Enhanced Cybersecurity Services

July 18, 2016
Fiscal Year 2016 Report to Congress
Message from the Under Secretary

July 18, 2016

I am pleased to present the following report, “Enhanced Cybersecurity Services,” prepared by the National Protection and Programs Directorate (NPPD).

This report has been compiled pursuant to language in Senate Report 114-68, which accompanies the Fiscal Year 2016 Department of Homeland Security (DHS) Appropriations Act (P.L. 114-113). This report addresses the Committee’s request for NPPD’s Enhanced Cybersecurity Services (ECS) strategy with the private sector to include state and local stakeholders.

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. DHS plays a pivotal role in helping to secure the Federal civilian 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 DHS’s authority to help the private sector manage cybersecurity risks.

ECS is a key program in achieving this important national mission. Through ECS, DHS shares sensitive and classified cyber threat information with qualified commercial service providers (CSP). These CSPs, in turn, use that information to protect their participating customers from certain types of cybersecurity threats. ECS is meant to augment, not replace, the existing cybersecurity capabilities of these protected entities. The cyber threat information shared through ECS is sourced from partners across the Federal Government. ECS is now available to all U.S.-based public and private organizations.

ECS is managed by the DHS Office of Cybersecurity and Communications (CS&C), within NPPD. NPPD/CS&C is responsible for protecting the federal civilian executive branch and for helping the private sector and state, local, tribal, and territorial (SLTT) governments manage their own risk.

CS&C engages in six related lines of effort to fulfill its mission:

1. Serve as the national hub for cybersecurity information sharing
2. Shape and promote adoption of leading practices
3. Respond to incidents
4. Ensure the interoperability and continuity of National Security/Emergency Preparedness communications
5. Build a strong cyber ecosystem
6. Provide a common baseline of security for the Federal civilian Government

The ECS model, which commonly is known as a Managed Security Service, allows customers to contract directly with a CSP to receive services. The advantages of this model are twofold:
1. **Scalability** – ECS customers are able to sign up directly with a CSP to receive services. They do not have to acquire security clearances or conduct expensive, time-consuming system buildouts in order to protect themselves. One CSP can protect many organizations via this model.

2. **Privacy** – CSPs function as an intermediary between customers and the U.S. Government. Customers are protected by government-furnished information without having to engage technically or contractually with the U.S. Government. CSPs handle all aspects of customer participation.

CS&C engages with its CSP partners regularly to discuss program requirements, identify methods for improving current processes, and conduct external outreach to potential ECS customers. This report articulates how ECS will continue to integrate SLTT entities into its outreach and to drive further participation and awareness among SLTT and private-sector groups.
## Enhanced Cybersecurity Services (ECS)

### Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Legislative Language</td>
<td>1</td>
</tr>
<tr>
<td>II. Background</td>
<td>2</td>
</tr>
<tr>
<td>III. Scope and Strategy for Further Expansion</td>
<td>4</td>
</tr>
<tr>
<td>IV. Conclusion</td>
<td>6</td>
</tr>
</tbody>
</table>
I. Legislative Language

This report has been compiled pursuant to language in Senate Report 114-68, which accompanies the *Fiscal Year 2016 Department of Homeland Security (DHS) Appropriations Act* (P.L. 114-113).

Senate Report 114-68 states:

**ENHANCED CYBERSECURITY SERVICES**

The Enhanced Cybersecurity Services [ECS] program is another DHS-sponsored protection and information sharing capability between selected Commercial Service Providers and validated critical infrastructure companies as well as State and local customers. While the relationship between ECS and the private sector has been utilized since this program began as a pilot in 2010, the addition of State and local partners is relatively new. 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 they have access to the latest tools. The Committee expects NPPD to ensure ECS stakeholders are engaged in the development of requirements and process improvements. Overall, the ECS program must be scalable and integrated with other programs within the Directorate. Not later than 90 days after the date of enactment of this act, NPPD is to report to the Committee on its strategy to integrate State and local stakeholders in the ECS process, develop a strategy to make the ECS program scalable, and the strategic priorities moving forward.
II. Background

ECS shares unclassified, sensitive, and classified government-vetted cyber threat indicators, known as government-furnished information (GFI), with qualified commercial service providers (CSP) and operational implementers (OI). In turn, CSPs use the cyber threat indicators to protect participating U.S.-based customers. OIs use the cyber threat indicators to protect their own networks. In June 2015, DHS expanded the ECS program to allow the participation of all U.S.-based public and private organizations, including state, local, tribal, and territorial (SLTT) governments. Participation previously was limited to critical infrastructure entities that were validated by DHS.

ECS is a partnership between DHS and each CSP. DHS shares GFI, accredits each CSP’s ECS systems, and helps each CSP to conduct outreach to potential customers. This outreach occurs through a variety of mechanisms such as briefings to industry partners, the DHS Critical Infrastructure Cyber Community (C3) Voluntary Program, and panel discussions at industry events.

As noted, ECS is available to all U.S.-based public and private organizations, including SLTT governments, Information Sharing Analysis Centers (ISAC), and Information Sharing Analysis Organizations (ISAO). Currently, entities in six sectors are protected by ECS: Commercial Facilities, Communications, Critical Manufacturing, Defense, Energy, and Finance. As of February 2016, the program has signed a total of 24 memoranda of agreement (MOA) with entities interested in becoming CSPs or OIs. These signatories are at various stages of the security accreditation process. Once accredited, CSPs and OIs are eligible to receive GFI and can begin offering ECS services to their customers or using GFI to protect their own networks. Four CSPs currently are accredited to provide ECS:

- AT&T
- CenturyLink
- Verizon
- Lockheed Martin

Currently, ECS CSPs may offer three services: Domain Name Service Sinkholing, Email Filtering, and Netflow Analysis.\(^1\) All service offerings are provided voluntarily by each CSP and include robust privacy protections, which are documented in the recently

\(^1\) The third service, Netflow Analysis, was added in February 2016, in response to a request from an ECS CSP. Netflow Analysis allows CSPs to use an additional type of GFI to identify and analyze malicious activity transiting customer networks.
updated ECS Privacy Impact Assessment (PIA). The ECS program strives to respond to the needs of CSPs and their customers by considering proposals for future service offerings. Approval of such proposals is based primarily upon the availability of relevant GFI to support particular services. Additionally, DHS continues to coordinate with other U.S. Government agencies and programs regarding possible capability additions that could enhance the security protections available under the program. It is important to highlight that any enhancements to ECS will undergo the appropriate privacy and legal assessments.

The security processes associated with accreditation are significant and require extensive resource investment by the potential CSPs and DHS. Because ECS is governed by MOAs with CSPs rather than by contract, companies pursuing accreditation may choose to stop participation at any time. This creates significant planning and timeline uncertainties and concomitant challenges in long-term resource planning.

CSPs are responsible for marketing ECS to their customers based upon contractual service-level agreements. However, DHS assists CSPs in raising awareness of the program in public fora. DHS also works to expand service offerings and share actionable and timely GFI with CSPs to increase the program’s value. However, the addition of any new service entails extensive system security reviews and approvals before implementation is possible. These system reviews are critical to maintaining classified GFI protection.

Since its inception, ECS has blocked more than one million instances of potentially malicious activity. Without ECS, these intrusion attempts may well have gone unnoticed and resulted in damaging compromises. A significant number of these attempts were correlated with known major threat actors. The ECS program distributes a monthly unclassified report outlining the malicious activity identified by ECS indicators.

---

III. Scope and Strategy for Further Expansion

DHS seeks to ensure that ECS is available to all U.S.-based public and private entities, including SLTT governments. As part of this goal, CS&C continually encourages SLTT governments to participate in ECS. Those efforts include regular ECS briefings to SLTT organizations, participation in events and panels focused on SLTT audiences, and timely responses to requests for information from SLTT partners.

For example, CS&C led an ECS panel with the operational CSPs at the annual meeting of the Multi-State Information Sharing and Analysis Center (MS-ISAC) in November 2015. The MS-ISAC is a DHS-funded membership organization consisting of SLTT governments that serves as a focal point for threat prevention, protection, response, and recovery. Of note, MS-ISAC offers an intrusion detection capability to identify threat activity in certain types of Internet traffic for participating state governments. This service is known as ALBERT. The MS-ISAC’s ALBERT system uses only unclassified indicators and does not block cybersecurity threats actively, differentiating the system from the ECS program. ECS should be considered complementary to rather than in competition with unclassified intrusion detection systems such as ALBERT. As another example, CS&C highlighted ECS in a briefing to National Association of State Chief Information Officers in May 2016.

Although most SLTT governments deem cybersecurity to be a high priority, many lack the financial resources to purchase services like ECS. CS&C is working to educate SLTT governments about resources available to help with this financial burden. For example, SLTT governments can request grant funding from the Homeland Security Grant Program for cybersecurity capabilities such as ECS. CS&C is working with the Federal Emergency Management Agency and SLTT partners to ensure broad recognition of this resource.

Additionally, most SLTT governments are required to obtain cybersecurity services via formal procurement processes. Such government entities generally cannot purchase ECS services without a formal bidding process. CS&C works with SLTT governments to help craft procurement announcements that could be fulfilled by ECS CSPs.

Currently, ECS is the only cybersecurity offering on the commercial market that can ingest and utilize classified information to protect unclassified networks. To maximize the usefulness of that classified information, CS&C strives to downgrade any contextual information that may be useful to CSPs and their customers. But the primary value of ECS is immediate: it actively blocks cybersecurity threats before they can compromise customer networks. To this end, CS&C intends to continue marketing ECS for SLTT
governments and the private sector in order to increase the breadth of participating CSPs and customers.
IV. Conclusion

The ECS program is working actively to increase participation from all U.S.-based public and private entities, including SLTT governments. Over the past year, CS&C has relaxed eligibility criteria for ECS customers, accredited a fourth CSP, and added a new service offering. All of these achievements are intended to meet customer needs: increasing the number of participants, the availability of services, and the number of services. With a robust foundation now in place, CS&C will continue to educate potential customers about the benefits of ECS with the goal of expanding ECS participation to all critical infrastructure sectors and state governments.