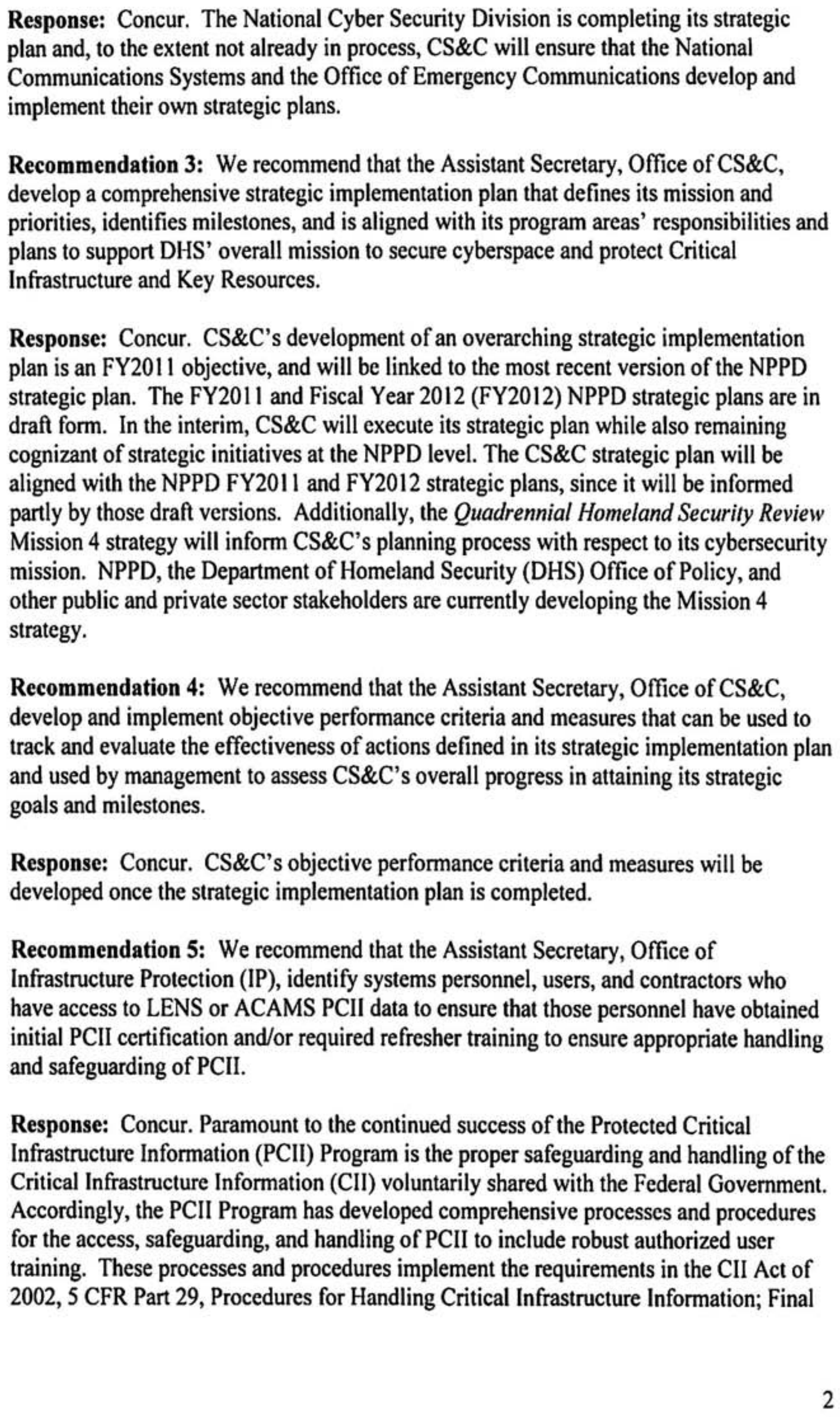
SUBJECT: Response to Office of Inspector General Draft Report, *Planning, Management, and Systems Issues Hinder DHS' Efforts to Protect Cyberspace and the Nation's Cyber Infrastructure (10-061-ITA-NPPD)*

The National Protection and Programs Directorate (NPPD) appreciates the opportunity to respond to the Office of Inspector General (OIG) draft report , *Planning, Management, and Systems Issues Hinder DHS' Efforts to Protect Cyberspace and the Nation's Cyber Infrastructure.* As NPPD works towards enhancing its programs, the OIG's independent analysis of program performance greatly benefits our ability to refine and improve our activities. Responses to the ten recommendations are set forth below. Questions concerning specific comments should be addressed to Michael McPoland, Director, NPPD GAO-OIG Audit Liaison Office, at (703) 235-2175.

Recommendation 1: We recommend that the Assistant Secretary, Office of Cybersecurity and Communications (CS&C), define its program areas' responsibilities, priorities, and goals based on cybersecurity policy and the results of the Cyberspace Policy Review, Quadrennial Homeland Security Review, and Bottom-Up Review.

Response: Concur. We agree that the responsibilities, priorities, and goals of the Office of CS&C' program areas require clear definition to ensure the most efficient application of resources based on administration and departmental policies. These responsibilities, priorities, and goals will inform a CS&C strategic plan, on target for completion by the end of Fiscal Year 2011 (FY2011).

Recommendation 2: We recommend that the Assistant Secretary, Office of CS&C, ensure that each program area develops and implements strategic plans that are focused on the critical tasks necessary to support DHS' efforts to safeguard and secure cyberspace and protect critical infrastructures, with an emphasis on the Information Technology and communications sectors.



Response: Concur. The National Cyber Security Division is completing its strategic plan and, to the extent not already in process, CS&C will ensure that the National Communications Systems and the Office of Emergency Communications develop and implement their own strategic plans.

Recommendation 3: We recommend that the Assistant Secretary, Office of CS&C, develop a comprehensive strategic implementation plan that defines its mission and priorities, identifies milestones, and is aligned with its program areas' responsibilities and plans to support DHS' overall mission to secure cyberspace and protect Critical Infrastructure and Key Resources.

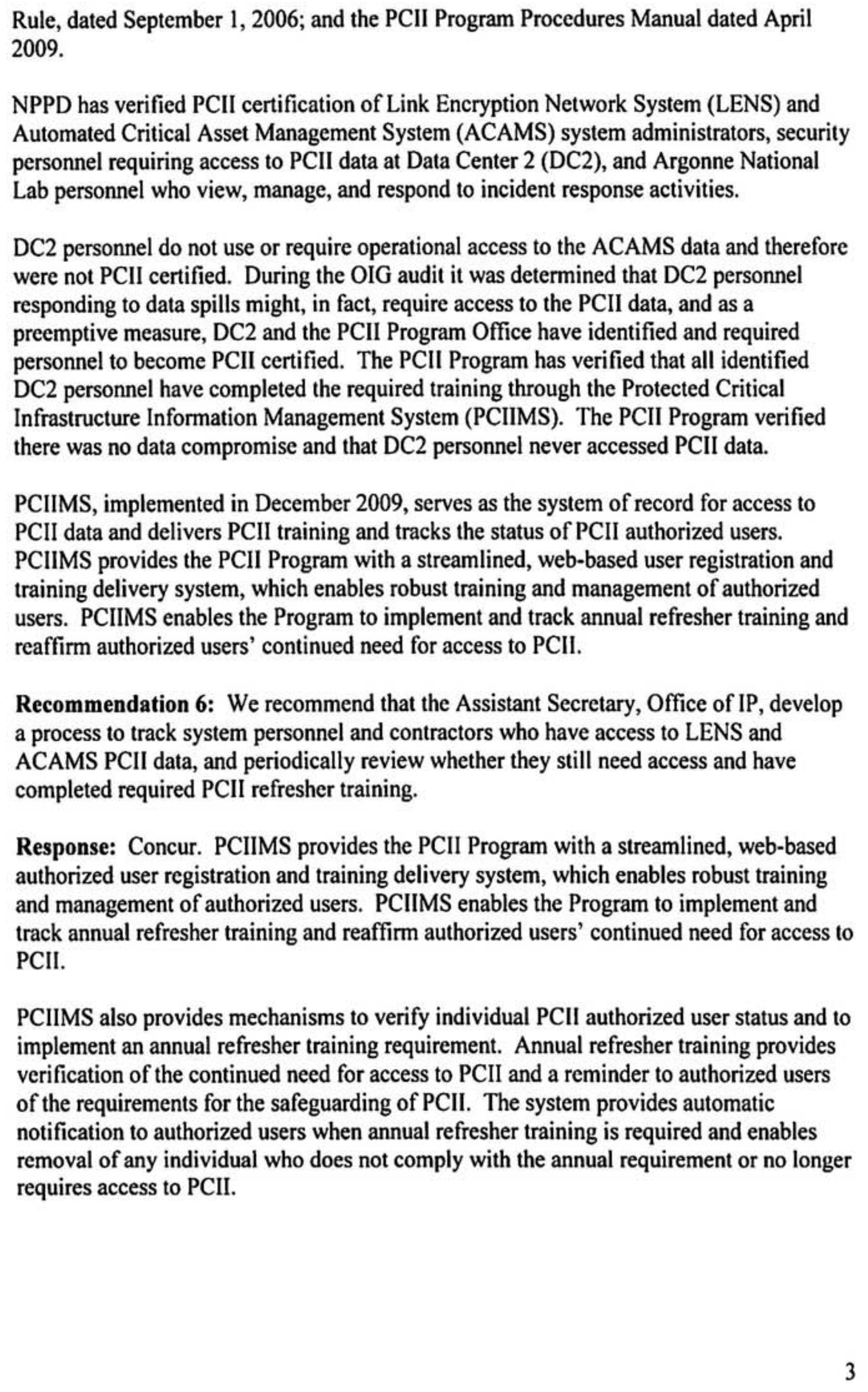
Response: Concur. CS&C's development of an overarching strategic implementation plan is an FY2011 objective, and will be linked to the most recent version of the NPPD strategic plan. The FY2011 and Fiscal Year 2012 (FY2012) NPPD strategic plans are in draft form. In the interim, CS&C will execute its strategic plan while also remaining cognizant of strategic initiatives at the NPPD level. The CS&C strategic plan will be aligned with the NPPD FY2011 and FY2012 strategic plans, since it will be informed partly by those draft versions. Additionally, the *Quadrennial Homeland Security Review* Mission 4 strategy will inform CS&C's planning process with respect to its cybersecurity mission. NPPD, the Department of Homeland Security (DHS) Office of Policy, and other public and private sector stakeholders are currently developing the Mission 4 strategy.

Recommendation 4: We recommend that the Assistant Secretary, Office of CS&C, develop and implement objective performance criteria and measures that can be used to track and evaluate the effectiveness of actions defined in its strategic implementation plan and used by management to assess CS&C's overall progress in attaining its strategic goals and milestones.

Response: Concur. CS&C's objective performance criteria and measures will be developed once the strategic implementation plan is completed.

Recommendation 5: We recommend that the Assistant Secretary, Office of Infrastructure Protection (IP), identify systems personnel, users, and contractors who have access to LENS or ACAMS PCII data to ensure that those personnel have obtained initial PCII certification and/or required refresher training to ensure appropriate handling and safeguarding of PCII.

Response: Concur. Paramount to the continued success of the Protected Critical Infrastructure Information (PCII) Program is the proper safeguarding and handling of the Critical Infrastructure Information (CII) voluntarily shared with the Federal Government. Accordingly, the PCII Program has developed comprehensive processes and procedures for the access, safeguarding, and handling of PCII to include robust authorized user training. These processes and procedures implement the requirements in the CII Act of 2002, 5 CFR Part 29, Procedures for Handling Critical Infrastructure Information; Final



Rule, dated September 1, 2006; and the PCII Program Procedures Manual dated April 2009.

NPPD has verified PCII certification of Link Encryption Network System (LENS) and Automated Critical Asset Management System (ACAMS) system administrators, security personnel requiring access to PCII data at Data Center 2 (DC2), and Argonne National Lab personnel who view, manage, and respond to incident response activities.

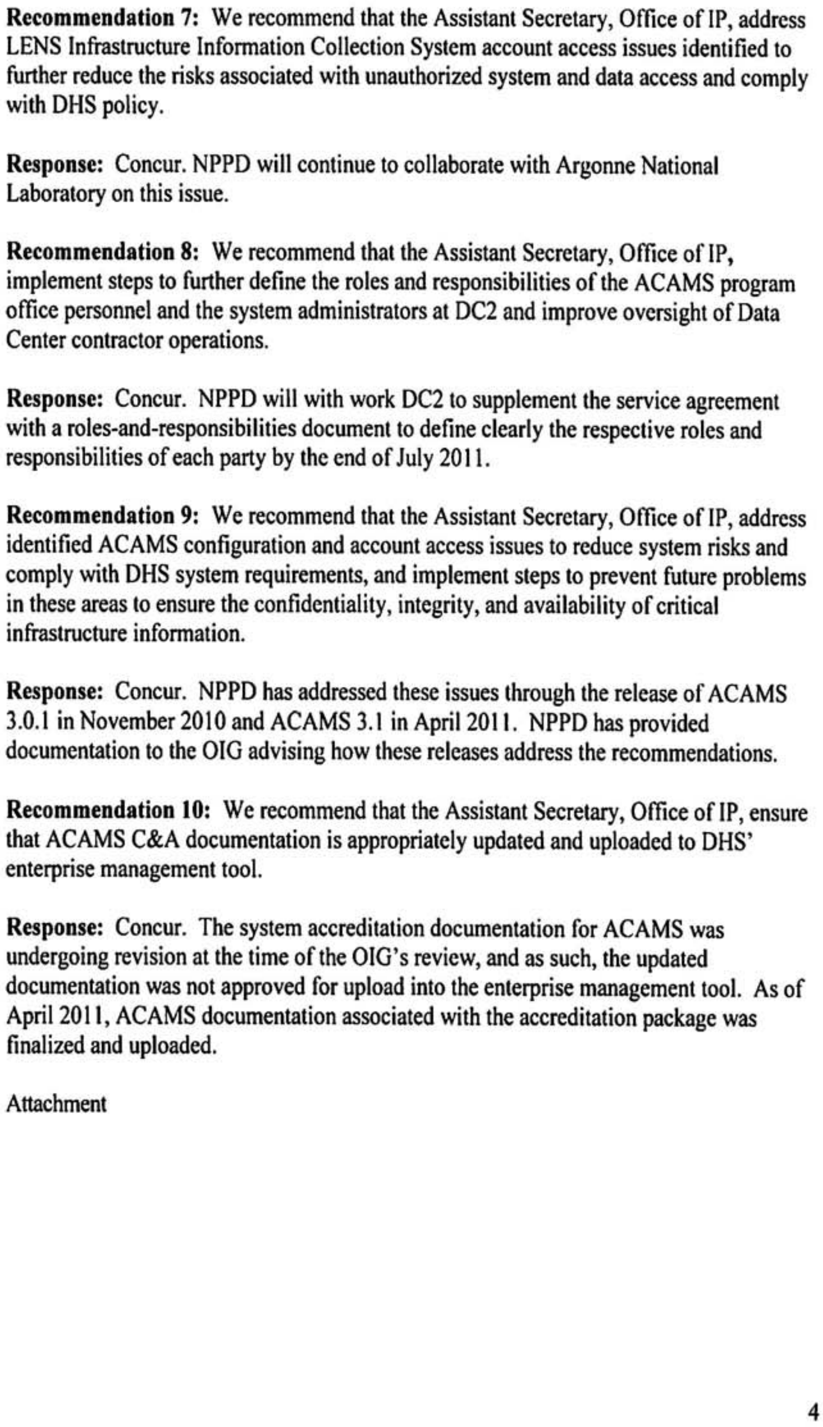
DC2 personnel do not use or require operational access to the ACAMS data and therefore were not PCII certified. During the OIG audit it was determined that DC2 personnel responding to data spills might, in fact, require access to the PCII data, and as a preemptive measure, DC2 and the PCII Program Office have identified and required personnel to become PCII certified. The PCII Program has verified that all identified DC2 personnel have completed the required training through the Protected Critical Infrastructure Information Management System (PCIIMS). The PCII Program verified there was no data compromise and that DC2 personnel never accessed PCII data.

PCIIMS, implemented in December 2009, serves as the system of record for access to PCII data and delivers PCII training and tracks the status of PCII authorized users. PCIIMS provides the PCII Program with a streamlined, web-based user registration and training delivery system, which enables robust training and management of authorized users. PCIIMS enables the Program to implement and track annual refresher training and reaffirm authorized users' continued need for access to PCII.

Recommendation 6: We recommend that the Assistant Secretary, Office of IP, develop a process to track system personnel and contractors who have access to LENS and ACAMS PCII data, and periodically review whether they still need access and have completed required PCII refresher training.

Response: Concur. PCIIMS provides the PCII Program with a streamlined, web-based authorized user registration and training delivery system, which enables robust training and management of authorized users. PCIIMS enables the Program to implement and track annual refresher training and reaffirm authorized users' continued need for access to PCII.

PCIIMS also provides mechanisms to verify individual PCII authorized user status and to implement an annual refresher training requirement. Annual refresher training provides verification of the continued need for access to PCII and a reminder to authorized users of the requirements for the safeguarding of PCII. The system provides automatic notification to authorized users when annual refresher training is required and enables removal of any individual who does not comply with the annual requirement or no longer requires access to PCII.



Recommendation 7: We recommend that the Assistant Secretary, Office of IP, address LENS Infrastructure Information Collection System account access issues identified to further reduce the risks associated with unauthorized system and data access and comply with DHS policy.

Response: Concur. NPPD will continue to collaborate with Argonne National Laboratory on this issue.

Recommendation 8: We recommend that the Assistant Secretary, Office of IP, implement steps to further define the roles and responsibilities of the ACAMS program office personnel and the system administrators at DC2 and improve oversight of Data Center contractor operations.

Response: Concur. NPPD will with work DC2 to supplement the service agreement with a roles-and-responsibilities document to define clearly the respective roles and responsibilities of each party by the end of July 2011.

Recommendation 9: We recommend that the Assistant Secretary, Office of IP, address identified ACAMS configuration and account access issues to reduce system risks and comply with DHS system requirements, and implement steps to prevent future problems in these areas to ensure the confidentiality, integrity, and availability of critical infrastructure information.

Response: Concur. NPPD has addressed these issues through the release of ACAMS 3.0.1 in November 2010 and ACAMS 3.1 in April 2011. NPPD has provided documentation to the OIG advising how these releases address the recommendations.

Recommendation 10: We recommend that the Assistant Secretary, Office of IP, ensure that ACAMS C&A documentation is appropriately updated and uploaded to DHS' enterprise management tool.

Response: Concur. The system accreditation documentation for ACAMS was undergoing revision at the time of the OIG's review, and as such, the updated documentation was not approved for upload into the enterprise management tool. As of April 2011, ACAMS documentation associated with the accreditation package was finalized and uploaded.

Attachment

Appendix C
Major Contributors to this Report

Information Security Audit Division

Chiu-Tong Tsang, Director
Barbara Bartuska, IT Audit Manager
Charles Twitty, Team Lead
Megan Ryno, Program Analyst
Amanda Strickler, IT Specialist
Michael Kim, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary, NPPD
Acting Deputy Under Secretary, NPPD
Chief Information Officer, DHS
Chief Information Security Officer, DHS
Chief Information Officer, NPPD
Chief Information Security Officer, NPPD
Director, Compliance and Oversight Program
Deputy Director, Compliance and Oversight Program
Director, OIG/GAO Audit Liaison Office, NPPD
Chief Information Security Officer Audit Liaison, DHS
CS&C External Affairs Audit Liaison
Office of IP Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603;

- Fax the complaint directly to us at (202) 254-4292;

- Email us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

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