Department of Homeland Security

Office of Inspector General

DHS Can Make Improvements to Secure Industrial Control Systems

OIG-13-39

February 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

February 14, 2013

MEMORANDUM FOR: The Honorable Rand Beers
Under Secretary
National Protection and Programs Directorate

FROM: Charles K. Edwards
Deputy Inspector General

SUBJECT: *DHS Can Make Improvements to Secure Industrial Control Systems*

Attached for your action is our final report, *DHS Can Make Improvements to Secure Industrial Control Systems.* We incorporated your formal comments in the final report.

The report contains two recommendations aimed at improving the security of control systems. Your office concurred with all recommendations. As prescribed by the Department of Homeland Security Directive 077-1, Follow-Up and Resolutions for the Office of Inspector General Report Recommendations, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination."

Please call me with any question, or your staff may contact Frank W. Deffer, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4100.

Attachment

Table of Contents

Appendixes

Abbreviations

CIKR	critical infrastructure and key resources
CIO	Chief Information Officer
CISO	Office of Chief Information Security Office
CSSP	Control Systems Security Program
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
ICS	industrial control systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
INL	Idaho National Laboratory
NPPD	National Protection and Programs Directorate
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
US-CERT	United States Computer Emergency Readiness Team

Executive Summary

We evaluated the progress the Department of Homeland Security (DHS) has made in addressing cybersecurity issues and coordinating the response efforts between the public and private sectors for industrial control systems. Security for industrial control systems has been inherently weak because the systems were not designed to be accessible from external networks or the Internet. However, beginning in 1990, companies began to connect their industrial control systems with enterprise systems that are connected to the Internet. This transition allowed remote control of processes and exposed industrial control systems to cyber security risks that could be exploited over the Internet. The National Cybersecurity and Communications Integration Center, a division of the Office of Cybersecurity and Communications within the National Protection and Programs Directorate (NPPD), is the operational arm of NPPD and is responsible for providing full-time monitoring, information sharing, analysis, and incident response capabilities to protect Federal agencies' networks and critical infrastructure and key resources, such as industrial control systems.

NPPD has strengthened the security of industrial control systems by establishing the Industrial Control Systems Cyber Emergency Response Team to address the need to share critical cybersecurity information, analyze vulnerabilities, verify emerging threats, and disseminate mitigation strategies. NPPD also facilitates cybersecurity information sharing between the public and private sectors through various working groups, issuing alerts and bulletins, and conducting cybersecurity training and conferences regarding industrial control systems.

Although NPPD has made progress in securing control systems, further improvements can be made in information sharing. For example, NPPD needs to consolidate the multiple information sharing communities of interests used to disseminate control system cybersecurity information efficiently and effectively. Additionally, NPPD should provide advance notification of technical and ongoing vulnerability and malware assessments to better coordinate response efforts with the public and private sectors to prevent, detect, and mitigate potential cyber threats.

We are making two recommendations to NPPD to improve its information sharing process and response coordination efforts. NPPD concurred with all recommendations and has begun to take actions to implement them. NPPD's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

Background

Industrial control systems (ICS) are systems that include supervisory control and data acquisition, process control, and distributed control that manage and monitor the Nation's critical infrastructure and key resources (CIKR).[1] ICS are an integral part of our Nation, and help facilitate operations in vital sectors. Security for ICS was inherently weak because the systems were never intended to be accessible from external networks or the Internet. However, beginning in 1990, companies began connecting their operational ICS with enterprise systems that are connected to the Internet. The migration allows asset owners to access new and more efficient methods of communication, as well as more robust data, and gain quicker time to market and interoperability.

Examples of CIKR sectors – Dams, Energy, and Nuclear

This transition allowed remote control of processes and exposed ICS to cyber security risks that could be exploited over the Internet. ICS are increasingly under attack by a variety of malicious sources. These range from hackers looking for attention and notoriety to sophisticated nation-states intent on damaging equipment and facilities,

[1] There are 18 CIKR 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, Information Technology, National Monuments and Icons, Nuclear Reactors, Material and Waste, Postal and Shipping, Transportation Systems, and Water.

disgruntled employees, competitors, and even personnel who inadvertently bring malware into the workplace by inserting an infected flash drive into a computer. A successful cyber attack on ICS may result in physical damage, loss of life, and cascading effects that could disrupt services. A recent survey in the energy sector revealed that a majority of the companies in the sector had experienced cyber attacks, and about 55 percent of these attacks targeted ICS. The cyber attacks involved large-scale denial-of-service and network infiltrations. Successful attacks on ICS can give malicious users direct control of operational systems, creating the potential for large-scale power outages or man-made environmental disasters. Some recent cyber attacks have included the following:

- In February 2011, the media reported that hackers had stolen proprietary information worth millions of dollars from the networks of six energy companies in the United States and Europe.

- In December 2011, a sophisticated threat actor targeted the oil and natural gas subsector. Affected asset owners across the sector voluntarily worked with DHS during the investigation.

- Throughout 2011, there were reports of spear-phishing via email in the Energy sector; no negative impacts occurred to the companies' control processes and operations.

- In March 2012, an alert was issued regarding phone-based social engineering attempts at two or more power distribution companies. The callers attempted to direct the company personnel to take action to correct a problem that would have allowed the attacker to gain access to their ICS.

- In April 2012, media reported that a Canadian ICS manufacturing company inadvertently planted a backdoor login account in its own operating systems, which contain switches and servers used in mission-critical communications networks that operate power grids and railway and traffic control systems. This account could have allowed attackers to access the devices via the Internet.

Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Identification, Prioritization, and Protection directs DHS to produce a comprehensive and integrated national plan to protect CIKR. HSPD-7 also designated DHS as a national focal point for securing cyberspace. To lead this effort, NPPD established the Control Systems Security Program (CSSP). The goal of the CSSP is to guide a cohesive effort between government and industry to reduce the cyber risk on ICS. The CSSP provides guidance and reduces risk to CIKR control systems by

- Implementing the *Strategy to Secure Control Systems* as part of its mission to coordinate and lead efforts to improve control systems security in the Nation's critical infrastructures; and

- Establishing the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) as the operational arm to coordinate with the United States Computer Emergency Readiness Team (US-CERT) to respond to control systems related incidents and promote situational awareness activities on ICS.

ICS-CERT's operational capabilities focus on the private sector CIKR ICS and networks, which is essential to the Department's mission to protect the Nation's critical infrastructure, particularly against emerging cyber threats. Additionally, ICS-CERT uses the Request Tracker Ticketing System to capture analytical and status information regarding vulnerabilities and incidents. The ticketing system maintains the incident response team's remote technical assistance and onsite assessment status and reports. Tickets are color-coded based on age. The ticketing system notifies the assigned personnel when the status of a ticket is changed or further action is needed. Additionally, ICS-CERT coordinates control systems-related security incidents and information sharing with Federal, state, and local agencies and organizations, as well as private sector constituents, including vendors, owners, and operators of ICS.

ICS-CERT exchanges information with stakeholders via the Homeland Security Information Network (HSIN) – Critical Sector. The Office of Chief Information and Officer (OCIO) develops and maintains HSIN and serves as data governance steward for HSIN policy documents, including the HSIN Model Charter and HSIN Terms of Service. Although OCIO is the data steward, the office is not responsible for maintaining the content that users and communities of interest post to any element of HSIN.[2] Each community of interest sponsor is responsible for maintaining and sharing the content within the community of interest and through the community of interest shared space.[3] The administration and governance of the communities of interests, including creation of individual sites within the community, is at the discretion of their sponsors. OCIO works in cooperation with each community of interest to enforce the rules in the charter and terms of services. OCIO conducts regular reviews of communities of

[2] HSIN communities of interest are separate environments wherein users involved in the same subject matter area or industry may post and view potentially relevant news and information and use collaborative tools.

[3] The HSIN shared space allows authorized stakeholders and content contributors to publish finished products and relevant documents that (1) have appropriate markings providing sharing permissions at the document level, and (2) are targeted to an authorized audience based on their credentials and related community of interest and system wide rules for sharing.

interest to validate and justify its purpose, objectives, and operational need. NPPD sponsors and manages the critical sector communities of interests.

Results of Audit

Progress Made in Improving the Security of Industrial Control Systems

NPPD has strengthened the security of ICS by addressing the need to share critical cybersecurity information, analyze vulnerabilities, verify emerging threats, and disseminate mitigation strategies. For example, DHS has taken the following actions to improve ICS security and foster better partnerships between the Federal and private sectors:

- Establishing ICS-CERT Incident Response Team, also known as the fly away teams, to support the public and private sectors through onsite and remote incident response services on a variety of cyber threats, ranging from general malicious code infections to advanced persistent threat intrusions. Additionally, in March 2012, NPPD released the Cyber Security Evaluation Tool Version 4.1. The updated tool assists users in identifying devices connected to their networks, as well as external connections, by creating a diagram of their systems.

- Operating a malware lab that provides testing capabilities to analyze vulnerabilities and malware threats to control system environments. The team verifies vulnerabilities for researchers and vendors, performs impact analysis, and provides patch validation and testing prior to deployment to the asset-owner community.

- Improving the quality of its alerts and bulletins by including actionable information regarding vulnerabilities and recommended mitigations and best practices for securing ICS.

- Providing products to the ICS community on a daily, weekly, monthly, quarterly, and as-needed basis, through email, website, and portal postings. These products help ICS-CERT to improve the situational awareness of ICS and provide status updates of its working groups, articles of interest, and upcoming events and training.

- Implementing a virtual private network solution to allow CSSP program officials to access program applications and systems (e.g., the ICS-CERT ticketing system) located at the Idaho National Laboratory (INL).[4]

- Assisting in developing various roadmaps for the cross-sector, dams, nuclear, water, and transportation. The roadmaps provide vision and framework for mitigating cybersecurity risk to the wide variety of systems critical to each sector's operations.

NPPD has strengthened its outreach efforts with the ICS community, including vendors, owners/operators, academia, and other Federal agencies. These efforts include participating in the monthly Cross-Sector Cyber Security Working Group meetings; Government Coordinating Council and Sector Coordinating Council meetings; monthly Electricity subsector teleconference, quarterly Oil and Natural Gas subsector conference, and monthly Nuclear sector teleconferences; and Industrial Control Systems Joint Working Group and its subgroup meetings. Finally, the awareness of CSSP and ICS-CERT has increased with ICS-CERT's participation at various sector conferences, such as the cross-sector International Society of Automation in October 2011, American Petroleum Institute Conference in November 2011, Dams Sector Federal Energy Regulatory Commission Security Review and Training Course in December 2011, Nuclear Energy Institute Cyber Security Implementation Workshop in February 2012, and Southwest Power Pool Critical Infrastructure Protection Workshop in May 2012.

Despite these actions, NPPD still faces challenges in reducing the cybersecurity risks for the Nation's ICS. Further, NPPD can improve its efforts to protect and secure control systems that are essential to the Nation's security and economy.

Better Information Sharing and Communication Can Enhance Coordination Efforts With the Public

ICS-CERT needs to improve its information sharing and communication efforts with Sector Specific Agencies and the private sector to ensure that these stakeholders are provided with potential ICS threats and vulnerabilities to mitigate security threats timely. Specifically, NPPD has implemented multiple information sharing communities of interest, which, according to the private sector, leads to confusion among its stakeholders and hinders its efforts to share cyber threat information on ICS. In addition, DHS needs to improve communications with Sector Specific Agencies and the

[4] A virtual private network is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. Users can access resources on remote networks, such as files, printers, databases, or internal websites.

private sector by providing advanced notification of ICS-CERT's remote technical and onsite incident assessments.

Consolidation of Multiple Information Sharing Communities of Interest

DHS does not have a consolidated summary overview page on the HSIN-Critical Sectors that highlights new information and activities to ensure that ICS cybersecurity information is shared effectively. Many of the private sector partners we interviewed (e.g., owners/operators, regulators, and working groups) use the HSIN, ICS-CERT, and US-CERT portals to retrieve advisories, vulnerability information, and best practices. The HSIN-Critical Sectors communities of interest are designed to encourage communication and collaboration among all CIKR sectors and the Federal Government based on a different community of interest. Currently, there are 55 communities of interests on HSIN-Critical Sectors. The content is tailored for each of the CIKR sectors and must be searched individually for pertinent and updated information. For example, the Dams, Emergency Management, and Electricity and Oil and Natural Gas subsector communities of interest, which are used by companies that belong to multiple sectors, have to be searched individually and may contain non-cybersecurity information, such as physical security, emergency response, and planning. These searches can be time-consuming for the stakeholders.

Additionally, each community of interest is arranged differently, making it more cumbersome for the users to retrieve useful information. For example, some HSIN users told us that the communities of interest contain a lot of duplicate information from a variety of sources and it is a challenge to get useful information from these communities of interest. As a result, some Sector Specific Agencies want to build additional portals for their stakeholders to streamline the information DHS provides.

ICS-CERT officials acknowledged that existing communities of interest could confuse owners/operators. To eliminate duplicate information from the communities of interest, ICS-CERT created the Improve Communications Subcommittee within the Industrial Control Systems Joint Working Group to address stakeholder concerns regarding the communities of interests. ICS-CERT officials said that ICS-CERT only contributed contents to the communities of interest and did not determine how these sites were set up. However, NPPD plans discussions with OCIO to determine whether these communities of interest could be consolidated to better serve stakeholder needs.

Advance Notification of Remote Technical and Onsite Assessments

DHS does not communicate the results of its remote technical and onsite assessments to the public timely. We interviewed officials from three Sector Specific Agencies, six government and private sector councils, and 23 private companies from the dams, energy, and nuclear sectors to evaluate whether ICS-CERT shared sufficient information and communicated effectively. Overall, these officials acknowledged that DHS had improved the quality of alerts and bulletins that addressed various cyber topics. However, they expressed concerns regarding the timeliness of ICS-CERT's information sharing and communications. As a result, the stakeholders perceived that a great deal of time might have elapsed until stakeholders were made aware of the same or similar incident that could affect their systems.

All the Sector Specific Agencies senior officials expressed a need to be notified in advance when ICS-CERT is performing onsite or remote technical assistance assessments with private companies within their sectors. For example, these officials suggested that ICS-CERT publish a "heads-up" or "quick anonymous" informational alert regarding an ongoing investigative/pending event, sectors and devices affected, and whether a potential fix exists. The Sector Specific Agencies believe that such notifications would be helpful and would allow them to react more appropriately if other companies call them with questions. For example, according to Nuclear Sector Specific Agency officials, the Department's Domestic Nuclear Detection Office sends an email alert to state authorities and its offices regarding upcoming site visits.[5]

Additionally, both Sector Specific Agencies and private sector officials said that an advance notification would be helpful to increase dialogue with ICS-CERT on an event or threat that has not been made public. The private sector officials suggested that advance notification can allow them to assist ICS-CERT in developing solutions and mitigating strategies as well as determining whether an incident is isolated or systemic.

ICS-CERT management acknowledged the Sector Specific Agencies', councils', and private sector's concerns regarding the sharing of active incidents and

[5] The Domestic Nuclear Detection Office (DNDO) is the primary U.S. government entity for implementing domestic nuclear detection efforts for a managed and coordinated response to radiological and nuclear threats, as well as integration of Federal nuclear forensics programs. Additionally, DNDO is charged with coordinating the development of the global nuclear detection and reporting architecture, with partners from Federal, state, local, and international governments and the private sector.

threats, such as identified cyber intrusions and spear-phishing emails. Additionally, ICS-CERT management told us that the private sector perceives that ICS-CERT has more useful information available than it is willing to share. However, ICS-CERT management said that proprietary information and ongoing law enforcement investigations limit the amount of information ICS-CERT can disseminate. For example, there were instances in which the Federal Bureau of Investigation was engaged in an ongoing investigation and had withheld sensitive law enforcement information. Additionally, the protected critical infrastructure information between DHS and the private sector owner prohibits ICS-CERT from sharing vulnerability and malware assessment information.

Recommendations

We recommend that the Undersecretary, NPPD:

Recommendation #1:

Collaborate with OCIO to streamline the HSIN portal to ensure that ICS cyber information is shared effectively.

Recommendation #2:

Promote collaboration with Sector Specific Agencies and private sector owners/operators by communicating preliminary technical and onsite assessment results to address and mitigate potential security threats on ICS.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Under Secretary, NPPD. We have included a copy of the comments in its entirety at appendix B. We also obtained technical comments to the draft report, which we incorporated into the final report where appropriate.

NPPD concurred with recommendation 1. In the comments, the Under Secretary stated that NPPD will collaborate with the DHS OCIO to ensure that ICS cyber information is shared effectively in the HSIN portal. Currently, OCIO is planning to deploy "HSIN Release 3 Shared Space," which will allow NPPD to share ICS and other information in one shared space on the portal. The Under Secretary also stated that it must be recognized that the HSIN portal supports multiple communities of interests, composed of DHS stakeholders who share an interest in similar types of information. ICS and other programs often tailor the

information posted to these communities of interest so that it is relevant to the stakeholder recipients' interests. According to the Under Secretary, a central ICS repository on HSIN will ensure that all ICS information can be found in one location. The Under Secretary stated as well that it is important to preserve the ability to post tailored information to communities of interest since critical infrastructure owners have expressed an interest in this distribution method. "HSIN Release 3 Shared Space" will enable both methods of information sharing.

We agree that the steps that NPPD has taken and plans to take begin to satisfy this recommendation. This recommendation will remain open until NPPD provides documentation to support that all planned corrective actions are completed.

NPPD concurred with recommendation 2. The Under Secretary stated in the comments that NPPD will continue its strong promotion of increased information sharing and collaboration with both Sector Specific Agencies and the private sector. This collaboration includes increased awareness and use of the Protected Critical Infrastructure Information program. In addition, the Under Secretary indicated that NPPD's Office of Cybersecurity and Communications will collaborate with NPPD's Office of Infrastructure Protection Protected Critical Infrastructure Information program office on the best approach to enhance collaboration and communication with Sector Specific Agencies and private sector partners regarding security threats to ICS.

Appendix A
Objectives, Scope, and Methodology

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.

The objective of our audit was to evaluate the progress DHS has made in addressing cybersecurity issues and coordinating the response efforts for control systems between the public and private sectors. Specifically, we determined whether NPPD/ICS-CERT is:

- Effectively coordinating the response on security incidents related to control systems.

- Conducting vulnerability and malware analyses to reduce security risks on control systems.

- Coordinating and sharing vulnerability information and threat analyses through information products, alerts, and adequate disclosure.

Our audit focused on NPPD's program for control system security for compliance with applicable requirements outlined in HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection* (December 2003), the *National Infrastructure Protection Plan* (February 2009), *Cyberspace Policy Review* (2009), *Strategy for Securing Control Systems* (October 2009) and National Institute of Standards and Technology Special Publication 800-82, *Guide to Industrial Control System Security* (June 2011).

We interviewed selected officials from NPPD and Office of Infrastructure Protection management, as well as INL personnel. Further, we interviewed selected personnel from various sectors, including Dams, Energy, and Nuclear Reactors, Materials and Waste to obtain feedback regarding NPPD's communication and information sharing, vulnerability assessments, and cybersecurity concerns.

We conducted our work at the program level and visited the INL. Additionally, we visited selected private sector companies in Alabama, Maryland, North Carolina, and Pennsylvania, and conducted a number of teleconferences with companies in the Dams, Energy, and Nuclear Reactors, Materials and Waste sectors.

We conducted this performance audit between May and November 2012 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, Office of Information Technology Audits, at (202) 254-4100.

Appendix B
Management Comments to the Draft Report

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

Homeland Security

JAN 23 2013

Mr. Charles K. Edwards
Acting Inspector General
Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Edwards:

Re: Office of Inspector General Report, DHS Can Make Improvements to Secure Industrial Control Systems (OIG Project No. 12-136-ITA-NPPD)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the OIG's work in planning and conducting its review and issuing this report.

The National Protection and Programs Directorate (NPPD) is pleased to note OIG's recognition of the actions taken to improve the Industrial Control Systems (ICS) security and foster better partnerships between the Federal and private sectors. In particular, the Industrial Control Systems Cyber Emergency Response Team has made significant progress in increasing the timeliness of actionable mitigation information shared with all stakeholders, both government (Federal, state, local and tribal) and the private sector.

Technical comments have been provided under separate cover. Following are our detailed responses to the two OIG recommendations made in the draft report.

Recommendation 1: The Under Secretary of NPPD collaborate with the Office of the Chief Information Officer (OCIO) to streamline the Homeland Security Information Network (HSIN) portal to ensure that ICS cyber information is shared effectively.

Response: Concur. NPPD will collaborate with the DHS OCIO to ensure that ICS cyber information is shared effectively in the HSIN portal. Currently, OCIO is planning to deploy "HSIN Release 3 Shared Space," which will allow NPPD to share ICS and other information in one shared space on the portal. It must be recognized that the HSIN portal supports multiple Communities of Interest (COIs), composed of DHS stakeholders who share an interest in similar types of information. ICS and other programs often tailor the information posted to these COIs so that it is relevant to the stakeholder recipients' interests. A central ICS repository on HSIN will ensure that all ICS information can be found in one location. However, it is important to preserve the ability to post tailored information to COIs since critical infrastructure owners have

expressed an interest in this distribution method. "HSIN Release 3 Shared Space" will enable both methods of information sharing.

Recommendation 2: The Under Secretary of NPPD promote collaboration with Sector Specific Agencies and private sector owners/operators by communicating preliminary technical and onsite assessment results to address and mitigate potential security threats on ICS.

Response: Concur. NPPD will continue its strong promotion of increased information sharing and collaboration with both Sector-Specific Agencies (SSA) and with the private sector. This collaboration includes increased awareness and use of the Protected Critical Infrastructure Information (PCII) program. NPPD's Office of Cybersecurity and Communications will collaborate with NPPD's Office of Infrastructure Protection PCII program office on the best approach to enhance collaboration and communication with SSAs and private sector partners regarding security threats on ICS.

We look forward to working with you on future homeland security engagements.

Sincerely,

Rand Beers
Under Secretary

Appendix C
Major Contributors to This Report

Chiu-Tong Tsang, Director
Tarsha Cary, IT Audit Manager
Shannon Frenyea, Senior Program Analyst
Megan Ryno, Program Analyst
Anna Hamlin, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
Acting General Counsel
Executive Secretary
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
Assistant Secretary, Cyber Security and Communications
Chief Information Officer (CIO)
Deputy CIO
Chief Information Security Officer
Director, National Cybersecurity and Communications Integration Center
Director, ICS-CERT
Director, Critical Infrastructure Cyber Protection and Awareness, NPPD
Director, US-CERT
Director, Department GAO/OIG Liaison Office
Director, Compliance and Oversight Program, Office of Chief Information Security Office (CISO)
Audit Liaison, NPPD
Audit Liaison, DHS/CISO
Audit Liaison, DHS/CIO
Acting Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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