

Department of Homeland Security **Office of Inspector General**

Implementation Status of the Enhanced Cybersecurity Services Program






OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

July 29, 2014

MEMORANDUM FOR: Andy Ozment
Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate

FROM: 
Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Implementation Status of the Enhanced Cybersecurity Services Program*

Attached for your information is our final report, *Implementation Status of the Enhanced Cybersecurity Services Program*. We incorporated your comments in the final report.

The report contains three recommendations aimed at improving the effectiveness of the Enhanced Cybersecurity Services program. The National Protection and Programs Directorate concurred with all recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for 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.

Based on information provided in your response to the draft report, we consider recommendations #1 and #2 open and resolved. Recommendation #3 is closed and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

the report on our website for public dissemination. Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Attachment



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Executive Summary	1
Background	2
Results of Audit.....	5
Progress Made in Expanding the ECS Program.....	5
Further Enhancement Needed To Expand the ECS Program.....	6
Recommendations	8
Management Comments and OIG Analysis	9

Appendixes

Appendix A: Objectives, Scope, and Methodology.....	12
Appendix B: Management Comments to the Draft Report.....	13
Appendix C: Major Contributors to This Report	17
Appendix D: Report Distribution.....	18

Abbreviations

CS&C	Cybersecurity and Communications
CSP	commercial service provider
DHS	Department of Homeland Security
ECS	Enhanced Cybersecurity Services
FY	fiscal year
OI	operational implementer
OIG	Office of Inspector General
NPPD	National Protection and Programs Directorate
US-CERT	United States Computer Emergency Readiness Team



Executive Summary

In February 2013, in an effort to strengthen the Nation’s critical infrastructure, the President directed the Department of Homeland Security (DHS), in collaboration with the Secretary of Defense, to expand the Enhanced Cybersecurity Services program to all 16 critical infrastructure sectors. The Enhanced Cybersecurity Services program is a voluntary information sharing initiative in which DHS shares both unclassified and classified indicators of malicious cyber activity with critical infrastructure sector participants.

The National Protection Programs Directorate (NPPD) is primarily responsible for fulfilling the DHS national, non-law enforcement cybersecurity missions. Within NPPD, the Office of Cybersecurity and Communications is responsible for the implementation of the Enhanced Cybersecurity Services program. Our overall objective was to determine the effectiveness of the Enhanced Cybersecurity Services program to disseminate cyber threat and technical information with the critical infrastructure sectors through commercial service providers.

NPPD has made progress in expanding the Enhanced Cybersecurity Services program. For example, as of May 2014, 40 critical infrastructure entities participate in the program. Additionally, 22 companies have signed memorandums of agreement to join the program. Further, NPPD has established the procedures and guidance required to carry out key tasks and operational aspects of the program, including an in-depth security validation and accreditation process. NPPD has also addressed the privacy risk associated with the program by developing a Privacy Impact Assessment. Finally, NPPD has engaged sector-specific agencies and government furnished information providers to expand the program, and has developed program reporting and metric capabilities to monitor the program.

Although NPPD has made progress, the Enhanced Cybersecurity Services program has been slow to expand because of limited outreach and resources. In addition, cyber threat information sharing relies on NPPD’s manual reviews and analysis, which has led to inconsistent cyber threat indicator quality.

We are making three recommendations to NPPD to help expand the implementation of the Enhanced Cybersecurity Services program. 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

The prevalence of cyber attacks—including attempts to gain unauthorized access to information systems or sensitive data stored and processed by these systems—has triggered an expansion of cybersecurity initiatives in the government and private sector. The President has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation. In May 2012, the Department of Defense and DHS established a pilot program to enhance the resiliency of defense industrial base critical infrastructure entities by sharing cyber threat information with participating Defense Industrial Base companies.

In an effort to strengthen the Nation’s critical infrastructure, in February 2013 the President signed Executive Order 13636, which, in part, directed DHS, in collaboration with the Secretary of Defense, to expand the pilot program to all 16 critical infrastructure sectors (listed in figure 1).¹ This program is now known as the Enhanced Cybersecurity Services (ECS) program.

Figure 1. Designated Critical Infrastructure Sectors

Chemical	Financial Services
Commercial Facilities	Food and Agriculture
Communications	Government Facilities
Critical Manufacturing	Healthcare and Public Health
Dams	Information Technology
Defense Industrial Base	Nuclear Reactors
Emergency Services	Materials, Waste, and Transportation Systems
Energy	Water and Wastewater Systems

Source: DHS

The goal of Executive Order 13636 is to strengthen the cybersecurity of critical infrastructure by increasing the volume and timeliness, as well as improve the quality of, cyber threat information shared between the Federal Government and private sectors.

ECS is a voluntary program between DHS and participating commercial service providers (CSPs) and operational implementers (OIs) to share unclassified, sensitive, and classified indicators of malicious cyber activity.² In return, CSPs use this information to protect

¹ Executive Order 13636 - *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.

² An indicator is information that can be used to identify malicious cyber activity, such as Internet protocol addresses, domains, email headers, and files.

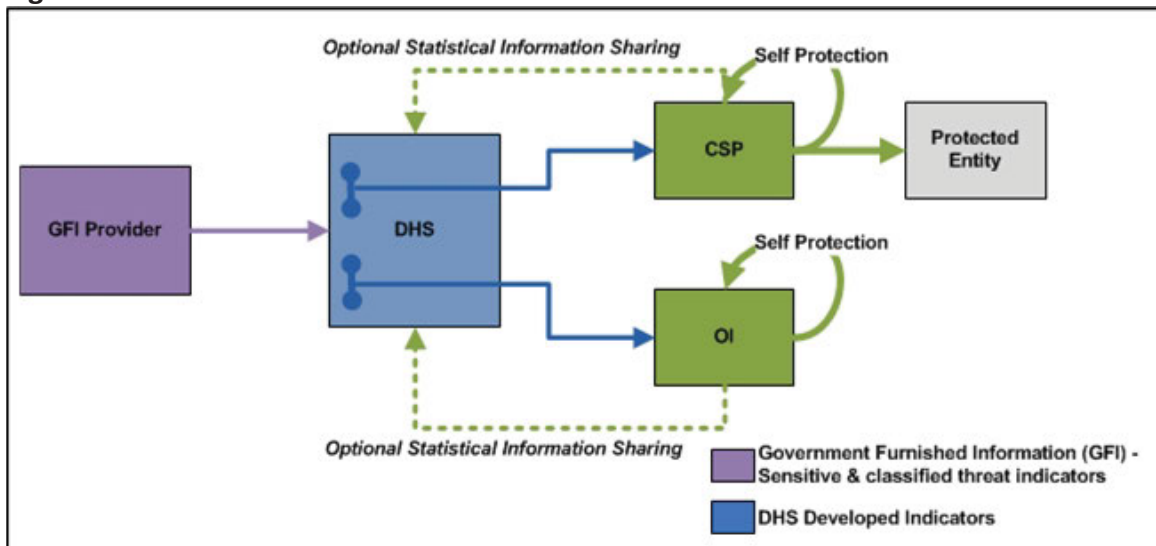


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

critical infrastructure entities through commercial relationships, while OIs use this information to protect their own networks.³ For example, indicators provided through the ECS program can alert CSPs to scan and quarantine email for malicious attachments and code prior to delivering these messages to critical infrastructure end-users. The ECS program requires the collaboration of DHS components. In addition, ECS includes partnerships with Federal critical infrastructure sector-specific agencies and government furnished information providers, who supply the cyber threat indicators and technical information. Figure 2 depicts the information data flow from the government furnished information provider to the protected entity or OI.

Figure 2. ECS Data Flow



Source: NPPD

NPPD is primarily responsible for fulfilling the DHS national, non-law enforcement cybersecurity missions. Through the Office of Cybersecurity and Communications (CS&C), a subcomponent of NPPD, the Department provides crisis management, incident response, and defense capabilities for the Nation's cyber and communication infrastructure. CS&C is primarily responsible for implementing the ECS program. The ECS program has three functional areas—program, security, and operations—that are managed by three different divisions within CS&C. The following are the roles each division plays in support of the ECS program:

³ A CSP is identified as a public or private company that receives threat information from DHS and uses it to offer specified services to critical infrastructure customers in a secure environment. OIs are qualified critical infrastructure entities that use cyber threat information from DHS to protect their internal network only. All CSP security and information safeguarding requirements apply to OIs.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- The Network Security Deployment Division ensures that each CSP and OI meets operational and technical security requirements prior to sharing cyber threat indicators. Specifically, the Network Security Deployment Division oversees the security function of the ECS program and conducts security validation and accreditation for potential CSPs and OIs.⁴ In partnership with the DHS Chief Information Officer, the Network Security Deployment Division has developed a process to facilitate compliance for those CSPs and OIs that do not meet the required classified processing environment and personnel security requirements. The DHS Security Office provides physical and contractor security development assistance.
- The ECS Program Management Office, which is part of CS&C's Stakeholder Engagement and Cyber Infrastructure Resilience division, is responsible for the oversight of the program. For example, the Program Management Office manages CSP and OI involvement and engagement in the program, such as the establishment of eligibility requirements and development of memorandums of agreement required to participate in the program. The Program Management Office also validates whether a private entity is recognized as critical infrastructure prior to enrolling the entity into the program. Finally, the Program Management Office is responsible for coordinating with sector-specific agencies and government furnished information providers to expand the ECS program's coverage and capabilities.
- The National Cybersecurity and Communications Integration Center division's United States Computer Emergency Readiness Team (US-CERT) is responsible for the operational aspect of ECS, including the review of all cyber threat indicators obtained from government furnished information providers for operational relevance and privacy data. US-CERT provides CSPs and OIs with approved cyber threat indicators over classified communication only after the Network Security Deployment Division and DHS Office of Security grant security validation and accreditation to CSPs and OIs.

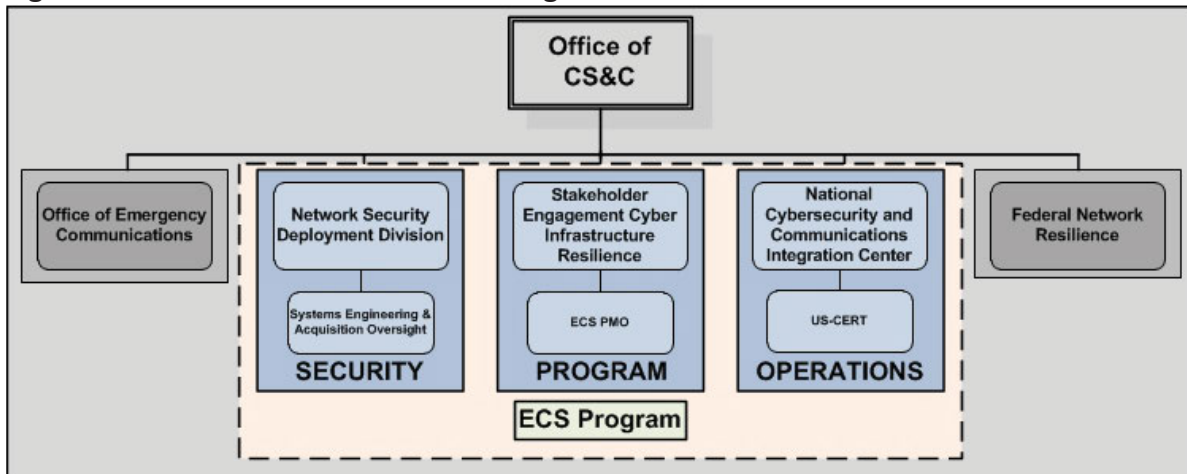
Figure 3 depicts CS&C's organizational chart and the three primary divisions that implement the three functional aspects of the program.

⁴ The security validation and accreditation process includes facility and personnel security clearance vetting, system engineering and architecture assessment, and risk acceptance.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Figure 3. Functional Areas of the ECS Program



Source: OIG diagram based on documentation review and interviews with NPPD personnel

Results of Audit

Progress Made in Expanding the ECS Program

CS&C has made progress in expanding the ECS program to protect critical infrastructure assets by sharing and disseminating cyber threat and technical information with CSPs. Specifically, CS&C has taken the following actions:

- enlisted 40 critical infrastructure entities to participate in the program;
- established memorandums of agreement with 22 critical infrastructure entities to become a CSP or OI, as of May 2013. In addition, 60 organizations have expressed interest in participating in the ECS program;
- developed standard operating procedures required to carry out the key tasks and operational aspects of the program. Specifically, the Program Management Office has issued guidance on government furnished information and sector-specific agency engagement, communication and coordination with ECS stakeholders, and program reporting and metrics;
- increased the frequency of weekly cyber threat data feeds (i.e., indicators) to participating CSPs from two to three times per week;



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- addressed the privacy risk that may be associated with the program and the protection of personally identifiable information by developing the Privacy Impact Assessment for the ECS program;
- developed, in conjunction with the Offices of Intelligence & Analysis and Chief Information Officer and the National Security Agency, an in-depth security validation and accreditation process, for potential and active ECS program participants;
- conducted monthly status meetings with sector-specific agencies to update them on the progress made implementing the ECS program; and
- developed the ECS Five Year Plan – Fiscal Year (FY) 2016–FY 2020. The five year plan identifies several long-term programmatic aspects of the ECS program, including workload projections, resources requirements, and long-term performance goals.⁵

Further Enhancement Needed To Expand the ECS Program

Although CS&C has made progress, enrollment in the ECS program has been slow because of limited communication and outreach and a necessary in-depth security validation and accreditation process for potential program participants. Further, the lack of analysis and manual reviews has affected the quality of cyber threat information provided to CSP participants.

Enrollment in the ECS Program Has Been Slow

As of March 2014, entities from only 3 of the 16 critical infrastructure sectors (defense industrial base, energy, and communication services) were receiving ECS program services. Further, CS&C has only two operational CSP participants and has not enrolled an additional CSP or OI since DHS assumed program responsibility from the Department of Defense in February 2013.

CS&C has promoted the ECS program through media requests, public testimony, and the DHS website. However, CS&C has not communicated with critical infrastructure entities to inform them of the benefits of participating in the ECS program. Through the ECS program, DHS provides cyber threat indicators to CSPs which, in return, use this information to protect critical infrastructure entities.

⁵ *Enhanced Cybersecurity Services Program Five Year Plan – FY 2016 – FY 2020*, March 21, 2014.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Consequently, DHS does not directly communicate with critical infrastructure entities, primarily relying on CSPs to promote their protective services to critical infrastructure sector agencies and operators.

Two CSPs indicated that the Program Management Office can improve its outreach efforts to prospective entities. Specifically, participating CSPs believe it would be beneficial for CS&C to take additional steps to promote the program to expand participation in ECS. For example, the Program Management Office could increase the awareness of the ECS program through the use of websites, issuance of press releases, and information sharing and analysis centers.

As of March 2014, the Program Management Office had established memorandums of agreement with 22 potential CSPs and OIs that are interested in joining the ECS program. While many potential CSPs and OIs are currently in various stages of the security validation and accreditation process, most do not possess the required security capabilities to enroll in the program. Further, CS&C has only completed the security validation and accreditation process for one CSP. According to Network Security Deployment Division personnel, the entire security eligibility and vetting process can take 8 months to complete, depending on the level of security maturity of the potential CSP or OI and CS&C available resources.

DHS is required to expand the ECS program to all critical infrastructure sectors to protect their systems and networks from unauthorized access, exploitation, or destruction. According to the Program Management Office's ECS Program Strategic Initiatives, the ECS program should include all 16 critical infrastructure sectors by increasing the number of operational CSPs that provide ECS services.

Increased CSP and OI enrollment is vital to the success and effectiveness of the ECS program. Without improving communication and outreach to increase critical infrastructure sector entities' interest, CSPs may not have the financial means or incentive to participate in the ECS program due to the lack of new critical infrastructure entity customers. Further, with growing interest in the ECS program, CS&C needs sufficient resources and capacity to perform security assessments and accreditations to ensure that potential CSPs and OIs meet security requirements.

Automated System Is Needed To Improve Cyber Indicators

CS&C can further improve the quality of cyber threat indicators. While CS&C provides an average of 50 to 60 cyber threat indicators to CSPs 3 times a week,



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

one CSP stated that some of the information was inconsistent and not exclusive to the ECS program. Specifically, some of the threat indicators provided were redundant, formatting was not standardized, and a majority of the information provided was unclassified and available through other sources.

While US-CERT serves as an intermediary between government-furnished information providers and CSPs and OIs, US-CERT does not have an automated system to process and analyze classified cybersecurity threat indicators. As a result, US-CERT analysts must manually review and manage all cyber threat and technical information. According to US-CERT personnel, an automated system to manage and process both sensitive and classified threat indicators would improve the efficiency of the program by reducing the amount of time needed to conduct manual reviews and allow for further analysis. In addition, US-CERT does not have the capabilities to validate the accuracy of the indicators provided and determine whether they are unique to the ECS program.

Executive Order 13636 expresses the U.S. Government policy to increase in the volume, timeliness, and quality of cyber threat information shared with private sector entities so that these entities may better protect and defend themselves against cyber threats. In addition, the *National Strategy for Information Sharing and Safeguarding* (December 2012), establishes the need for information sharing processes and sector-specific protocols with the private sector to improve information quality and timeliness.

The success of the ECS program is dependent on CS&C's ability to provide critical infrastructure entities with reliable and specialized cyber threat information. Without an automated system to aggregate and analyze threat indicators expediently, resource-heavy manual reviews will persist. Finally, CS&C will not be able to accurately gauge the effectiveness of each indicator and the program without a system to accurately track and manage ECS provided data.

Recommendations

We recommend that the Assistant Secretary, Office of Cybersecurity and Communications:

Recommendation #1:

Ensure sufficient resources are available for the timely completion of the security validation and accreditation process for CSPs and OIs.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation #2:

Improve the ECS program's outreach efforts across all 16 critical infrastructure sectors, including service providers.

Recommendation #3:

Develop a system to manage and analyze both sensitive and classified cyber threat indicators for the ECS program.

Management Comments and OIG Analysis

Recommendation #1

NPPD concurred with recommendation 1. The Assistant Secretary of CS&C stated that ensuring the success of the ECS program is one of DHS' top priorities. Further, the interest in critical infrastructure entities to become a CSP or an OI exceeded the Department's expectations. For example, as of May 2014, DHS entered into 22 memorandums of agreement with critical infrastructure entities interested in becoming a CSP or an OI. To address this increase in interest, CS&C has allocated additional resources to support the CSP/OI growth and has requested more resources to support the out-years.

It is also important to highlight that the Federal Government—through DHS—is sharing Government Furnished Information that may be classified up to the Top Secret Sensitive Compartmented Information to qualified CSPs/OIs. The classification of the information and purpose of the system dictates an intensive security process. This combined with the various CSP architectures creates a highly involved, yet cooperative process, between the CSP/OI and DHS.

CS&C has a highly qualified staff of security experts to support the security validation and accreditation process; however, the limited number of experts restricts the number of assessment activities that can be accomplished at one time. To address this limitation, CS&C brought in additional Federally Funded Research & Development Center security experts to support the security validation and accreditation process. In addition, CS&C is actively recruiting additional government resources with the required security expertise to augment the current government staff. Finally, CS&C is in the process of awarding a contract for security engineering services to provide support for additional security assessments. These measures will significantly increase the number of assessment activities that can be accomplished at one time, resulting



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

in the timely completion of the security validation and accreditation process for CSPs and OIs.

Additional Federally Funded Research & Development Center resources were added to the program as of June 1, 2014. DHS has identified several FY 2014 and FY 2015 open positions against which to recruit for security experts. The NPPD CS&C Security Engineering Services contract is planned to be awarded by December 2014.

We agree that the steps CS&C is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until CS&C provides supporting documentation that all planned corrective actions are completed.

Recommendation #2

NPPD concurred with recommendation 2. The Assistant Secretary of CS&C stated that the DHS launched the Critical Infrastructure Cyber Community Voluntary Program in February 2014, and NPPD is conducting extensive outreach and communication activities with critical infrastructure owners and operators all over the country interested in improving their cyber risk management processes. ECS is a major component within this voluntary program under the "Resources to Protect" and "Resources to Detect" Cybersecurity Framework Function Areas. Since the launch, DHS has delivered over 100 briefings and eight webinars that have informed over thousands of potential ECS critical infrastructure customers. The Critical Infrastructure Cyber Community Voluntary Program site has had nearly 18,000 visitors.

Additionally, CS&C's ECS Program Management Office is supplementing the strategic ECS program communication plan by drafting a targeted ECS outreach strategy. This strategy will build on DHS' approach of closely partnering with the CSPs by further promoting the benefits of the ECS program to critical infrastructure entities in all 16 critical infrastructure sectors. In addition, the strategy will highlight benefits that the ECS program may provide critical infrastructure entities through the value of the sensitive and classified federal government data and approved ECS services which use this data—via approved CSPs. A final ECS Outreach Strategy will be completed by October 2014.

We agree that the steps CS&C is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

CS&C provides supporting documentation that all planned corrective actions are completed.

Recommendation #3

CS&C concurred with recommendation 3. The Assistant Secretary of CS&C stated that this recommendation should be closed as implemented since NPPD CS&C has already deployed an instance of the Cyber Indicator Analysis Platform to the Top Secret Mission Operating Environment network to support NPPD CS&C's cyber intrusion prevention capabilities. The Top Secret instance of the Cyber Indicator Analysis Platform provides CS&C's National Cybersecurity and Communications Integration Center US-CERT the capabilities needed to manage and analyze sensitive and classified cyber threat indicators for the ECS program. This web application allows analysts to create, update, search, import, export, and assign relationships between indicators and sightings. We note that NPPD CS&C reliance on individuals in some portions of the analysis and sharing process functions as a privacy and civil liberties safeguard, to ensure that threat information and countermeasures shared with CSPs are appropriate, calculated to assist them in the detection of malware and other exploits while not impairing lawful communications.

The installation and accreditation of the Cyber Indicator Analysis Platform, capable of managing both sensitive and classified cyber threat indicators, was completed on May 16, 2014. NPPD CS&C will provide evidence to the OIG under a separate cover.

CS&C personnel provided us with documentation supporting the approval of the Cyber Indicator Analysis Platform to process both unclassified and classified cyber threat indicators. The documentation provided satisfies the intent of this recommendation. We consider this recommendation closed and resolved.



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 determine the effectiveness of the NPPD ECS program to disseminate cyber threat and technical information with the critical infrastructure sector through commercial service providers. Specifically, we determined whether NPPD CS&C (1) has made progress in implementing the ECS program to all critical infrastructure sectors; (2) shares and disseminates effective cybersecurity information with ECS stakeholders, including owners and operators of critical infrastructure; and (3) ensures the protection of classified and personally identifiable information that is transmitted and received through the ECS program.

Our audit focused on the requirements outlined in Executive Order 13636 (February 2013) and other applicable criteria. Specifically, we used the *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (December 2003), *Comprehensive National Cybersecurity Initiative* (January 2008), and the *Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience* (February 2013), as well as other guidance published by the National Institute of Standards and Technology.

We interviewed selected officials within NPPD, including CS&C personnel, as well as representatives from CSPs and personnel from other Federal agencies. In addition, we reviewed and evaluated CS&C security policies, standard operating procedures, training requirements, and other appropriate documentation as necessary. We performed fieldwork at the program level in the Washington, DC, area.

We conducted this performance audit between November 2013 and March 2014 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.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B Management Comments to the Draft Report

*Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528*



**Homeland
Security**

July 2, 2014

Mr. Richard Harsche
Acting Assistant Inspector General
Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Harsche:

Re: Office of Inspector General Report "Implementation Status of the Enhanced Cybersecurity Services Program" (OIG Project No. 13-167-ITA-NPPD)

Thank you for the opportunity to review and comment on this draft report. The Department is pleased to note the Office of Inspector General's (OIG's) positive recognition of the progress DHS's National Protection and Programs Directorate's (NPPD's) Office of Cybersecurity and Communications (CS&C) has made in expanding the Enhanced Cybersecurity Services (ECS) program to all 16 critical infrastructure sectors. For example, CS&C has taken the following actions:

- Per Executive Order 13636 ("Improving Critical Infrastructure Cybersecurity"), developed processes and procedures to expand the ECS program out to all 16 critical infrastructure sectors within 120 days of its issuance.
- Completed all procedures and guidance required to carry out key tasks and operational aspects of the ECS program that includes an in-depth security validation and accreditation process.
- Addressed the privacy risk associated with the ECS program by conducting and publishing a Privacy Impact Assessment¹.
- Engaged sector-specific agencies and Government Furnished Information (GFI) providers to expand the ECS program, and developed program reporting and metric capabilities to monitor the program.
- Conducted a rigorous technical review and onsite system security assessment for Authorization to Operate to one ECS Commercial Service Provider (CSP)².

¹ Additionally, CS&C worked with the DHS Chief Privacy Officer and DHS Office for Civil Rights and Civil Liberties (CRCL) to complete a Privacy and Civil Liberties Assessment as required by E.O. 13636. The ECS program routinely seeks guidance from the NPPD Privacy Office and CRCL to address policy issues associated with the program, and to inform operational decision-making where privacy or individual rights questions may arise.

² A Commercial Service Provider (CSP) is a qualified critical infrastructure entity that uses Government cyber threat information to protect their internal network and may offer ECS services to validated critical infrastructure entities.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendations

The draft report contained three recommendations directed to NPPD's Assistant Secretary of CS&C with which NPPD CS&C concurs. Specifically, OIG recommended:

Recommendation 1: Ensure sufficient resources are available for the timely completion of the security validation and accreditation process for CSPs and operational implementers.

Response: Concur. Ensuring the success of the ECS program is one of DHS' top priorities. Further, the interest in critical infrastructure entities to become a CSP or an Operational Implementer (OI)³ exceeded the Department's expectations. For example, as of May 2014, DHS entered into 22 Memorandum of Agreements (MOAs) with critical infrastructure entities interested in becoming a CSP or OI. To address this increase in interest, NPPD CS&C has allocated additional resources to support the CSP/OI growth and has requested an increase to support the out-years.

It is also important to highlight that the federal government—through DHS—is sharing GFI that may be classified up to the Top Secret Sensitive Compartmented Information to qualified CSPs/OIs. The classification of the information and purpose of the system (using classified information to protect unclassified traffic) dictates an intensive security process. This combined with the various CSP architectures creates a highly involved, yet cooperative process, between the CSP/OI and DHS.

CS&C has a highly qualified staff of security experts currently on board to support the security validation and accreditation process; however, the limited number of experts restricts the number of assessment activities that can be accomplished at one time. To address this limitation, CS&C brought in additional Federally Funded Research & Development Center (FFRDC) security experts to support the security validation and accreditation process. In addition, CS&C is actively recruiting additional government resources with the required security expertise to augment the current government staff. Finally, CS&C is in the process of awarding a contract for security engineering services to provide support for additional security assessments. These measures will significantly increase the number of assessment activities that can be accomplished at one time, resulting in the timely completion of the security validation and accreditation process for CSPs and OIs.

Estimated Completion Date (ECD): Additional FFRDC resources were added to the program as of June 1, 2014. DHS has identified several FY14 and FY15 billets against which to recruit for security experts. The NPPD CS&C Security Engineering Services contract is planned to be awarded by December 2014.

Recommendation 2: Improve the ECS program's outreach efforts across all 16 critical infrastructure sectors, including service providers.

³ An Operational Implementer (OI) is a qualified critical infrastructure entity that uses Government cyber threat information to protect their internal network only.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Response: Concur. DHS launched the Critical Infrastructure Cyber Community (C³) Voluntary Program in February 2014, and NPPD is conducting extensive outreach and communication activities with critical infrastructure owners and operators all over the country interested in improving their cyber risk management processes. ECS is a major component within this voluntary program under the “Resources to Protect” and “Resources to Detect” Cybersecurity Framework Function Areas. Since the launch, DHS has delivered over 100 briefings and eight webinars that has informed over thousands of potential ECS critical infrastructure customers. The C³ Voluntary Program site has had nearly 18,000 visitors.

Additionally, NPPD CS&C’s ECS Program Management Office (PMO) is supplementing the strategic ECS program communication plan by drafting a targeted ECS outreach strategy.

This strategy will build on DHS’ approach of closely partnering with the CSPs by further promoting the benefits of the ECS program to critical infrastructure entities in all 16 critical infrastructure sectors. In addition, the strategy will highlight benefits that the ECS program may provide critical infrastructure entities through the value of the sensitive and classified federal government data and approved ECS services which utilize this data—via approved CSPs.

Estimated Completion Date (ECD): A final ECS Outreach Strategy will be completed by October 2014.

Recommendation 3: Develop a system to manage and analyze both sensitive and classified cyber threat indicators for the ECS program.

Response: Concur. We believe this recommendation should be closed as implemented since NPPD CS&C has already deployed an instance of the Cyber Indicator Analysis Platform (CIAP) to the Top Secret Mission Operating Environment (TS MOE) network to support NPPD CS&C’s cyber intrusion prevention capabilities. The TS instance of CIAP provides CS&C’s National Cybersecurity and Communications Integration Center (NCCIC) United States Computer Emergency Readiness Team (US-CERT) the capabilities needed to manage and analyze sensitive and classified cyber threat indicators for the ECS program. This web application allows analysts to create, update, search, import, export, and assign relationships between indicators and sightings. We note that NPPD CS&C reliance on individuals in some portions of the analysis and sharing process functions as a privacy and civil liberties safeguard, to ensure that threat information and countermeasures shared with CSPs are appropriate, calculated to assist them in the detection of malware and other exploits while not impairing lawful communications.

Estimated Completion Date (ECD): The installation and accreditation of the Cyber Indicator Analysis Platform, capable of managing both sensitive and classified cyber threat indicators, was completed on May 16, 2014. NPPD CS&C will provide evidence to the OIG under a separate cover.

Again, we thank you for the opportunity to review and provide comment on this draft report. Technical and sensitivity comments on the draft report have been provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Sincerely,

A handwritten signature in blue ink, appearing to read "AOzment", written over a horizontal line.

Andy Ozment
Assistant Secretary
Office of Cybersecurity and Communications



Appendix C

Major Contributors to This Report

Chiu-Tong Tsang, Director
Tarsha Cary, Audit Manager
Michael Kim, Team Lead
Aaron Zappone, Program Analyst
Patricia Thapanawat, IT Auditor
Fred Shappee, Referencer



Appendix D

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
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
Under Secretary, NPPD
Chief Information Officer, DHS
Chief Information Security Office, DHS
Chief Information Officer, NPPD
Chief Information Security Officer, NPPD
Director, Compliance and Oversight, DHS OCISO
Chief Privacy Officer, DHS
Audit Liaison, CIO, DHS
Audit Liaison, CISO, DHS
Audit Liaison, NPPD

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/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:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

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