United States Government Accountability Office

Testimony

Before the Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10 a.m. ET
Tuesday, March 28, 2017

INFORMATION SECURITY

DHS Needs to Continue to Advance Initiatives to Protect Federal Systems

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO Highlights

Highlights of GAO-17-518T, a testimony before the Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security, House of Representatives

March 28, 2017

INFORMATION SECURITY

DHS Needs to Continue to Advance Initiatives to Protect Federal Systems

Why GAO Did This Study

Cyber-based intrusions and attacks on federal systems are evolving and becoming more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include the protection of cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

DHS plays a key role in strengthening the cybersecurity posture of the federal government. Among other things, DHS has initiatives for (1) detecting and preventing malicious cyber intrusions into agencies' networks and (2) deploying technology to assist agencies to continuously diagnose and mitigate cyber threats and vulnerabilities.

This statement provides an overview of GAO's work related to DHS's efforts to improve the cybersecurity posture of the federal government. In preparing this statement, GAO relied on previously published work, as well as information provided by DHS on its actions in response to GAO's previous recommendations.

What GAO Recommends

In a January 2016 report, GAO made nine recommendations related to expanding NCPS's capability to detect cyber intrusions; notifying customers of potential incidents; providing analytic services; and sharing cyber-related information, among other things. DHS concurred with the recommendations and is taking actions to implement them.

View GAO-17-518T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) is spearheading multiple efforts to improve the cybersecurity posture of the federal government. Among these, the National Cybersecurity Protection System (NCPS) provides a capability to detect and prevent potentially malicious network traffic from entering agencies' networks. In addition, DHS's continuous diagnostics and mitigation (CDM) program provides tools to agencies to identify and resolve cyber vulnerabilities on an ongoing basis.

In January 2016, GAO reported that NCPS was limited in its capabilities to detect or prevent cyber intrusions, analyze network data for trends, and share information with agencies on cyber threats and incidents. For example, it did not monitor or evaluate certain types of network traffic and therefore would not have detected malicious traffic embedded in such traffic. NCPS also did not examine traffic for certain common vulnerabilities and exposures that cyber threat adversaries could have attempted to exploit during intrusion attempts. In addition, at the time of the review, federal agencies had adopted NCPS to varying degrees. GAO noted that expanding NCPS's capabilities, such as those for detecting and preventing malicious traffic and developing network routing guidance, could increase assurance of the system's effectiveness in detecting and preventing computer intrusions and support wider adoption by agencies. By taking these steps, DHS would be better positioned to achieve the full benefits of NCPS.

The tools and services delivered through DHS's CDM program are intended to provide agencies with the capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. In May 2016, GAO reported that most of the 17 civilian agencies covered by the *Chief Financial Officers Act* that also reported having high-impact systems were in the early stages of CDM implementation. For example, 14 of the 17 agencies reported that they had deployed products to automate hardware and software asset inventories, configuration settings, and common vulnerability management but only 2 had completed installation of agency and bureau/component-level dashboards. Some of the agencies noted that expediting CDM implementation could be of benefit to them in further protecting their high-impact systems. GAO concluded that the effective implementation of the CDM program can assist agencies in resolving cybersecurity vulnerabilities that expose their information systems and information to evolving and pernicious threats. By continuing to make available CDM tools and capabilities to agencies, DHS can have additional assurance that agencies are better positioned to protect their information system and information.

In addition, DHS offered other services such as monthly operational bulletins, CyberStat reviews, and cyber exercises to help protect federal systems. In May 2016, GAO reported that although participation varied among the agencies surveyed, most agencies had found that the services were very or somewhat useful. By continuing to make these services available to agencies, DHS is better able to assist agencies in strengthening the security of their information systems.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee:

Thank you for the opportunity to appear before you to discuss the Department of Homeland Security's (DHS) efforts to secure federal computer networks. As recent cyberattacks have illustrated, the need for robust and effective cybersecurity has never been greater.

Today, I will provide an overview of our work related to efforts by DHS to improve the cybersecurity posture of the federal government. In particular, I will focus on two of the department's initiatives: the National Cybersecurity Protection System (NCPS), operationally known as Einstein, and the Continuous Diagnostics and Mitigation (CDM) program.

In developing this testimony, we relied on our previous reports[1] as well as information provided by the department on its actions in response to our previous recommendations. A more detailed discussion of the objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1]GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016); *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016); *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk*, GAO-16-513 (Washington, D.C.: Aug. 30, 2016); *Information Security: Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data*, GAO-16-493 (Washington, D.C.: Apr. 28, 2016); *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, GAO-16-398 (Washington, D.C.: Mar. 28, 2016); *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls*, GAO-16-265 (Washington, D.C.: Mar. 23, 2016); *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Washington, D.C.: Sept. 29, 2015); *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*, GAO-15-221 (Washington, D.C.: Jan. 29, 2015); and *Information Security: VA Needs to Address Identified Vulnerabilities,* GAO-15-117 (Washington, D.C.: Nov. 13, 2014).

Background

Federal agencies are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, ineffective security controls to protect these systems and data could have a significant impact on a broad array of government operations and assets.

Computer networks and systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. These systems are often interconnected with other internal and external systems and networks, including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface.

In addition, cyber threats to systems supporting the federal government are evolving and becoming more sophisticated. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, foreign nations—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks.

Safeguarding federal computer systems has been a long-standing concern. This year marks the 20th anniversary of when GAO first designated information security as a government-wide high-risk area in 1997.[2] We expanded this high-risk area to include safeguarding the systems supporting our nation's critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.[3]

Over the last several years, GAO has made about 2,500 recommendations to agencies aimed at improving the security of federal systems and information. These recommendations identified actions for agencies to take to strengthen their information security programs and technical controls over their computer networks and systems. Many

[2]GAO designates agencies and program areas as high risk due to their vulnerability to fraud, waste, abuse, and mismanagement, or when they are most in need of transformation.

[3]See GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

agencies continue to be challenged in safeguarding their information systems and information, in part because many of these recommendations have not been implemented. As of February 2017, about 1,000 of our information security-related recommendations had not been implemented.

Our audits of the effectiveness of information security programs and controls at federal agencies have consistently shown that agencies are challenged in securing their information systems and information. In particular, agencies have been challenged in the following activities:

- *Enhancing capabilities to effectively identify cyber threats to agency systems and information.* A key activity for assessing cybersecurity risk and selecting appropriate mitigating controls is the identification of cyber threats to computer networks, systems, and information. In 2016, we reported on several factors that agencies identified as impairing their ability to identify these threats to a great or moderate extent. The impairments included an inability to recruit and retain personnel with the appropriate skills, rapidly changing threats, continuous changes in technology, and a lack of government-wide information sharing mechanisms.[4] We believe that addressing these impairments will enhance the ability of agencies to identify the threats to their systems and information and be in a better position to select and implement appropriate countermeasures.
- Implementing sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices. In our reports, we routinely determine that agencies do not enable key information security capabilities of their operating systems, applications, workstations, servers, and network devices. Agencies were not always aware of the insecure settings that introduced risk to the computing environment. We believe that establishing strong configuration standards and implementing sustainable processes for monitoring and enabling configuration settings will strengthen the security posture of federal agencies.
- *Patching vulnerable systems and replacing unsupported software.* Federal agencies we have reviewed consistently fail to apply critical security patches on their systems in a timely manner, sometimes doing so years after the patch becomes available. We have

[4]GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

consistently identified instances where agencies use software that is no longer supported by their vendors. These shortcomings place agency systems and information at significant risk of compromise, since many successful cyberattacks exploit known vulnerabilities associated with software products. We believe that using vendor-supported and patched software will help to reduce this risk.

- *Developing comprehensive security test and evaluation procedures and conducting examinations on a regular and recurring basis.* Federal agencies we have reviewed often do not test or evaluate their information security controls in a comprehensive manner. The agency evaluations we reviewed were sometimes based on interviews and document reviews (rather than in depth security evaluations), were limited in scope, and did not identify many of the security vulnerabilities that our examinations identified. We believe that conducting in-depth security evaluations that examine the effectiveness of security processes and technical controls is essential for effectively identifying system vulnerabilities that place agency systems and information at risk.

Federal Laws Provide a Framework for Securing Agencies' Information and Systems

The Federal Information Security Modernization Act of 2014 (FISMA)[5] provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and for ensuring the effective oversight of information security risks, including those throughout civilian, national security, and law enforcement agencies. The law requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency.

FISMA also establishes key government-wide roles for DHS. Specifically, with certain exceptions, DHS is to administer the implementation of agency information security policies and practices for information systems including:

[5]The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, Dec. 17, 2002). As used here, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

- monitoring agency implementation of information security policies and practices;
- providing operational and technical guidance to agencies;
- operating a central federal information security incident center; and
- deploying technology upon request to assist the agency to continuously diagnose and mitigate cyber threats and vulnerabilities.

In addition, the *Cybersecurity Act of 2015* requires DHS to deploy, operate, and maintain for use by any federal agency, a capability to (1) detect cybersecurity risks in network traffic transiting to or from agency information systems and (2) prevent network traffic with such risks from traveling to or from an agency information system or modify the traffic to remove the cybersecurity risk.[6]

Advancing DHS Initiatives Could Improve the Cybersecurity Posture of the Federal Government

In implementing federal law for securing agencies' information and systems, DHS is spearheading several initiatives to assist federal agencies in protecting their computer networks and electronic information. These include NCPS, CDM, and other services. However, our work has highlighted the need for advances within these initiatives.

NCPS Capabilities and Adoption Could Be Improved

Operated by DHS's United States Computer Emergency Readiness Team (US-CERT),[7] NCPS is intended to detect and prevent cyber intrusions into agency networks, analyze network data for trends and anomalous data, and share information with agencies on cyber threats and incidents. Deployed in stages, NCPS, operationally known as EINSTEIN, has provided increasing capabilities to detect and prevent potential cyber-attacks involving the network traffic entering or exiting the networks of participating federal agencies. Table 1 provides an overview of the EINSTEIN deployment stages to date.

[6]Div. N, sec. 223, Pub. L. No. 114-113 (Dec. 18, 2015); 129 Stat. 2935, 2964; 6 U.S.C. § 151.

[7]Within DHS, US-CERT is a component of the National Cybersecurity and Communications Integration Center. It serves as the central federal information security incident center specified by FISMA.

Table 1: Overview of the National Cybersecurity Protection System (NCPS) Deployment

Operational name	Deployment year	NCPS objective	Description
EINSTEIN 1	2003	Intrusion detection	Provides an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their Internet connections.[a]
EINSTEIN 2	2009	Intrusion detection	Monitors federal agency Internet connections for specific predefined signatures of known malicious activity and alerts US-CERT when specific network activity matching the predetermined signatures is detected.[b]
EINSTEIN 3 Accelerated	2013	Intrusion detection Intrusion prevention	Automatically blocks malicious traffic from entering or leaving federal civilian agency networks. This capability is managed by Internet service providers, who administer intrusion prevention and threat-based decision making using DHS-developed indicators of malicious cyber activity to develop signatures.[c]

Source: GAO analysis of Department of Homeland Security data. | GAO-17-518T

[a]The network traffic information includes source and destination Internet Protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

[b]Signatures are recognizable, distinguishing patterns associated with cyber-attacks, such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

[c]An indicator is defined by DHS as human-readable cyber data used to identify some form of malicious cyber activity. These data may be related to Internet Protocol addresses, domains, e-mail headers, files, and character strings. Indicators can be either classified or unclassified.

The overarching objectives of NCPS are to provide functionality that supports intrusion detection, intrusion prevention, analytics, and information sharing.[8] However, in January 2016, we reported that NCPS had partially, but not fully, met these objectives:[9]

- **Intrusion detection:** NCPS provided DHS with a limited ability to detect potentially malicious activity entering and exiting computer networks at federal agencies. Specifically, NCPS compared network traffic to known patterns of malicious data, or "signatures," but did not detect deviations from predefined baselines of normal network

[8]The National Institute of Standards and Technology (NIST) describes intrusion detection as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to bypass the security mechanisms of a computer or network or to compromise the confidentiality, integrity and availability of the information they contain. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Analytics is the synthesis of knowledge from the collection, preparation and analysis of data. Information sharing is the process of exchanging of cyber threat and incident data.

[9]GAO-16-294.

behavior. In addition, NCPS did not monitor several types of network traffic and therefore would not have detected malicious traffic embedded in such traffic. NCPS also did not examine traffic for certain common vulnerabilities and exposures that cyber threat adversaries could have attempted to exploit during intrusion attempts.

- **Intrusion prevention:** The capability of NCPS to prevent intrusions was limited to the types of network traffic it monitored. For example, the intrusion prevention function monitored and blocked e-mail determined to be malicious. However, it did not monitor malicious content within web traffic, although DHS planned to deliver this capability in 2016.
- **Analytics:** NCPS supported a variety of data analytical tools, including a centralized platform for aggregating data and a capability for analyzing the characteristics of malicious code. However, DHS had not developed planned capabilities to facilitate near real-time analysis of various data streams, perform advanced malware behavioral analysis, and conduct forensic analysis in a more collaborative way. DHS planned to develop and implement these enhancements through 2018.
- **Information sharing:** DHS had yet to develop most of the planned functionality for NCPS's information-sharing capability, and requirements had only recently been approved at the time of our review. Agencies and DHS also did not always agree about whether notifications of potentially malicious activity had been sent or received, and agencies had mixed views about the usefulness of these notifications. Further, DHS did not always solicit—and agencies did not always provide—feedback on them.

In addition, while DHS had developed metrics for measuring the performance of NCPS, the metrics did not gauge the quality, accuracy, or effectiveness of the system's intrusion detection and prevention capabilities. As a result, DHS was unable to describe the value provided by NCPS.

To enhance the functionality of NCPS, we made six recommendations to DHS, which if implemented, could help the agency to expand the capability of NCPS to detect cyber intrusions, notify customers of potential incidents, and track the quality, efficiency, and accuracy of supporting actions related to detecting and preventing intrusions, providing analytic services, and sharing cyber-related information. DHS concurred with the recommendations. In February 2017 when we followed up on the status of the recommendations, DHS officials stated that they have implemented 2 of the recommendations and initiated

actions to address the other 4 recommendations. We are in the process of evaluating DHS's actions for the two implemented recommendations.

In January 2016, we also reported that federal agencies had adopted NCPS to varying degrees. Specifically, the 23 civilian agencies covered by the *Chief Financial Officers (CFO) Act*[10] that were required to implement the intrusion detection capabilities had routed some traffic to NCPS intrusion detection sensors. However, as of January 2016, only 5 of the 23 agencies were receiving intrusion prevention services, due to certain policy and implementation challenges. For example, officials stated that the ability to meet DHS security requirements to use the intrusion prevention capabilities varied from agency to agency. Further, agencies had not taken all the technical steps needed to implement the system, such as ensuring that all network traffic was being routed through NCPS sensors. This occurred in part because DHS had not provided network routing guidance to agencies. As a result, it had limited assurance regarding the effectiveness of the system.

We recommended that DHS work with federal agencies and the Internet service providers to document secure routing requirements in order to better ensure the complete, safe, and effective routing of information to NCPS sensors. DHS concurred with the recommendation. When we followed up with DHS on the status of the recommendations, DHS officials said that nearly all of the agencies covered by the CFO Act are receiving at least one of the intrusion prevention services, as of March 2017. Further, the officials stated that DHS has collaborated with the Office of Management and Budget (OMB) to develop new guidance for agencies on perimeter security capabilities as well as alternative routing strategies. We will evaluate the network routing guidance when DHS finalizes and implements it.

Effective Implementation of the CDM Program Could Improve Information Security at Agencies

The CDM program provides federal agencies with tools and services that are intended to provide them with the capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. These tools include sensors that perform automated scans or searches for known cyber vulnerabilities, the results of which can feed

[10]31 U.S.C. 901(b).

into a dashboard that alerts network managers and enables the agency to allocate resources based on the risk.

DHS, in partnership with and through the General Services Administration, established a government-wide acquisition vehicle for acquiring continuous diagnostics and mitigation capabilities and tools. The CDM blanket purchase agreement is available to federal, state, local, and tribal government entities for acquiring these capabilities.

There are three phases of CDM implementation:

Phase 1: This phase involves deploying products to automate hardware and software asset management, configuration settings, and common vulnerability management capabilities. According to the *Cybersecurity Strategy and Implementation Plan*, DHS purchased Phase 1 tools and integration services for all participating agencies in fiscal year 2015.

Phase 2: This phase intends to address privilege management and infrastructure integrity by allowing agencies to monitor users on their networks and to detect whether users are engaging in unauthorized activity. According to the *Cybersecurity Strategy and Implementation Plan*, DHS was to provide agencies with additional Phase 2 capabilities throughout fiscal year 2016, with the full suite of CDM phase 2 capabilities delivered by the end of that fiscal year.

Phase 3: According to DHS, this phase is intended to address boundary protection and event management for managing the security life cycle. It focuses on detecting unusual activity inside agency networks and alerting security personnel. The agency planned to provide 97 percent of federal agencies the services they need for CDM Phase 3 in fiscal year 2017.

As we reported in May 2016,[11] most of the 18 agencies covered by the CFO Act that had high-impact systems[12] were in the early stages of CDM

[11]GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016). We surveyed the 18 agencies covered by the Chief Financial Officers (CFO) Act that reported having high-impact systems on a variety of information security-related issues including their implementation of government-wide security initiatives such as the CDM program.

implementation. All 17 of the civilian agencies[13] that we surveyed indicated they had developed their own strategy for information security continuous monitoring. Additionally, according to survey responses, 14 of the 17 had deployed products to automate hardware and software asset configuration settings and common vulnerability management. Further, more than half of the agencies noted that they had leveraged products/tools provided through the General Services Administration's acquisition vehicle. However, only 2 of the 17 agencies reported that they had completed installation of agency and bureau/component-level dashboards and monitored attributes of authorized users operating in their agency's computing environment. Agencies also noted that expediting the implementation of CDM phases could be of benefit to them in further protecting their high-impact systems.

The effective implementation of the CDM tools and capabilities can assist agencies in overcoming the challenges we have identified that they face when securing their information systems and information. As noted earlier, our audits often identify insecure configurations, unpatched or unsupported software, and other vulnerabilities in agency systems. We believe that the tools and capabilities available under the CDM program, when effectively used by agencies, can help them to diagnose and mitigate vulnerabilities to their systems. By continuing to make these tools and capabilities available to federal agencies, DHS can also have additional assurance that agencies are better positioned to protect their information systems and information.

Other DHS Services Are Available to Help Protect Systems, but Are Not Always Used by Agencies

DHS provides other services that could help agencies protect their information systems. Such services include, but are not limited to:

- *US-CERT monthly operational bulletins* are intended to provide senior federal government information security officials and staff with actionable information to improve their organization's cybersecurity

[12]High-impact systems are those where the loss of the confidentiality, integrity, or availability of the information or information system could be expected to have a severe or catastrophic adverse effect on organizations operations, assets, or personnel. For example, it might cause the organization to be unable to perform one or more of its primary functions or result in a major financial loss. Of the 24 CFO Act agencies, 18 reported having high-impact systems at the time of our review.

[13]The Department of Defense, one of the 18 agencies with high-impact systems, is not required to participate in the CDM program.

posture based on incidents observed, reported, or acted on by DHS and US-CERT.

- *CyberStat reviews* are in-depth sessions with National Security Staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and opportunities for collaboration. According to OMB, these interviews are face-to-face, evidence-based meetings intended to ensure agencies are accountable for their cybersecurity posture. The sessions are to assist the agencies in developing focused strategies for improving their information security posture in areas where there are challenges.
- *DHS Red and Blue Team exercises a*re intended to provide services to agencies for testing their systems with regard to potential attacks. A Red Team emulates a potential adversary's attack or exploitation capabilities against an agency's cybersecurity posture. The Blue Team defends an agency's information systems when the Red Team attacks, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group.

In May 2016, we reported that although participation varied among the 18 agencies we surveyed, most of those that chose to participate generally found these services to be useful in aiding the cybersecurity protection of their high-impact systems. [14] Specifically,

- 15 of 18 agencies participated in US-CERT monthly operational bulletins, and most found the service very or somewhat useful.
- All 18 agencies participated in the CyberStat reviews, and most found the service very or somewhat useful.
- 9 of 18 agencies participated in DHS' Red/Blue team exercises, and most found the exercises to be very or somewhat useful.

Half of the agencies in our survey reported that they wanted an expansion of federal initiatives and services to help protect their high-impact systems. For example, agencies noted that expediting the implementation of CDM phases, sharing threat intelligence information, and sharing attack vectors, could be of benefit to them in further protecting their high-impact systems. We believe that by continuing to make these services available to agencies, DHS will be better able to assist agencies in strengthening the security of their information systems.

[14]See GAO-16-501.

In conclusion, DHS is leading several programs that can benefit federal efforts to secure agency information systems and information. Two such programs, NCPS and CDM, offer the prospect of important advances in the security over federal systems. Enhancing NCPS's capabilities and greater adoption by agencies will help DHS achieve the full benefit of the system. Effective implementation of CDM functionality by federal agencies could better position them to protect their information technology resources from evolving and pernicious threats.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee, this concludes my statement. I would be happy to respond to your questions.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Christopher Businsky, Michael W. Gilmore, Nancy Glover, Jeff Knott, Kush K. Malhotra, Scott Pettis, David Plocher, and Angela D. Watson.