Enhanced Cybersecurity Services Program

August 26, 2015

Fiscal Year 2015 Report to Congress

Homeland Security

National Protection & Programs Directorate

Message from the Under Secretary

August 26, 2015

I am pleased to present the following report, "Enhanced Cybersecurity Services Program," prepared by the National Protection and Programs Directorate.

This report has been compiled pursuant to a requirement in Senate Report 113-198, which accompanies the *Fiscal Year 2015 Department of Homeland Security Appropriations Act* (P.L. 114-4). This report provides an overview of Enhanced Cybersecurity Services' development and operations since establishment in 2013 following the issuance of Executive Order 13636 on *Improving Critical Infrastructure Cybersecurity*.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable John R. Carter
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Lucille Roybal-Allard
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable John Hoeven
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jeanne Shaheen
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to me at (202) 282-8260 or to the Department's Deputy Under Secretary for Management and Chief Financial Officer, Chip Fulghum, at (202) 447-5751.

Sincerely,

Suzanne Spaulding
Under Secretary
National Protection & Programs Directorate

Executive Summary

Cyber intrusions and attacks have increased significantly over the last decade, exposing sensitive personal and business information, disrupting operations, and imposing high costs on the U.S. economy. The Department of Homeland Security (DHS) plays a pivotal role in helping to secure the Federal Government and private-sector partners against these threats. This role is codified in the Department's 2014 *Quadrennial Homeland Security Review* (QHSR). Under the QHSR, DHS focuses on enhancing critical infrastructure security and resilience by reducing vulnerabilities; detecting malicious activity; promoting resilient critical infrastructure design; partnering with critical infrastructure owners and operators; and sharing information on threats, consequences, and mitigations. In 2014, Congress passed the *National Cybersecurity Protection Act*, which codifies the authority of DHS to assist the private sector with cybersecurity issues.

Enhanced Cybersecurity Services (ECS) is a key cybersecurity program through which DHS fulfills its mission to protect the private sector from cybersecurity threats. ECS is a voluntary information-sharing program that shares cyber threat information with qualified commercial service providers (CSP), enabling them to better protect their customers. ECS augments, but does not replace, an entity's existing cybersecurity capabilities. DHS works with cybersecurity organizations from across the Federal Government to gain access to a broad range of unclassified, sensitive, and classified cyber threat information. This information is shared with CSPs to protect their customers' data and systems from unauthorized access, exploitation, or data exfiltration. DHS was directed to expand the breadth of the ECS Program in *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity* in February 2013.

ECS is managed by the Department's Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate (NPPD). Within DHS, NPPD/CS&C is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical infrastructure to protect the public, economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks. Sharing cyber threat information with the private sector is an important goal of NPPD/CS&C.

This report meets the Senate Appropriations Committee (SAC) request for information on the ECS Program. The report details ECS' current size, expected growth rates, sectors participating in the program, and the anticipated demand for ECS over the next 2 years. Additionally, the report includes the plan for expanding public and private-sector

participation, including an articulation of any barriers to ECS adoption by certain users and how NPPD will assist in overcoming those barriers.

Enhanced Cybersecurity Services Program

Table of Contents

I. Legislative Language

Senate Report 113-198, which accompanies the *Fiscal Year* (FY) *2015 Department of Homeland Security* (DHS) *Appropriations Act* (P.L. 114-4), includes the following requirement:

> *Enhanced Cybersecurity Services.*—The Committee supports NPPD's efforts to make available Enhanced Cybersecurity Services (ECS) and urges NPPD to begin working with State and local governments on risks to government systems and to critical infrastructure in their communities. Since these governments oversee the safety of, and in some cases directly operate, elements of the electrical grid, water utilities, public transportation, communications systems, and other key assets it is critical that they have access to the latest tools in this fiscal year. Further, NPPD shall report to the Committee, no later than 60 days after the date of enactment of this act, on the current size and expected growth and need for ECS protection services. The report shall include the number of entities utilizing ECS today, the anticipated need for ECS use in the next 2 years, and NPPD's plan for expanding use of ECS, including an articulation of any barriers to ECS use by particular types of users and how NPPD will assist in overcoming those barriers.

II. Background

Enhanced Cybersecurity Services (ECS) shares unclassified, sensitive, and classified government-vetted cyber threat information (indicators), known as government-furnished information (GFI), with qualified commercial service providers (CSP) and operational implementers (OI). In turn, the CSPs use the cyber threat information to protect their customers, who have been limited to critical infrastructure entities validated by DHS. OIs use the cyber threat information to protect only their internal networks. In February 2013, *Executive Order* (E.O.) *13636: Improving Critical Infrastructure Cybersecurity* directed DHS to expand the ECS Program to all 16 critical infrastructure sectors. ECS is also available to state, local, tribal, and territorial (SLTT) governments, and information sharing and analysis centers (ISAC).

ECS currently provides two operational services: Domain Name Services (DNS) Sinkholing and Email (SMTP) Filtering. These services include robust privacy protections, which are documented in the ECS Privacy Impact Assessment (PIA).[1,2]

As a result of ongoing, high-profile cyber incidents and as our adversaries become more sophisticated, DHS and the interagency, through the Presidential Policy Directive 1 process, recently decided to expand ECS beyond critical infrastructure.[3] This expansion decision allows CSPs to market their ECS offerings beyond critical infrastructure entities and SLTT governments to all U.S.-based public and private entities. Further, ECS will be available to Information Sharing and Analysis Organizations (ISAO) facilitated through the implementation of *E.O. 13691: Promoting Private Sector Cybersecurity Information Sharing*. ISAOs, like all other public and private organizations, will be able to gain ECS protections by receiving services from a fully operational CSP.

The three operational CSPs and DHS continue to conduct outreach through a variety of mechanisms to expand the number of entities benefiting from ECS protections. ECS is

[1] National Institute of Standards and Technology Special Publication 800-95, "Guide to Secure Web Services," defines a service "as a processing or communication service that is provided by a system to give a specific kind of protection to resources, where said resources may reside with said system or reside with other systems." Countermeasures, which can be provided as services, are interpreted by the program to include automated actions with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on an information system, for the purpose of protecting the information system from cybersecurity threats. As used in this report, the term "services" can be read to include countermeasures.

[2] The ECS PIA is available at: http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf

[3] The "General Cyber Summary of Conclusions," dated January 30, 2015. Interagency Planning Committees are the main forum for interagency coordination under the Presidential Policy Directive 1 process. These groups conduct the day-to-day interagency analysis, generation of courses of action, policy development, coordination, resource determination, and policy implementation planning. They are organized around regional or functional areas; this one in particular is on cyber.

referenced in senior-level briefings to industry partners, and is a key component of DHS's Critical Infrastructure Cyber Community (C^3) Voluntary Program. Under the C^3 Program, ECS falls under the "Protect" and "Defend" functions of the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.

III. Results and Resources

ECS is currently available to companies in all critical infrastructure sectors, SLTT governments, and ISACs. This service is available through the three fully operational CSPs: AT&T, Verizon, and CenturyLink. Currently, 43 entities receive services through the ECS Program. As of June 2015, the program has signed a total of 22 memoranda of agreement (MOA) with entities interested in becoming an operational CSP or OI. The 21 entities are at different stages in the overall security process, and DHS continues to work with prospective CSPs to assist them with building their ECS capability. These entities will begin receiving unclassified, sensitive, and classified cyber threat indicators only when they have a DHS-accredited system that can receive and protect GFI. The security process requires that actions be taken by the prospective CSP, DHS, and, in some cases, other federal partners. The security requirements of the program are significant and require extensive resource investments by potential CSPs as well as by DHS. Because ECS is governed by MOAs with OIs and CSPs and not by a contract vehicle, companies pursuing the CSP/OI route can choose to change their path, temporarily hold progress, or stop participation at any time. This introduces uncertainty into the Department's resource planning.

Through ECS, DHS is sharing timely, actionable, and vetted GFI with qualified CSPs. In February 2015, ECS shared more than 370 indicators and has shared more than 5,000 indicators since May 2013. As a result of these indicators, ECS discovered more than 800,000 instances of malicious activity that otherwise likely would have gone undetected. The ECS Program Management Office (PMO) circulates unclassified reporting outlining the malicious activity identified by ECS indicators. This reporting is detailed in Section IV. The performance reports summarized in Section IV are derived from anonymized, aggregated cybersecurity metric data shared with DHS from participating CSPs and demonstrate the value of receiving ECS for the protected entity. The data in these reports are shared with DHS on a voluntary basis that is agreed upon between CSPs and their customers. Because ECS is a voluntary program, customers can opt out of having their reporting shared with DHS. However, voluntarily sharing with DHS helps to improve overall data quality and informs program performance.

As referenced in Section II, the ECS customer base is expanding. The program is moving forward with formal expansion messaging enabling CSPs to expand their ECS customer base. In this new model, CSPs will be able to provide ECS protections to any organization that meets the program requirements without having to validate their new customers with DHS. As more entities begin receiving protection from ECS, NPPD believes that additional CSPs will join the market and thereby increase the overall capacity of the program. Furthermore, NPPD continues to work with the CSPs, OIs, and GFI providers on ways to expand current service offerings and further streamline

program processes. However, adding any new service to the program using sensitive and classified GFI requires extensive system security reviews and approvals before implementation. To support the demand and growth of the program, NPPD actively is recruiting individuals to fill five new FY 2015 positions.

The ECS Program is an NPPD CS&C cross-divisional program, and the CS&C Assistant Secretary is the program's executive sponsor. The ECS PMO branch is responsible for managing the overall program; the Network Security Deployment (NSD) branch handles all the security aspects; and, finally, the National Cybersecurity and Communications Integration Center's (NCCIC) United States Computer Emergency Readiness Team (US-CERT) is the program's operational arm. The following chart depicts approved funding for ECS in FY 2014 and FY 2015 and includes program descriptions.

NPPD/CS&C ECS Costs			
$ in thousands	**FY 2014 Enacted**	**FY 2015 Enacted**	**FY 2016 Request**
PMO Engagement/Validation	909	1,229	2,115
Operations	237	446	789
Certification & Accreditation*	4,596	4,776	10,465
Secure Communications*	7,299	6,459	5,439
TOTAL	**$13,041**	**$12,910**	**$18,808**
*FYs 2014–2015 certification & accreditation and secure communications are associated with EINSTEIN 3 Accelerated[4] activities and are funded out of NPPD's National Cybersecurity Protection System profile.			

ECS contains embedded privacy protections that use the Fair Information Practice Principles to assess and mitigate any privacy impacts.[5] DHS has conducted and published a PIA for the ECS Program that ensures ECS is structured in a way that protects individual rights. Additionally, the ECS Program does not involve government monitoring of private networks or communications.

PMO Engagement/Validation – Stakeholder Engagement and Cyber Infrastructure Resilience

- In FY 2014, five full-time positions (FTP) were approved to manage all aspects of the program to include ongoing engagements with ECS partners and stakeholders, validation of CI entities, GFI service expansion, requirements, and the development of all performance reporting.
- In FY 2015, three additional FTPs were approved and actively are being recruited to support program growth; this will bring the PMO staff to eight FTPs.

[4] http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf

[5] http://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-02.pdf

- In FY 2016, 2 additional FTPs, bringing the PMO staff to 10 FTPs, and $0.602 million in program funding are requested.

Operations – NCCIC/US-CERT

- CS&C received one FTP in FY 2014 and two additional FTPs in FY 2015.
- In FY 2016, two additional FTPs are being requested; this will bring the Operations staff to five FTPs.
- As the operational component of ECS, NCCIC/US-CERT has the responsibility for vetting all GFI to ensure that the data shared are actionable, timely, and relevant to current cyber threats. The NCCIC/US-CERT disseminates the ECS data feed with the approved CSPs/OIs, and has the responsibility of addressing ECS-related requests for information (RFI).
- There are no program dollars to support this initiative, only FTPs.

Certification & Accreditation – NSD

- Certification & Accreditation – the Sensitive Compartmented Information Facility (SCIF) is required to be certified and accredited before entering operation at the CSP/OI. This is part of the security requirements to protect classified and sensitive information from unauthorized disclosure and to ensure operational security for the ECS Program.
- NPPD estimates increasing the number of fully accredited CSPs/OIs from two to four by the end of FY 2015 and from four to eight by the end of FY 2016.
- In FY 2015, NSD is allocating $4.776 million toward this effort.
- In FY 2016, $10.255 million in program funding and two FTPs/$0.210 million in Salaries and Benefits are requested.
- NSD is leveraging existing contracts to accomplish the Certification and Accreditation of CSP/OI SCIFs.

Secure Communications – NSD

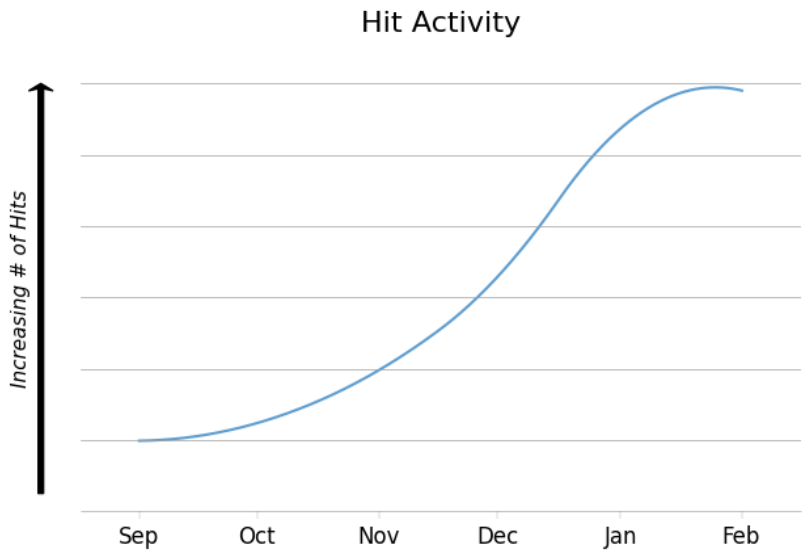
- Secure Communications – the necessary equipment and network accreditation for CSPs/OIs to communicate classified and sensitive information, as required by the ECS Program
- NPPD estimates increasing the number of fully accredited CSPs/OIs from two to four by the end of FY 2015 and from four to eight by the end of FY 2016.
- In FY 2015, NSD is allocating $6.459 million toward this effort.
- In FY 2016, $5.229 million in program funding and two FTPs/$.210 million in Salaries and Benefits are requested.
- NPPD is leveraging existing contracts to accomplish the accreditation of secure network communications.

IV. Analysis/Discussion

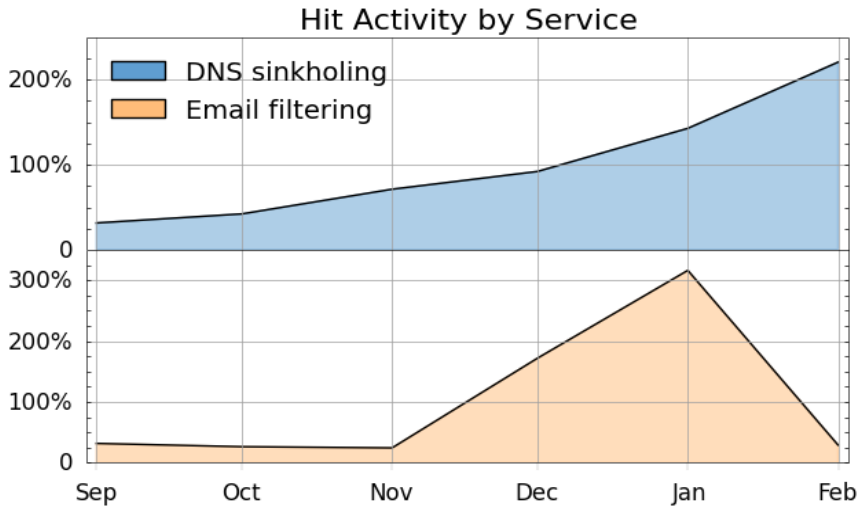
The ECS PMO receives anonymized, aggregated cybersecurity metric data from participating CSPs. These anonymized data are shared voluntarily and their availability is determined through contract language between CSPs and their customers before sharing them with DHS. Because ECS is a voluntary program, customers of these services can opt out of having their metric information shared with the Department. The process for sharing information with CSP/OI and for CSP/OI to share metric data with DHS has been fully coordinated with DHS's Privacy Office, Office of General Counsel, and the Office for Civil Rights and Civil Liberties.

The ECS Program has developed several performance reports that can be distributed at both the Unclassified and For Official Use Only (FOUO) levels. These performance reports showcase malicious activity level by ECS service (DNS and email) and show trends by critical infrastructure sector. However, not all CSPs share metric data by sector.

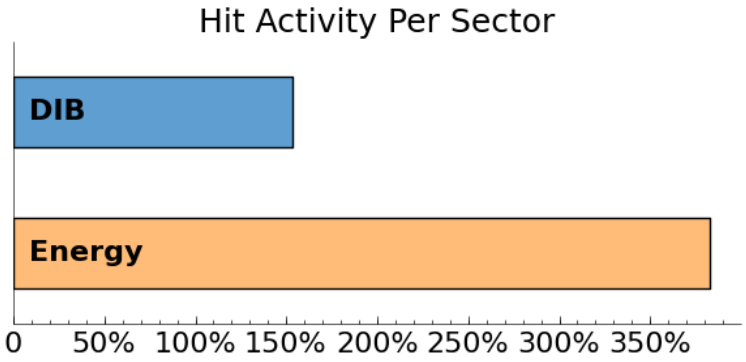
The following are examples of Unclassified ECS Performance Graphs:



The above graph showcases the total number of hits for the past 6 months. Total program activity increased more than 10 percent in February compared to January. Overall, the number of hits experienced by ECS participants has increased substantially during the past 4 months.



The Service graph above depicts the trends of the two approved services: DNS Sinkholing (blue) and Email Filtering (orange). Over the last 6 months, there has been a significant increase in the number of DNS Sinkholing hits. Email Filtering experienced a noticeable increase in December and January, but decreased in February. Activity can vary for a variety of reasons, including threat actor activity and changing tactics.



This illustration represents the number of hits in a given sector (Defense Industrial Base (DIB) and Energy), normalized by the 6-month average. Both Energy and DIB experienced a higher-than-average number of events in February. The Energy Sector, in particular, saw over 350 percent more hits than the 6-month average. Again, hit activity can vary on the basis of a variety of reasons. In this particular case, some sectors are more represented than others depending on which companies are receiving services and whether they opt in to having their hit data shared with DHS.

V. Independent Oversight and DHS Response

The ECS Program has undergone multiple oversight reviews. DHS's Office of Inspector General (OIG) conducted an audit of the program between November 2013 and March 2014, and the final report, *Implementation Status of the Enhanced Cybersecurity Services Program*, was published in July 2014. The OIG's objective in this audit was to determine the effectiveness of the program at disseminating cyber threat and technical information to CSPs that is used to protect critical infrastructure. OIG made three recommendations to NPPD. Recommendation 1 outlined the need to ensure that sufficient resources are available for the timely completion of the security validation and accreditation process for CSPs and operational implementers. Recommendation 2 stated that improvements need to be made to the ECS Program's outreach efforts across all critical infrastructure sectors, including to CSPs. Recommendation 3 stated the need to develop a system that manages and analyzes sensitive and classified cyber threat indicators for the ECS Program. All three recommendations have been closed: Recommendations 1 and 2 were implemented by NPPD and closed by the OIG within 4 months after the report was released, and recommendation 3 was implemented and closed before publication.

Section 5 of E.O. 13636 requires the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties annually to assess the privacy and civil liberties impacts of the activities that DHS undertakes pursuant to the E.O. and to provide those assessments with recommendations for mitigating identified privacy risks in an annual public report. The 2014 report highlighted NPPD's transparency and determined that the program has little to no effect on civil liberties or individual rights. However, the report recommended that the DHS Privacy Office should continue its vigilant oversight of the ECS Program to ensure that any potential privacy impact that may arise is identified and addressed promptly. The 2015 report continued to highlight NPPD's transparency with the ECS Program. Additionally, the DHS Privacy Office conducted a Privacy Compliance Review in coordination with NPPD/CS&C and the NPPD Office of Privacy, for the activity period of January 2013 through September 2014. This report was published on April 10, 2015, and is posted on DHS's website. [6]

Finally, the Government Accountability Office (GAO) conducted a review titled *Defense Cybersecurity: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats* (GAO-12-762). This was a Department of Defense (DOD) review; however, one recommendation was directed to both DOD and DHS and is related to the ECS Program. This report is FOUO, and the joint recommendation was issued on DOD's DIB Opt-In Pilot. The recommendation directed

[6] *See,* E.O. 13636-required Privacy and Civil Liberties Assessments at: http://www.dhs.gov/cybersecurity-and-privacy

DOD and DHS to develop a feedback mechanism that would enable participating DIB companies to report cyber threat information back to the government to improve information sharing and to identify and clarify all stakeholders in the pilot. DHS considers this recommendation closed and has provided GAO with supporting documentation.

VI. Conclusion

As codified in E.O. 13636, ECS is the U.S. Government's program for sharing classified cyber threat information to protect private-sector networks. DHS continues to work with all companies that have signed an MOA with DHS to assist them through the many security processes included in the ECS Program to become a CSP. The Department's goal is to partner with interested companies to expand the ECS marketplace by accrediting more CSPs and enabling the private sector to innovate in expanding the scope of available ECS protections beyond email and DNS. DHS will continue to work diligently with government partners and the private sector to expand the reach of ECS in protecting a greater share of the Nation's companies at risk from an increasing cybersecurity threat.