Department of Homeland Security
Office of Inspector General

Challenges Remain in DHS' Efforts to Secure Control Systems

OIG-09-95

August 2009

Office of Inspector General

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

Homeland Security

AUG 12 2009

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 audits, inspections, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the National Cyber Security Division's (NCSD) Control Systems Security Program (CSSP) efforts to establish a cohesive partnership between the public and private sectors to reduce risk to the nation's critical infrastructure control systems. It is based on direct observations and analyses of applicable documents. We obtained additional supporting documentation through interviews with employees and contractors in the NCSD Program Office, the Office of Infrastructure Protection, the Idaho National Laboratory (INL), the Office of Intelligence and Analysis, the United States Computer Emergency Readiness Team (US-CERT), and various Sector Specific Agencies (SSAs).

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.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Table of Contents/Abbreviations

Abbreviations

CIKR	Critical Infrastructure and Key Resources
CS2SAT	Control System Cyber Security Self-Assessment Tool
CSCSWG	Cross-Sector Cyber Security Working Group
CSSP	Control Systems Security Program
DHS	Department of Homeland Security
FY	Fiscal Year
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICSJWG	Industrial Control Systems Joint Working Group
INL	Idaho National Laboratory
IT	Information Technology
NCSD	National Cyber Security Division
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
PSA	Protective Security Advisors
SSA	Sector-Specific Agency
US-CERT	United States Computer Emergency Readiness Team

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We reviewed the National Cyber Security Division's (NCSD) Control Systems Security Program (CSSP) to determine its effectiveness in improving cybersecurity for control systems within the nation's critical infrastructure and key resources. Control systems are vital to the operation of production systems within factories and plant facilities across the nation. They are used in industries, such as chemical, electric, oil and natural gas, and water and wastewater treatment. A disruption in control system operations may result in the loss of productivity and life, and have a negative impact on the economy and national security.

NCSD implemented its CSSP to coordinate the cybersecurity efforts for control systems between the public and private sectors. NCSD facilitates cybersecurity information sharing with the public and private sectors through various working groups, issuing white papers, and web postings. In coordination with other leading security organizations, NCSD jointly sponsors and participates in cybersecurity training. NCSD offers online training, via its United States Computer Emergency Readiness Team website, and conducts its own instructor-led training sessions designed to provide information on cyber threats and the mitigation of vulnerabilities. NCSD also performs vulnerability assessments of operational control systems and vendor equipment to improve their security posture.

While NCSD has made progress in implementing a cybersecurity program for control systems, opportunities still exist for improvements to its CSSP. NCSD needs to encourage more information sharing of critical infrastructures' needs, threats, and vulnerabilities between the public and private sectors. NCSD should increase the number of cybersecurity vulnerability assessments performed in order to reduce the overall risk to current operational control systems. NCSD should establish enhanced performance measures to ensure its mission and goals are attained as they relate to CSSP. Additionally, NCSD's education, training, and awareness program should be expanded to improve the public

and private sector personnel’s knowledge of control systems cybersecurity.

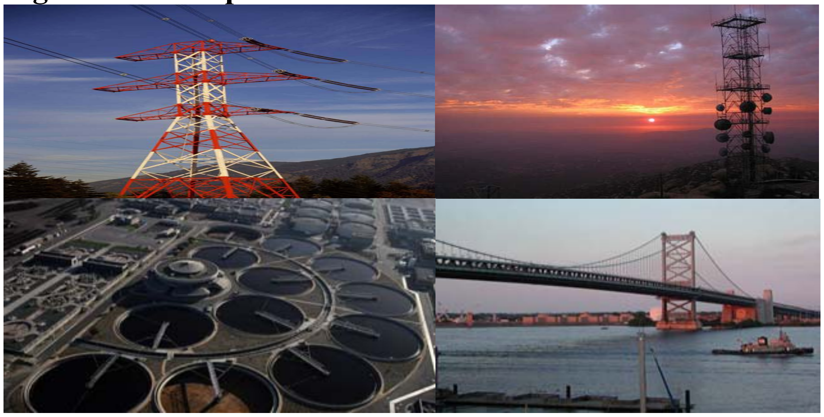
We originally proposed 8 recommendations to the Deputy Under Secretary of the National Protection and Programs Directorate (NPPD). Recommendation 7 was removed based on the response received from NPPD. NPPD has already begun to initiate actions to implement the remaining recommendations. NPPD’s response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

The information technology (IT) revolution has changed the way businesses and the public operate. Regardless of security implications, the nation shifted the control of essential processes in manufacturing, utilities, and communications to networked systems. Due to the nation’s reliance on the cyber infrastructure and the daily challenges of cybersecurity, the Department of Homeland Security (DHS) has the lead on coordinating efforts to enhance protection of the critical infrastructure and key resources (CIKR). Terrorists and spies are targeting public and private sector information networks in order to gain competitive advantages and cause disruptions in the nation’s CIKR.

Approximately 90% of critical infrastructures are privately owned and operated. The nation’s CIKR are composed of public and private institutions in 18 sectors: Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Healthcare and Public Health, IT, National Monuments and Icons, Nuclear Reactors, Materials, and Waste, Postal and Shipping, Transportation Systems, and Water. Control systems operate the production systems in these CIKR sectors.

Figure 1: Examples of CIKR Sectors



Initially, control systems had little resemblance to traditional IT systems because they were isolated systems running proprietary protocols using specialized hardware and software. Today, control systems are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities. Control systems that previously used proprietary protocols are becoming Internet Protocol-enabled, which can increase the likelihood of cyber vulnerabilities and incidents.

According to the *Homeland Security Act of 2002*, the Secretary of DHS is assigned the responsibility to coordinate the overall national effort to enhance the protection of CIKR. Within DHS, NCSD works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets. NCSD has two overarching priorities: (1) to build an effective national cyberspace response system; and (2) to implement a cyber risk management program for critical infrastructure protection. Furthermore, NCSD is to provide guidance and methodologies to sectors to assist them in managing cyber risks and to develop effective and appropriate protective plans and measures.

Although each of the critical infrastructure industries is vastly different, they all have one thing in common – their dependency on control systems to monitor, control, and safeguard vital processes. NCSD has recognized that the protection and security of control systems is essential to the nation's security and economy. NCSD established its CSSP to help coordinate cybersecurity efforts among public entities, as well as control systems owners, operators, and vendors. The goal of the program is to lead a cohesive effort between public and private sectors to reduce the risk and improve the security posture of control systems within and across all CIKR. Furthermore, NCSD coordinates risk mitigation activities to reduce the likelihood and severity of successful cyber attacks against critical control systems.

Results of Audit

Progress Made in Facilitating Control Systems Cybersecurity Awareness

NCSD has made progress in broadening awareness about control systems cybersecurity. NCSD undertook efforts to coordinate protection activities of critical infrastructure sectors and serve as the focal point for the security of cyberspace.

NCSD conducted exercises in order to demonstrate to control systems owners the possible effects to their systems as a result of a cyber incident. One such exercise was the Aurora project which specifically focused on the use of digital protection control devices.[1] NCSD issued a series of reports designed to improve cybersecurity by recommending best practices to address common hardware and software vulnerabilities. NCSD also partnered with several of the Sector Specific Agencies (SSAs) in preparing their sector specific roadmaps in addressing control systems cybersecurity initiatives. Additionally, NCSD established collaborative relationships with the public and private sectors to facilitate cybersecurity awareness for the control systems that protect the nation’s CIKR. Other progress included:

- Establishing the CSSP and the hiring of staff to address cybersecurity issues directly related to control systems. Additionally, a CSSP analyst assists United States Computer Emergency Readiness Team (US-CERT) with control systems-related incidents to quickly coordinate the activities needed to address the event and inform the public and private sectors.

- Establishing working groups within the public and private sectors to provide resources and forums for organizations to better approach cybersecurity issues. The working groups assist with the coordination of control systems cybersecurity initiatives.

[1] The Aurora project, sponsored by DHS, demonstrated the effect of hacking into a power plant’s control station via computers and digital devices.

- Distributing US-CERT vulnerability and critical infrastructure information notices pertaining to specific vulnerabilities, as well as quarterly trend and analysis reports to control system representatives.[2]

- Conducting in-person and online training. Training consists of basic understanding and awareness of control systems' security sessions, intermediate courses for managers and IT professionals, and classes on common vulnerabilities, as well as vulnerabilities specific to the energy sector.

While progress has been made, NCSD still faces difficult challenges in effectively reducing the cybersecurity risks to the nation's critical infrastructure. Improvements are needed in NCSD's effort to protect and secure controls systems that are essential to the nation's security and economy.

Improved Information Sharing and Communication Will Enhance Control Systems Cybersecurity

Though NCSD has made progress in establishing and monitoring collaborative efforts between the public and private sectors, communication issues continue to exist. Without the public and private sectors working together to identify and share critical cyber information, there is little assurance that critical data will be made available to key stakeholders in order to prevent, detect, or recover from a cyber incident.

In 2007, the Government Accountability Office (GAO) and our office reported that NCSD needed to improve information sharing and communications efforts within the control systems community.[3] We recommended that NCSD develop a strategy for guiding and coordinating control systems security efforts across public and private sectors. The strategy was to include a description of various public and private entities' roles and responsibilities, and mechanisms to improve information sharing and the dissemination of sensitive information to key cybersecurity personnel.

In response to these recommendations, NCSD drafted its *Strategy for Securing Control Systems*, dated December 2008. The primary goal of the

[2] Vulnerability and critical infrastructure information notices are public warnings describing the nature of an identified vulnerability, the software product, its impact, and the solution for correcting the vulnerability.
[3] GAO-07-1036, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain* (September 2007) and OIG-07-48, *Challenges Remain in Securing the Nation's Cyber Infrastructure* (June 2007).

strategy is to create a common vision for sector participation, information sharing, coalition building, and leadership to guide stakeholder activities and improve overall coordination. In the strategy, NCSD encourages the SSAs to coordinate cybersecurity efforts within their respective sectors. SSAs are to facilitate and enhance communication within the private sectors so that information about attack trends, vulnerabilities, and best practices is shared. Additionally, SSAs are to raise awareness, identify and remediate vulnerabilities when possible, disseminate sector-specific threat warnings, and plan recovery operations for the infrastructure.

The public and private sectors need information on cyber risks and hazards so that they can protect CIKR. Sharing control systems security information is an important element in reducing cyber risks. Information to be shared includes situational awareness, vulnerability detection and mitigation, and best practices.

Some SSAs, however, expressed concern with NCSD's leadership role in the efforts to address cybersecurity and information sharing. Many SSAs remained dissatisfied with the amount of shared information regarding vulnerability detection and mitigation. Not only were SSAs unaware of the latest cybersecurity developments and efforts, in many instances the SSAs were not informed of the results of cyber control system vulnerability assessments performed by NCSD or other federal agencies.[4]

When NCSD performed its vulnerability assessments of private sectors' control systems, the results were sometimes discussed with private sector personnel, and excluded the SSAs. In other instances, NCSD attempted to share the results of vulnerability assessments with the SSAs, but were prevented from sharing this information because of non-disclosure agreement restrictions between NCSD and the private sector owners. Furthermore, SSAs were unaware of cyber control system vulnerability assessment results that were performed by their regulatory SSA counterparts, such as the Department of Energy and the Department of Defense.

Homeland Security Presidential Directive - 7(HSPD-7) requires that DHS and the SSAs collaborate with the appropriate private sector entities and encourage the development of information sharing and analysis mechanisms. Information sharing and analysis should relate to physical and cyber threats, vulnerabilities, incidents, protective measures, and best practices. Furthermore, *The National Strategy to Secure Cyberspace*

[4] NCSD contracts with the Idaho National Laboratory (INL), a federally funded Department of Energy national laboratory that primarily focuses on energy and critical infrastructure security, to perform on-site cyber vulnerability assessments of control systems and evaluation of vendors' new system products.

recommends that DHS coordinate with other federal agencies to share specific warning information and advice about appropriate protective measures and countermeasures.

In the past, NCSD did not consistently hold its monthly or quarterly working group meetings with the SSAs to discuss cybersecurity developments and their impact on control systems. According to some SSA officials, the meetings were held infrequently during the calendar year 2008. The last meeting was held on May 2008 to discuss specific vulnerabilities. Since January 2009, NCSD has attempted to improve its relationship with the SSAs and the private sector by conducting monthly working group meetings to discuss cybersecurity efforts. During these meetings, NCSD discussed updates on cybersecurity initiatives and activities, the latest incident reporting by US-CERT, sub-working groups' progress, and upcoming training.

It is essential that the control systems community receives and is able to share critical information about identified vulnerabilities and reported events so that appropriate steps are taken to reduce the effects of a cyber incident. Therefore, the collaborative working groups should establish the trust and credibility needed to encourage open sharing of cybersecurity efforts and results. Information sharing also allows the control systems community to leverage other protective means used by the public and private sectors to secure control systems.

Recommendations

We recommend that the Deputy Under Secretary of the National Protection and Programs Directorate (NPPD) require NCSD to:

Recommendation #1: Consistently hold monthly working group meetings to coordinate control systems security efforts and enhance information sharing between the public and private sectors.

Recommendation #2: Establish alternative measures to reduce the non-disclosure restrictions on sharing control system vulnerability information. Possible alternatives could include the use of anonymity when gathering and reporting vulnerability information among stakeholders including system owners and SSAs.

Recommendation #3: Hold a joint conference where all affected stakeholders can offer or provide remedy in alleviating prohibitions on sharing vulnerability information among control systems owners.

Management Comments and OIG Analysis

NPPD concurred with recommendation 1. NCSD is already in compliance with this recommendation through a separate means, the Cross-Sector Cyber Security Working Group (CSCSWG) which was established in 2007 and meets monthly to coordinate cybersecurity in CIKR sectors.

In addition, the NCSD recently established the Industrial Control Systems Joint Working Group (ICSJWG) to coordinate security initiatives specifically associated with CIKR control systems. The ICSJWG meets quarterly and holds semi-annual conferences, but is planning to begin conducting monthly coordination meetings.

We agree that the steps that NPPD has taken, and plans to take, satisfy this recommendation. This recommendation will remain resolved and open until NPPD provides further updates on the progress of the monthly meetings.

NPPD concurred with recommendation 2. Non-disclosure agreements will always be necessary for vendor system assessments to protect proprietary information about system configurations and vulnerabilities. NCSD, however, encourages vendors to develop mitigation strategies, to share these strategies with their user base, and to report progress on their mitigation efforts. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) publishes security bulletins in cooperation with the US-CERT, but keeps specific information about vendors and event locations confidential. The CSSP also issues an annual report listing common vulnerabilities within control systems associated with CIKR sectors.

We agree that the steps that NPPD has taken, and plans to take, satisfy this recommendation. This recommendation will remain resolved and open until NPPD provides copies of ICS-CERT security bulletins and the annual report listing common vulnerabilities within control systems associated with CIKR sectors.

NPPD concurred with recommendation 3. A subgroup devoted to improving information sharing was formed under the auspices of the ICSJWG to address challenges associated with protecting sensitive and proprietary information. This subgroup, called the Information Sharing Subgroup, has developed a charter and will work with the CIKR community to develop a process for improving cybersecurity information sharing among control system stakeholders.

We agree that the steps that NPPD has taken, and plans to take, satisfy this recommendation. This recommendation will remain resolved and open until NPPD provides a copy of the Information Sharing Subgroup charter and develops the process for information sharing.

Increasing the Number of Vulnerability Assessments Can Reduce Sectors' Risks

Without an effective vulnerability assessment program, NCSD cannot develop strategies to mitigate common and sector-specific vulnerabilities. Through INL, NCSD has developed a vulnerability assessment program to reduce cyber risks for control systems and new vendor products. NCSD performs the following two types of assessments:

- On-site cybersecurity control system vulnerability assessments – Performed on existing control systems to evaluate the current security posture. NCSD partners with the Protective Security Advisors (PSA) program, under NPPD's Office of Infrastructure Protection, to perform on-site assessments. NCSD assesses cybersecurity, while the Office of Infrastructure Protection assesses the physical security of the facility.

- Vendor system assessments – Focused on building security into hardware and software IT products during development. INL partners with selected vendors to evaluate new control system products for security vulnerabilities. INL uses nonintrusive methods, such as reviewing network diagrams and firewall rules, and performs a hands-on assessment of a duplicate nonproduction installation of the system. INL and the vendors sign a non-disclosure agreement to protect proprietary information and ensure confidentiality.

NCSD's on-site vulnerability assessments were performed in 6 of the 18 sectors: Chemical, Dams, Energy, Healthcare and Public Health, Transportation, and Water. Vulnerability assessments identify areas of weakness in software, hardware, and operational equipment that are susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts. As part of these assessments, NCSD also determines what actions should be taken to mitigate risks.

NCSD tasked cybersecurity experts, such as INL, other national laboratories, and control system companies, to perform vulnerability assessments of control systems and network components. Additionally, the cybersecurity experts provide services to mitigate vulnerabilities and build a security culture within the control systems community. For example, they conduct outreach and awareness programs, develop and disseminate control systems security products, and provide a capability to respond to threats, vulnerabilities, and incidents.

INL also developed the automated Control System Cyber Security Self-Assessment Tool (CS2SAT). INL and the cybersecurity experts use CS2SAT to perform on-site vulnerability assessments. The CS2SAT tool provides a series of tests based on recognized security standards within the control system community. The tool is designed to identify gaps between the controls implemented on a system and the controls that should be implemented according to standards. Based on the identified gaps, recommendations are made to correct cited weaknesses. INL and the cybersecurity experts train private sector personnel on how to use the CS2SAT tool so that they can perform self-assessments of their control systems.

NCSD has conducted 11 on-site cybersecurity vulnerability assessments at private sector sites to date. NCSD discussed identified weaknesses, lessons learned, and best practices with the private sector owners. During FY 2008, 15 vendor product assessments were performed.

In its interagency agreement with INL, NCSD did not define its expected number of on-site and vendor product vulnerability assessments to be performed during FY 2008. For FY 2009, NCSD budgeted for 12 on-site cyber assessments to be conducted. NCSD personnel did not yet know how many vendor product assessments would be conducted during FY 2009.

In addition to NCSD, other federal agencies, such as the Department of Energy and the Department of Defense, perform control system vulnerability assessments. Most of the regulatory SSAs also perform periodic vulnerability assessments using customized assessment tools. The SSAs, however, do not consistently share the results of their assessments with the control systems community.

Participation in NCSD's vulnerability assessment program is voluntary and available to any interested control systems owner. NCSD does not have the authority to require assessments or the implementation of recommendations. As a result, some sectors – Agriculture and Food – have not had cybersecurity vulnerability assessments performed. According to NCSD management and the SSAs, cybersecurity is not a priority for most control systems owners because the importance of cybersecurity or its impact on their systems is not clearly understood.

The National Infrastructure Protection Plan (NIPP) requires DHS to ensure that comprehensive vulnerability assessments are performed for CIKR. Additionally, the NIPP requires SSAs and security partners to facilitate vulnerability assessment activities within their sectors. SSAs are responsible for working with DHS to validate the results of those assessments for assets that are of the greatest concern from the sector perspective.

DHS must work with the SSAs and control systems owners, as well as other security partners, to identify weaknesses and vulnerabilities in control systems. Without effective on-site cybersecurity assessments of control systems to identify and mitigate vulnerabilities and risks, critical control systems may be at risk of cyber attacks.

On-site and vendor system assessments allow NCSD to conduct trend analyses of vulnerabilities discovered, which would aid NCSD in identifying events that indicate increasing interest or significant developments. Additionally, NCSD should follow up on previously conducted assessments to determine the risk reduction of actions taken on mitigated vulnerabilities. The follow up program further demonstrates to the public and private sectors that improvements are being made in control systems cybersecurity. With assessment results, NCSD and the SSAs would be in a better position to help inform the control systems community of critical security investments that should be made to protect their systems.

Recommendations

We recommend that the Deputy Under Secretary of NPPD require NCSD to:

Recommendation #4: Increase the number of on-site assessments performed of the CIKR by:

- Seeking assistance from the Office of Infrastructure Protection via its PSA Program to perform cyber assessments when they perform physical security assessments.

- Encouraging the assistance of the SSAs in performing on-site cybersecurity assessments.

- Leveraging partnerships among the various Federal agencies in performing cybersecurity assessments.

- Developing incentive programs to encourage participation.

Recommendation #5: Develop a process to follow-up on the vulnerability assessments performed to obtain feedback on the actions implemented.

Management Comments and OIG Analysis

NPPD concurred with recommendation 4. The CSSP has planned for 12 on-site assessments in its FY09 work scope and agrees that additional assessments should be performed. NCSD works closely with the Office of Infrastructure Protection's regional PSAs to find asset owners in need of on-site assistance. NCSD also supports the Office of Infrastructure Protection with its Regional Resiliency Assessment Program by providing cybersecurity expertise during on-site assessments. NCSD also works with the SSAs through the ICSJWG to identify specific sector needs and provide support in developing and implementing sector roadmaps to secure control systems. NCSD has already scheduled training workshops for the water sector as that sector rolls out their roadmap. This training will include instruction in the use of the self-assessment tools and offers for on-site assessment support.

We agree that the steps that NPPD has taken, and plans to take, satisfy this recommendation. This recommendation will remain resolved and open until NPPD provides the 12 assessment trip reports and copies of the training packages for the water sector.

NPPD concurred with recommendation 5. Currently the vendors that participate in laboratory system assessments provide the program with a plan for developing and implementing mitigation strategies to eliminate the discovered vulnerabilities and share information with their user base.

Also, ICS-CERT has provided follow-up actions in cases where the industry has requested assistance for analysis of specific cyber events within their networks. Although it is understood that all responses back to ICS-CERT are voluntary, organizations have responded with acknowledgement that the assistance CSSP has provided was indeed useful to remediate vulnerabilities.

Lastly, NCSD is developing a process to collect feedback from stakeholders as they apply mitigation strategies through roadmap implementation in each sector. This process will encourage the sectors to collect common vulnerabilities in their security posture, which are discovered during the self-assessment process.

We agree that the steps that NPPD has taken, and plans to take, satisfy this recommendation. This recommendation will remain resolved and open until NPPD provides a copy of the policy and procedures outlining the follow up process to collect feedback from the stakeholders and a copy of a report log showing ICS-CERT's follow up efforts.

Specific Performance Measures Should be Defined to Assess Effectiveness of CSSP

Though performance measures exist, NCSD cannot determine that its CSSP is achieving the intended results and impact without developing sufficient outcome measures. As a result, NCSD will have difficulty in determining how effective its CSSP is in achieving its goal to strengthen control systems security.

Performance measures indicate whether a program is meeting its goals and whether expected results are being achieved. Furthermore, performance measures address the direct products and services delivered by a program (outputs) and the results of those products and services (outcomes). Outcomes are important as they often describe the intended results or consequences that will occur from carrying out a program or activity.

NCSD identified the following performance measures to monitor its overall cybersecurity efforts:

- Percentage of CIKR sectors that incorporated cybersecurity vulnerability assessments or its questions/concepts into their sector risk assessment methodologies;

- Percentage of targeted beneficiary satisfaction with cybersecurity collaboration events;

- Percentage of high priority stakeholders using CS2SAT to conduct assessments and mitigate known vulnerabilities;

- Number of cybersecurity information sharing products distributed to stakeholders; and

- Cost per incident (in U.S. dollars) reported to US-CERT.

Although overall performance measures have been established, NCSD has not identified specific outcome performance measures to monitor CSSP's progress with control systems cybersecurity. Also, NCSD does not monitor the control systems cybersecurity progress at the sector or national level. Performance measures at the sector and national levels allow for comparison and analysis between the different sectors.

Currently, NCSD's performance measure for CSSP relates to the number of cybersecurity information sharing products distributed to cybersecurity stakeholders. This performance measure emphasizes "output" (i.e., number of conferences conducted and sponsored, number of training sessions conducted and sponsored, and number of major reports issued), but these measures do not evaluate the "outcome" of products and services. Outcomes need to measure the effect of training on the control systems community. For example, personnel's increased cybersecurity education can lead to the use of tools or security assessments to identify and mitigate the risks of a control system attack.

According to the NIPP, a measure-based system should be used to provide feedback on efforts to attain the goals and supporting objectives of the programs implemented. Measures provide a basis for establishing accountability, documenting actual performance, promoting effective management, and reassessing goals and objectives. Additionally, measures offer a quantitative assessment to affirm that specific objectives are being met and identify gaps in the national effort or supporting sector efforts.

The Office of Management and Budget requires agencies to prepare an annual performance plan covering each program activity set forth in the budget of the agency. In the plan, goals are established to define the level of performance to be achieved by the budgeted program activity. In addition, performance measures should be objective and quantifiable, and should help management by providing information on how resources and efforts should be allocated to ensure program effectiveness.

By comparing performance to goals, NCSD can modify its strategies to ensure that its mission and objectives are achieved. Additional performance measures will enable NCSD to improve its accountability for control systems security, comply with laws and regulations, and increase the effectiveness of its CSSP.

Recommendation

We recommend that the Deputy Under Secretary of NPPD require NCSD to:

Recommendation #6: Define specific outcome-based performance measures that can be used to review and periodically evaluate the success of its CSSP in securing the nation's CIKR.

Management Comments and OIG Analysis

NPPD concurred with recommendation 6. NCSD agrees that additional performance measures should be developed to evaluate progress in securing the CIKR against cyber attacks. The CSSP is currently developing and evaluating new methods for measuring security progress and is working with specific sectors as they include performance measures in their roadmap goals and milestones.

The CSSP currently collects statistics for the number of participants in the various training courses offered. The program also works closely with vendors as they eliminate discovered vulnerabilities and share information with their user base.

We agree that the steps that NPPD has taken, and plans to take, satisfy this recommendation. This recommendation will remain resolved and open until NPPD provides a copy of the updated performance measures.

Formal Training Program Will Increase Public Awareness and Protection Expertise

NCSD has not implemented a formal training program for the control systems community. Without adequate training, control systems owners may not be able to handle disruptions in services and ensure business continuity in the event of a cyber attack or breach.

Training allows the control systems community to develop and maintain key CIKR protection expertise. It is important that individuals are appropriately trained on how to fulfill their security responsibilities. Furthermore, training should enhance the knowledge and skills required to detect, deter, defend, and mitigate cyber events, activities, and incidents that threaten the CIKR.

Since NCSD is the focal point for cybersecurity, all 18 critical sectors seek guidance from NCSD on how to protect their specific sector against vulnerabilities and threats that may directly impact their control systems. NCSD contracted with INL to perform training sessions with the CIKR sectors. Currently, NCSD's training program is limited to general control systems security and energy sector-related topics. There is no specialized training for the other 17 sectors to improve personnel's capabilities in securing their control systems.

NCSD is in the process of working with INL to establish a training program that will include a technical curriculum related to engineering, IT, and computer science. They also plan to leverage current training courses. However, due to staffing issues, it is unknown when the program will be completed or implemented.

In developing its training program, NCSD should include operational and technical topics, such as buffer zone protection, surveillance detection, high-risk target awareness, incident reporting, and accepted control system security practices. NCSD should also work with the SSAs and other CIKR partners in developing courses for its formal training program.

The NIPP stipulates that DHS, in conjunction with the SSAs and other CIKR partners, should provide training programs to security partners from which they can obtain specialized training to enhance critical infrastructure resource protection. Additionally, *The National Strategy to Secure Cyberspace* requires that a national cyberspace security and training program be developed. According to *The National Strategy to Secure Cyberspace*, DHS must implement and encourage the establishment of programs to advance the training of cybersecurity professionals. DHS must also develop a coordination mechanism linking federal cybersecurity training programs. The cyberspace training program is to raise cybersecurity awareness in companies, government agencies, universities, and among computer users.

A training program for the control systems community would ensure that situational awareness and the impact of vulnerabilities and threats are conveyed so that they can be addressed. By providing the latest advances in risk mitigation and best practices, the control systems community can improve the security of their systems, thus, contributing to the overall protection of CIKR.

Recommendations

We recommend that the Deputy Under Secretary of NPPD require NCSD to:

Recommendation #7: Develop specialized training for all CIKR sectors in order to improve public and private sector knowledge of control systems and cybersecurity risks.

Recommendation #8: Market the availability of formal training courses to the control systems community to stress the awareness of cybersecurity and its importance.

Management Comments and OIG Analysis

NCSD did not concur with recommendation 7. In general, NCSD does not recommend that specialized training for each sector be developed since control system applications and associated vulnerabilities are ubiquitous across all sectors. The current training curriculum already targets multiple sectors with examples of threats and consequences from many industries. Furthermore, control system components are used in every industry to perform the same control functions, irrespective to the process they control. When requested, the program has provided and will continue to develop specialized training for individual sectors to tailor it to their specific processes.

We agreed to remove this recommendation based on the response provided by NPPD. Additionally, NPPD indicated in its response to recommendation 4 that NCSD is already scheduling training workshops for the water sector.

NCSD concurred with recommendation 8. NSCD currently operates an extensive marketing effort to multiple sectors to highlights its products and training. This marketing is provided in the form of:

- Presentations and keynote address at national and international industry conferences;

- Booths at conferences which highlight the program products and training offerings;

- Postings on the US-CERT and Control Systems website;

- Invitations at ICSJWG and CSCSWG Meetings; and

- Invitations to training at on-site assessments.

NCSD plans to continue efforts to promote training and continuously improve the training curriculum.

We agree that the steps NPPD has taken satisfy this recommendation. Additionally, NPPD has provided copies of the ICSJWG Inaugural Symposium and the upcoming ISCJWG 2009 Fall Conference and Call for Papers, which advertised NCSD training. This recommendation is resolved and closed.

Appendix A
Purpose, Scope, and Methodology

The objective of our audit was to determine whether NCSD is effective in its efforts to improve cybersecurity within the nation's critical infrastructure. We determined whether NCSD:

- Is effectively reducing the risk to the nation's CIKR by providing guidance to the control system community through a variety of mechanisms, trends, and methodologies.

- Is properly monitoring collaborative efforts among federal, states, local and control systems owners, operators, and vendors.

- Has an incident response procedure in place to provide a level of assurance that the nation's control systems would recover from attacks in a timely manner.

Our review focused on NCSD's program for control system security based on the requirements outlined in HSPD 7, *Critical Infrastructure Identification*, *Prioritization, and Protection* (December 2003), NIPP (June 2006), *The National Strategy to Secure Cyberspace* (February 2003), National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (December 2007), and National Institute of Standards and Technology Special Publication 800-82, *Guide to Industrial Control System Security* (September 2008).

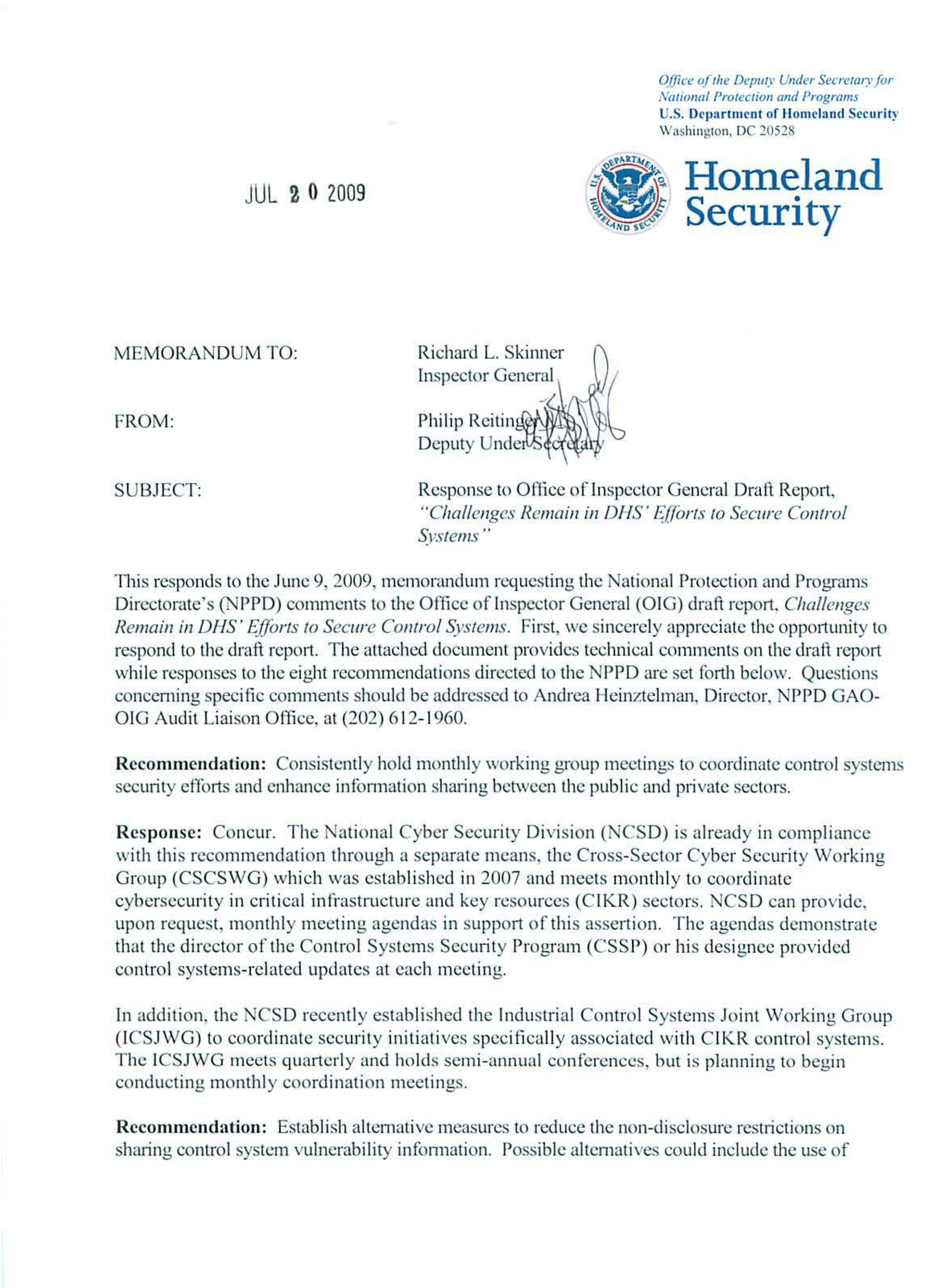
We interviewed NCSD and Office of Infrastructure Protection management, as well as personnel from the INL, including the program managers and the Cyber Security Assessment Lead. Furthermore, we interviewed personnel from various sectors, including Chemical, Commercial Facilities, Dams, Defense Industrial Base, Energy, Nuclear Reactors, Materials and Waste, and Water. We received feedback regarding NCSD's communication and information sharing, vulnerability assessments, and cybersecurity concerns.

We evaluated the quality of NCSD's performance measures. We reviewed vulnerability notes and critical infrastructure information notices to determine whether US-CERT issued adequate and timely incident response reports to the control systems community. We also evaluated the CS2SAT, a questionnaire used to conduct cybersecurity assessments, and determined whether security assessments are being performed.

We conducted our work at the program level and conducted a site visit at INL in Idaho Falls. We conducted this performance audit between December 2008 and April 2009 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Major OIG contributors to the audit are identified in Appendix C.

The principal OIG points of contact for the audit are Frank W. Deffer, Assistant Inspector General, Information Technology Audits, at (202) 254-4041, and Edward G. Coleman, Director, Information Security Audit Division, at (202) 254-5444.

Appendix B
Management Comments to the Draft Report



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

Homeland Security

JUL 20 2009

MEMORANDUM TO: Richard L. Skinner
Inspector General

FROM: Philip Reitinger
Deputy Under Secretary

SUBJECT: Response to Office of Inspector General Draft Report, *"Challenges Remain in DHS' Efforts to Secure Control Systems"*

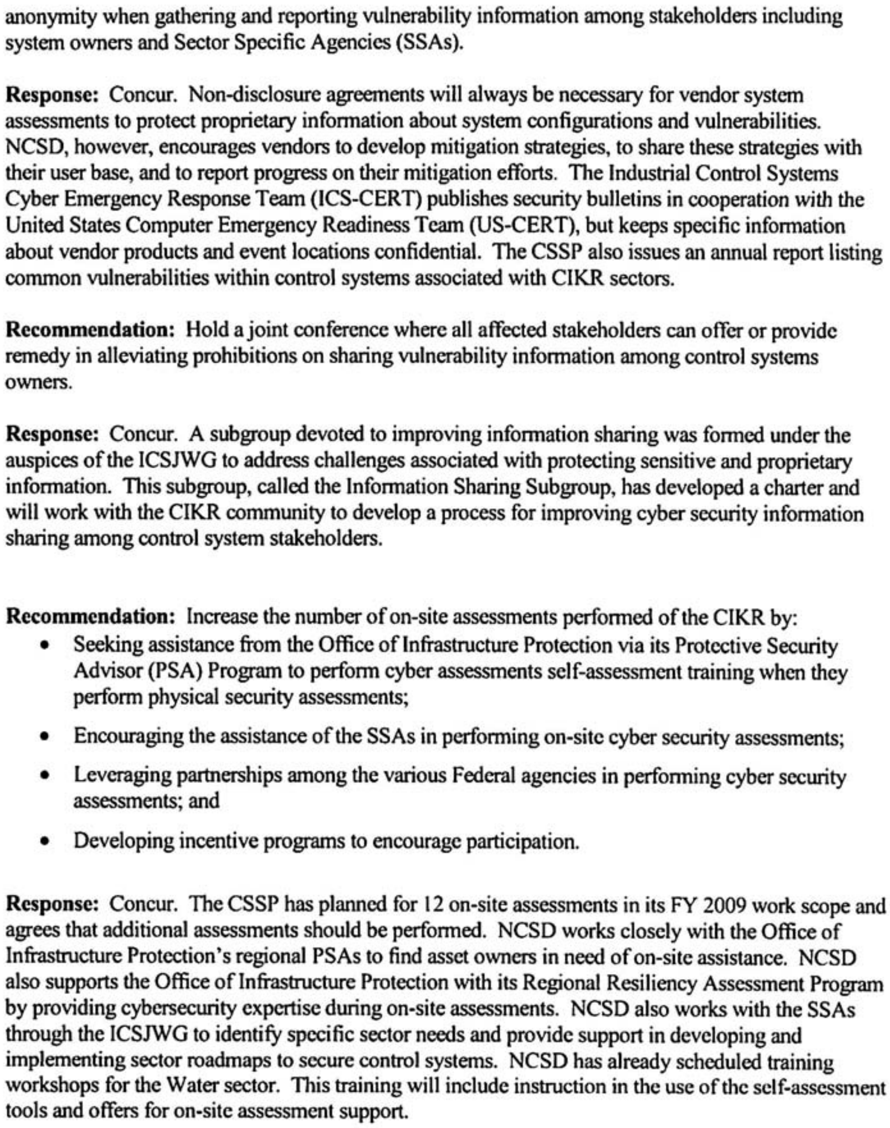
This responds to the June 9, 2009, memorandum requesting the National Protection and Programs Directorate's (NPPD) comments to the Office of Inspector General (OIG) draft report, *Challenges Remain in DHS' Efforts to Secure Control Systems*. First, we sincerely appreciate the opportunity to respond to the draft report. The attached document provides technical comments on the draft report while responses to the eight recommendations directed to the NPPD are set forth below. Questions concerning specific comments should be addressed to Andrea Heinztelman, Director, NPPD GAO-OIG Audit Liaison Office, at (202) 612-1960.

Recommendation: Consistently hold monthly working group meetings to coordinate control systems security efforts and enhance information sharing between the public and private sectors.

Response: Concur. The National Cyber Security Division (NCSD) is already in compliance with this recommendation through a separate means, the Cross-Sector Cyber Security Working Group (CSCSWG) which was established in 2007 and meets monthly to coordinate cybersecurity in critical infrastructure and key resources (CIKR) sectors. NCSD can provide, upon request, monthly meeting agendas in support of this assertion. The agendas demonstrate that the director of the Control Systems Security Program (CSSP) or his designee provided control systems-related updates at each meeting.

In addition, the NCSD recently established the Industrial Control Systems Joint Working Group (ICSJWG) to coordinate security initiatives specifically associated with CIKR control systems. The ICSJWG meets quarterly and holds semi-annual conferences, but is planning to begin conducting monthly coordination meetings.

Recommendation: Establish alternative measures to reduce the non-disclosure restrictions on sharing control system vulnerability information. Possible alternatives could include the use of



anonymity when gathering and reporting vulnerability information among stakeholders including system owners and Sector Specific Agencies (SSAs).

Response: Concur. Non-disclosure agreements will always be necessary for vendor system assessments to protect proprietary information about system configurations and vulnerabilities. NCSD, however, encourages vendors to develop mitigation strategies, to share these strategies with their user base, and to report progress on their mitigation efforts. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) publishes security bulletins in cooperation with the United States Computer Emergency Readiness Team (US-CERT), but keeps specific information about vendor products and event locations confidential. The CSSP also issues an annual report listing common vulnerabilities within control systems associated with CIKR sectors.

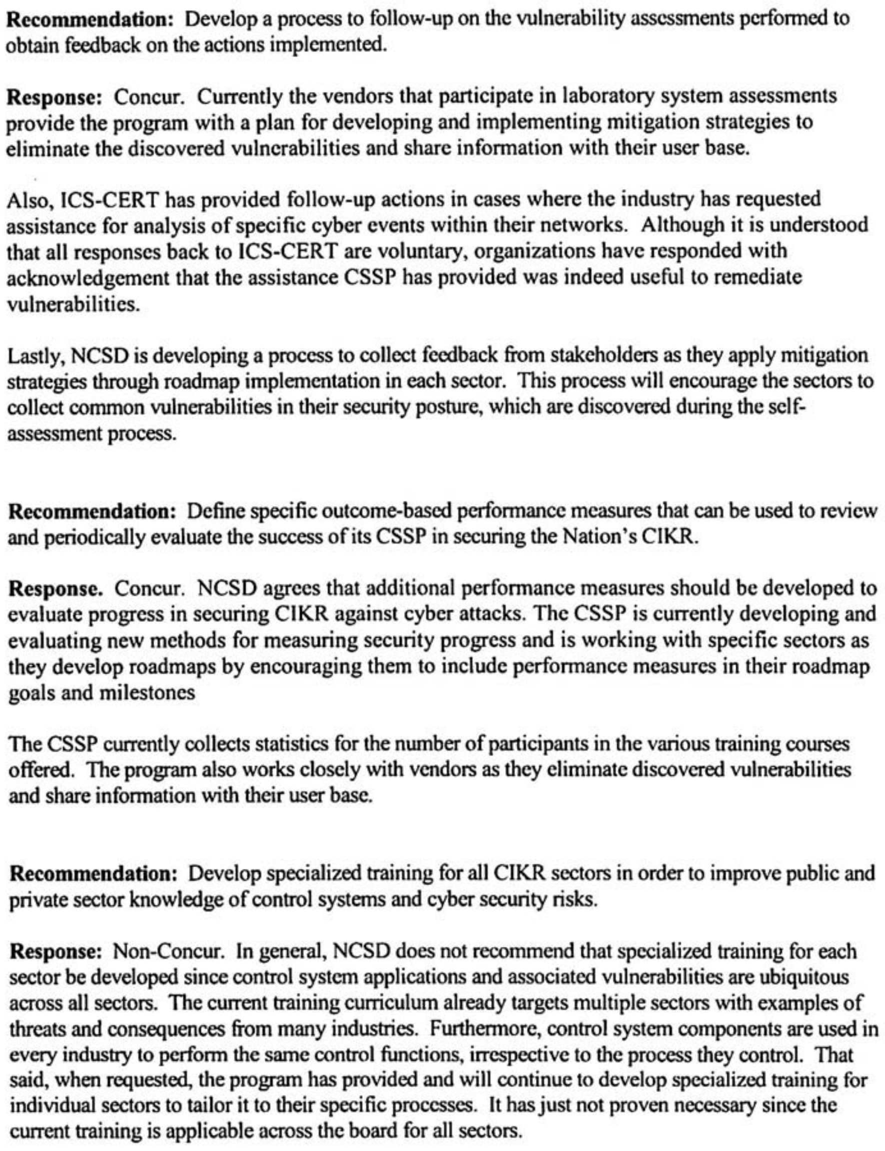
Recommendation: Hold a joint conference where all affected stakeholders can offer or provide remedy in alleviating prohibitions on sharing vulnerability information among control systems owners.

Response: Concur. A subgroup devoted to improving information sharing was formed under the auspices of the ICSJWG to address challenges associated with protecting sensitive and proprietary information. This subgroup, called the Information Sharing Subgroup, has developed a charter and will work with the CIKR community to develop a process for improving cyber security information sharing among control system stakeholders.

Recommendation: Increase the number of on-site assessments performed of the CIKR by:

- Seeking assistance from the Office of Infrastructure Protection via its Protective Security Advisor (PSA) Program to perform cyber assessments self-assessment training when they perform physical security assessments;
- Encouraging the assistance of the SSAs in performing on-site cyber security assessments;
- Leveraging partnerships among the various Federal agencies in performing cyber security assessments; and
- Developing incentive programs to encourage participation.

Response: Concur. The CSSP has planned for 12 on-site assessments in its FY 2009 work scope and agrees that additional assessments should be performed. NCSD works closely with the Office of Infrastructure Protection's regional PSAs to find asset owners in need of on-site assistance. NCSD also supports the Office of Infrastructure Protection with its Regional Resiliency Assessment Program by providing cybersecurity expertise during on-site assessments. NCSD also works with the SSAs through the ICSJWG to identify specific sector needs and provide support in developing and implementing sector roadmaps to secure control systems. NCSD has already scheduled training workshops for the Water sector. This training will include instruction in the use of the self-assessment tools and offers for on-site assessment support.



Recommendation: Develop a process to follow-up on the vulnerability assessments performed to obtain feedback on the actions implemented.

Response: Concur. Currently the vendors that participate in laboratory system assessments provide the program with a plan for developing and implementing mitigation strategies to eliminate the discovered vulnerabilities and share information with their user base.

Also, ICS-CERT has provided follow-up actions in cases where the industry has requested assistance for analysis of specific cyber events within their networks. Although it is understood that all responses back to ICS-CERT are voluntary, organizations have responded with acknowledgement that the assistance CSSP has provided was indeed useful to remediate vulnerabilities.

Lastly, NCSD is developing a process to collect feedback from stakeholders as they apply mitigation strategies through roadmap implementation in each sector. This process will encourage the sectors to collect common vulnerabilities in their security posture, which are discovered during the self-assessment process.

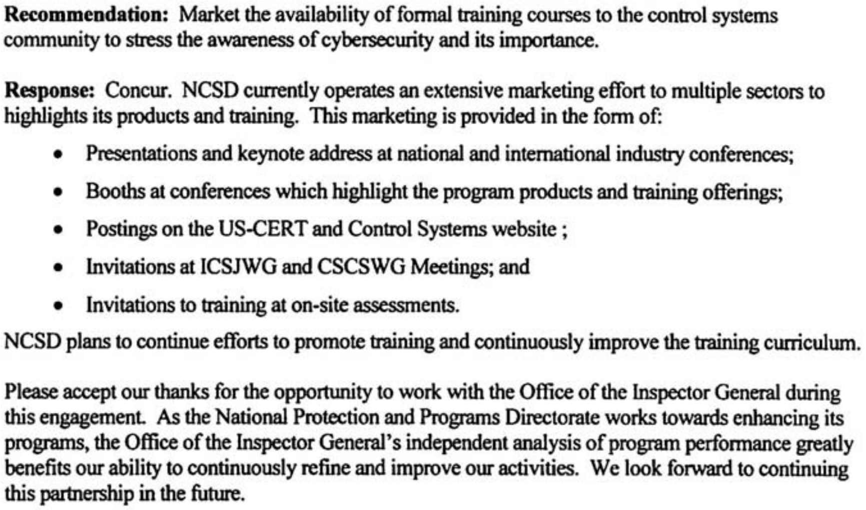
Recommendation: Define specific outcome-based performance measures that can be used to review and periodically evaluate the success of its CSSP in securing the Nation's CIKR.

Response. Concur. NCSD agrees that additional performance measures should be developed to evaluate progress in securing CIKR against cyber attacks. The CSSP is currently developing and evaluating new methods for measuring security progress and is working with specific sectors as they develop roadmaps by encouraging them to include performance measures in their roadmap goals and milestones

The CSSP currently collects statistics for the number of participants in the various training courses offered. The program also works closely with vendors as they eliminate discovered vulnerabilities and share information with their user base.

Recommendation: Develop specialized training for all CIKR sectors in order to improve public and private sector knowledge of control systems and cyber security risks.

Response: Non-Concur. In general, NCSD does not recommend that specialized training for each sector be developed since control system applications and associated vulnerabilities are ubiquitous across all sectors. The current training curriculum already targets multiple sectors with examples of threats and consequences from many industries. Furthermore, control system components are used in every industry to perform the same control functions, irrespective to the process they control. That said, when requested, the program has provided and will continue to develop specialized training for individual sectors to tailor it to their specific processes. It has just not proven necessary since the current training is applicable across the board for all sectors.



Recommendation: Market the availability of formal training courses to the control systems community to stress the awareness of cybersecurity and its importance.

Response: Concur. NCSD currently operates an extensive marketing effort to multiple sectors to highlights its products and training. This marketing is provided in the form of:

- Presentations and keynote address at national and international industry conferences;
- Booths at conferences which highlight the program products and training offerings;
- Postings on the US-CERT and Control Systems website ;
- Invitations at ICSJWG and CSCSWG Meetings; and
- Invitations to training at on-site assessments.

NCSD plans to continue efforts to promote training and continuously improve the training curriculum.

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

Appendix C
Major Contributors to this Report

Information Security Audit Division

Edward G. Coleman, Director
Tarsha Cary, Audit Manager
Pamela Williams, Senior IT Auditor
Charles Twitty, IT Auditor
Amanda Strickler, IT Specialist
Barbara Bartuska, Audit Manager
Matthew Worner, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Deputy Chief of Staff
Executive Secretary
Assistant Secretary, Legislative Affairs
Assistant Secretary, Policy
Assistant Secretary, Public Affairs
General Counsel
Office of Security
Office of Privacy
Assistant Secretary, Cyber Security and Communications
Chief Information Officer (CIO)
Deputy CIO
Chief Information Security Officer
Director, NCSD
Director, Critical Infrastructure Cyber Protection and Awareness, NCSD
Director, Control Systems Security Program, NCSD
Director, US-CERT
Information Systems Security Manager, NPPD
Director, Departmental GAO/OIG Liaison Office
Director, Compliance and Oversight Program
Audit Liaison, NPPD
Audit Liaison, DHS/CISO
Audit Liaison, DHS/CIO
Director, Information Security Audit Division (ISAD)
Audit Manager, ISAD

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Appendix D
Report Distribution

Congress

Appropriate Congressional Oversight and Appropriations Committees

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.