United States Government Accountability Office

Report to Congressional Committees

January 2016

INFORMATION SECURITY

DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System

GAO Highlights

Highlights of GAO-16-294, a report to congressional committees

January 2016

INFORMATION SECURITY

DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System

Why GAO Did This Study

Cyber-based attacks on federal systems continue to increase. GAO has designated information security as a government-wide high-risk area since 1997. This was expanded to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015. NCPS is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing.

Senate and House reports accompanying the 2014 Consolidated Appropriations Act included provisions for GAO to review the implementation of NCPS. GAO determined the extent to which (1) the system meets stated objectives, (2) DHS has designed requirements for future stages of the system, and (3) federal agencies have adopted the system. To do this, GAO compared NCPS capabilities to leading practices, examined documentation, and interviewed officials at DHS and five selected agencies. This is a public version of a report that GAO issued in November 2015 with limited distribution. Certain information on technical issues has been omitted from this version.

What GAO Recommends

GAO recommends that DHS take nine actions to enhance NCPS's capabilities for meeting its objectives, better define requirements for future capabilities, and develop network routing guidance. DHS concurred with GAO's recommendations.

View GAO-16-294. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov

What GAO Found

The Department of Homeland Security's (DHS) National Cybersecurity Protection System (NCPS) is partially, but not fully, meeting its stated system objectives:

- **Intrusion detection:** NCPS provides DHS with a limited ability to detect potentially malicious activity entering and exiting computer networks at federal agencies. Specifically, NCPS compares network traffic to known patterns of malicious data, or "signatures," but does not detect deviations from predefined baselines of normal network behavior. In addition, NCPS does not monitor several types of network traffic and its "signatures" do not address threats that exploit many common security vulnerabilities and thus may be less effective.
- **Intrusion prevention:** The capability of NCPS to prevent intrusions (e.g., blocking an e-mail determined to be malicious) is limited to the types of network traffic that it monitors. For example, the intrusion prevention function monitors and blocks e-mail. However, it does not address malicious content within web traffic, although DHS plans to deliver this capability in 2016.
- **Analytics:** NCPS supports a variety of data analytical tools, including a centralized platform for aggregating data and a capability for analyzing the characteristics of malicious code. In addition, DHS has further enhancements to this capability planned through 2018.
- **Information sharing:** DHS has yet to develop most of the planned functionality for NCPS's information-sharing capability, and requirements were only recently approved. Moreover, agencies and DHS 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 has developed metrics for measuring the performance of NCPS, they do not gauge the quality, accuracy, or effectiveness of the system's intrusion detection and prevention capabilities. As a result, DHS is unable to describe the value provided by NCPS.

Regarding future stages of the system, DHS has identified needs for selected capabilities. However, it had not defined requirements for two capabilities: to detect (1) malware on customer agency internal networks or (2) threats entering and exiting cloud service providers. DHS also has not considered specific vulnerability information for agency information systems in making risk-based decisions about future intrusion prevention capabilities.

Federal agencies have adopted NCPS to varying degrees. The 23 agencies required to implement the intrusion detection capabilities had routed some traffic to NCPS intrusion detection sensors. However, only 5 of the 23 agencies were receiving intrusion prevention services, but DHS was working to overcome policy and implementation challenges. Further, agencies have not taken all the technical steps needed to implement the system, such as ensuring that all network traffic is being routed through NCPS sensors. This occurred in part because DHS has not provided network routing guidance to agencies. As a result, DHS has limited assurance regarding the effectiveness of the system.

Contents

Tables

Figures

Abbreviations

CFO Act	Chief Financial Officers Act
CVE	common vulnerabilities and exposures
DHS	Department of Homeland Security
DNS	Domain Name System
FISMA 2002	Federal Information Security Management Act of 2002
IPv6	Internet Protocol version 6
IRS	Internal Revenue Service
MOA	memorandum of agreement
NCCIC	National Cybersecurity and Communications Integration Center
NCPS	National Cybersecurity Protection System
NIST	National Institute of Standards and Technology
NSD	Network Security Deployment
NVD	National Vulnerability Database
OMB	Office of Management and Budget
SCADA	supervisory control and data acquisition
SQL	Structured Query Language
US-CERT	United States Computer Emergency Readiness Team

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 28, 2016

The Honorable John Hoeven
Chairman
The Honorable Jeanne Shaheen
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable John Carter
Chairman
The Honorable Lucille Roybal-Allard
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

Cyber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive. This is illustrated by recently reported data breaches at the Office of Personnel Management, which affected millions of current and former federal employees. Protecting the information systems and the information that resides on them and effectively responding to cyber-incidents is critical to federal agencies because the unauthorized disclosure, alteration, and destruction of the information on those systems can result in great harm to those involved.

Due to the cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and the associated risks, we continue to designate information security as a government-wide high-risk area in our most recent biennial report to Congress, a designation we have made in each report since 1997.[1] In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure and we continued to do so in the most recent update

[1] See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

to our high-risk list. In the 2015 update, we further expanded this area to include protecting the privacy of personally identifiable information[2]—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities.

The National Cybersecurity Protection System (NCPS), designed and operated by the Department of Homeland Security (DHS), was developed to be one of the tools to aid federal agencies in mitigating information security threats. The system is to provide DHS with the capability to provide four cyber-related services to federal agencies: intrusion detection, intrusion prevention, analytics, and information sharing.[3]

Senate and House reports accompanying the Consolidated Appropriations Act, 2014, included provisions for us to review NCPS. Our objectives were to determine the extent to which (1) the system meets stated objectives, (2) DHS has designed requirements for future stages of the system, and (3) federal agencies have adopted the system.

This is a public version of a report we issued in November 2015 that was designated “for official use only” and released with limited distribution due to the sensitive nature of the material it contained. Certain information has been omitted. Although the information provided in this report is more limited in scope, it addresses the same objectives as the November 2015 report. Also, the overall methodology used for both reports is the same.

To determine the extent to which NCPS meets stated objectives, we compared NCPS’s four overarching capabilities to leading federal best

[2] Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, mother’s maiden name, or biometric records, and any other personal information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

[3] 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 exchanging of cyber threat and incident information.

practices related to intrusion detection, intrusion prevention, analytics, and information sharing. Further, we reviewed elements of each NCPS objective as well as intrusion detection incident notifications sent to five agencies: the Departments of Energy and Veterans Affairs, the General Services Administration, the National Science Foundation, and the Nuclear Regulatory Commission.[4]

To determine the extent to which DHS had designed requirements, we reviewed DHS's planning documentation and compared it to federal guidance issued by the Office of Management and Budget. In addition, for all new capabilities identified for funding in DHS's fiscal year 2016 funding request, we determined if formalized requirements had been documented and approved. Further, we determined if future capabilities plans for NCPS's intrusion prevention objective were developed using a risk-based approach, including threat, vulnerability, impact, and likelihood.

To determine the extent of federal adoption of NCPS, we reviewed DHS documentation and agreements to determine the adoption by the 23 non-defense agencies identified in the Chief Financial Officers Act. Additionally, we identified challenges to adoption by reviewing DHS program documentation and interviewing officials from DHS, the selected agencies identified above, and three Internet service providers participating in NCPS. See appendix I for additional details on our objectives, scope, and methodology.

We conducted this performance audit from June 2014 to January 2016 in accordance with 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 on our audit objectives. We believe that

[4] There are 24 agencies identified in the Chief Financial Officers Act: the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development. The customer agencies included for review were selected from 23 agencies identified in the Chief Financial Officers Act based on the number of DHS reported NCPS incident notifications sent to them during fiscal year 2014. The Department of Defense and members of the intelligence community do not participate in NCPS.

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, federal agencies have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. 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, deliver services to the public, and account for their resources without these cyber assets. Information security is thus especially important for federal agencies to ensure the confidentiality, integrity, and availability of their systems and data. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets, as the following examples illustrate:

- Computer resources could be used for unauthorized purposes or to launch attacks on other computer systems.
- Sensitive information, such as personally identifiable information, intellectual property, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other types of crime.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.
- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

The Nation Faces an Evolving Array of Cyber-Based Threats

Threats to systems are evolving and growing. Cyber threats can be unintentional or intentional. Unintentional or non-adversarial threats sources include failures in equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters. They also include natural disasters and failures of critical infrastructure on which the organization depends but are outside of the control of the organization. Intentional or adversarial threats include individuals, groups, entities, or nations that seek to leverage the organization’s dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies). Threats can come from a wide array of sources, including corrupt employees, criminal groups, and terrorists. These threat adversaries vary in terms of their capabilities, their willingness to act, and their motives, which can include seeking monetary gain, or seeking an economic, political, or military advantage. Table 1 describes the sources of cyber based threats in more detail.

Table 1: Common Cyber Threat Sources

Source	Description
Non-adversarial/non-malicious	
Failure in information technology equipment	Failures in displays, sensors, controllers, and information technology hardware responsible for data storage, processing, and communications.
Failure in environmental controls	Failures in temperature/humidity controllers or power supplies.
Failures in software	Failures in operating systems, networking, and general-purpose and mission-specific applications.
Natural or man-made disaster	Events beyond an entity's control such as fires, floods, tsunamis, tornados, hurricanes, and earthquakes.
Unusual or natural event	Natural events beyond the entity's control that are not considered disasters (e.g., sunspots).
Infrastructure failure or outage	Failure or outage of telecommunications or electrical power.
Unintentional user errors	Failures resulting from erroneous accidental actions taken by individuals (both system users and administrators) in the course of executing their everyday responsibilities.
Adversarial	
Hacker/hacktivist	Hackers break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals.
Malicious insiders	Insiders (e.g., disgruntled organization employees, including contractors) may not need a great deal of knowledge about computer intrusions because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. These individuals engage in purely malicious activities and should not be confused with non-malicious insider accidents.
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned programs use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities.
Criminal groups and organized crime	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence.
Unknown malicious outsiders	Unknown malicious outsiders are threat sources/agents that, due to a lack of information, remain anonymous and are unable to be classified as one of the five types of threat sources/agents listed above.

Source: GAO analysis of unclassified government and nongovernment data. | GAO-16-294

Cyber threat adversaries make use of various techniques, tactics, and practices, or exploits, to adversely affect an organization's computers, software, or networks, or to intercept or steal valuable or sensitive information. These exploits are carried out through various conduits, including websites, e-mails, wireless and cellular communications, Internet protocols, portable media, and social media. Further, adversaries can leverage common computer software programs, such as Adobe Acrobat and Microsoft Office, as a means by which to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program. Table 2 provides descriptions of common exploits or techniques, tactics, and practices used by cyber adversaries.

Table 2: Common Methods of Cyber Exploit

Method of exploit	Descriptions
Watering hole	A method by which threat actors exploit the vulnerabilities of websites frequented by users of the targeted system. Malware is then injected to the targeted system via the compromised websites.
Phishing and spear phishing	A digital form of social engineering that uses authentic-looking e-mails, websites, or in**st**ant messages to get users to download malware, open malicious attachments, or open links that direct them to a website that requests information or executes malicious code.
Credentials based	An exploit that takes advantage of a system's insufficient user authentication and/or any elements of cyber-security supporting it, to include not limiting the number of failed login attempts, the use of hard-coded credentials, and the use of a broken or risky cryptographic algorithm.
Trusted third parties	An exploit that takes advantage of the security vulnerabilities of trusted third parties to gain access to an otherwise secure system.
Classic buffer overflow	An exploit that involves the intentional transmission of more data than a program's input buffer can hold, leading to the deletion of critical data and subsequent execution of malicious code.
Cryptographic weakness	An exploit that takes advantage of a network employing insufficient encryption when either storing or transmitting data, enabling adversaries to read and/or modify the data stream.
Structured Query Language (SQL) injection	An exploit that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database resulting in data loss or corruption, denial of service, or complete host takeover.
Operating system command injection	An exploit that takes advantage of a system's inability to properly neutralize special elements used in operating system commands, allowing adversaries to execute unexpected commands on the system by either modifying already evoked commands or evoking their own.
Cross-site scripting	An exploit that uses third-party web resources to run lines of programming instructions (referred to as scripts) within the victim's web browser or scriptable application. This occurs when a user, using a browser, visits a malicious website or clicks a malicious link. The most dangerous consequences can occur when this method is used to exploit additional vulnerabilities that may permit an adversary to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, or remotely access and control the victim's machine.

Method of exploit	Descriptions
Cross-site request forgery	An exploit that takes advantage of an application that cannot, or does not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request, tricking the victim into executing a falsified request that results in the system or data being compromised.
Path traversal	An exploit that seeks to gain access to files outside of a restricted directory by modifying the directory pathname in an application that does not properly neutralize special elements (e.g., '…', '/', '…/') within the pathname.
Integer overflow	An exploit where malicious code is inserted that leads to unexpected integer overflow, or wraparound, which can be used by adversaries to control looping or make security decisions in order to cause program crashes, memory corruption, or the execution of arbitrary code via buffer overflow.
Uncontrolled format string	Adversaries manipulate externally controlled format strings in print-style functions to gain access to information and execute unauthorized code or commands.
Open redirect	An exploit where the victim is tricked into selecting a URL (website location) that has been modified to direct them to an external, malicious site which may contain malware that can compromise the victim's machine.
Heap-based buffer overflow	Similar to classic buffer overflow, but the buffer that is overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a memory allocation routine, such as "malloc ()".
Unrestricted upload of files	An exploit that takes advantage of insufficient upload restrictions, enabling adversaries to upload malware (e.g., .php) in place of the intended file type (e.g., .jpg).
Inclusion of functionality from un-trusted sphere	An exploit that uses trusted, third-party executable functionality (e.g., web widget or library) as a means of executing malicious code in software whose protection mechanisms are unable to determine whether functionality is from a trusted source, modified in transit, or being spoofed.
Certificate and certificate authority compromise	Exploits facilitated via the issuance of fraudulent digital certificates (e.g., transport layer security and Secure Socket Layer). Adversaries use these certificates to establish secure connections with the target organization or individual by mimicking a trusted third party.
Hybrid of others	An exploit which combines elements of two or more of the aforementioned techniques.

Source: GAO analysis of unclassified government and nongovernment data. | GAO-16-294

Reports of successfully executed cyber exploits illustrate the debilitating effects they can have on the nation's security and economy, and on public health and safety. Further, federal agencies have experienced security breaches in their networks, potentially allowing sensitive information to be compromised and systems, operations, and services to be disrupted. These examples illustrate that a broad array of federal information and critical infrastructures are at risk:

- In August 2015, the Internal Revenue Service (IRS) reported that approximately 390,000 tax accounts were potentially affected by unauthorized third parties gaining access to taxpayer information from the agency's "Get Transcript" application. According to testimony from the Commissioner of the IRS in June 2015, criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information; however, at that time, he reported that approximately 100,000 tax accounts had been affected. These data included Social Security information, dates of birth, and street addresses.

- In July 2015, the Office of Personnel Management reported that an intrusion into its systems compromised the background investigation files of 21.5 million individuals. This was in addition to a separate but related incident that affected personnel records of about 4 million current and former federal employees, which the agency announced in June 2015.
- In September 2014, a cyber-intrusion into the United States Postal Service's information systems may have compromised personally identifiable information for more than 800,000 of its employees.

Federal Law and Policy Provide a Framework for Securing Federal Information and Systems

The Federal Information Security Management Act of 2002 (FISMA 2002)[5] was enacted into law to provide a comprehensive framework for ensuring the effectiveness of information security controls over federal information resources. The law required 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. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and procedures; plans for providing adequate information security for networks, facilities, and systems; providing security awareness and specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; procedures for detecting, reporting, and responding to security incidents; and ensuring continuity of operations. The act also assigned oversight responsibilities to the Office of Management and Budget (OMB) and gave the National Institute of Standards and Technology (NIST) responsibility for developing standards and guidelines that include minimum information security requirements.

The Federal Information Security Modernization Act of 2014 largely supersedes FISMA 2002.[6] This law retains the requirements for agencies

[5] FISMA 2002 was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

[6] Pub. L. No. 113-283 (Dec. 18, 2014).

to develop, document, and implement an agency-wide information security program, as well as OMB oversight and NIST development of standards and guidelines. Its changes include requiring DHS to assist OMB with providing oversight by administering the implementation of information security policies and practices for information systems. DHS responsibilities include

- developing and overseeing the implementation of binding operational directives requiring agencies to implement OMB's information security standards and guidelines;
- operating a federal information security incident center (previously OMB's responsibility), which has been established as the DHS United States Computer Emergency Readiness Team (US-CERT);[7]
- deploying technology, upon request by an agency, to continuously diagnose and mitigate against cyber threats and vulnerabilities; and
- conducting targeted operational evaluations, including threat and vulnerability assessments, on agency information systems.

In January 2008, the President issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23. The directive established the Comprehensive National Cybersecurity Initiative, a set of projects with the objective of safeguarding federal executive branch government information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats against the federal government's networks.[8] Under the initiative, DHS was to lead several projects to better secure civilian federal government networks, while other agencies, including OMB, the Department of Defense, and the Office of the Director of National Intelligence had key roles in other projects, including monitoring military systems and classified networks, overseeing intelligence community systems and

[7] Established by DHS, the US-CERT serves as a focal point for the government's interaction with federal and nonfederal entities on a 24-hour-a-day, 7-day-a-week basis regarding cyber-related analysis, warning, information sharing, major incident response, and national-level recovery efforts. It is charged with aggregating and disseminating cybersecurity information to improve warning of and response to incidents, increasing coordination of response information, reducing vulnerabilities, and enhancing prevention and protection. In addition, US-CERT collects incident reports from all federal agencies and assists agencies in their incident response efforts.

[8] GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338 (Washington, D.C.: Feb. 1, 2010).

networks, and spearheading advanced technology research and development. The initiative's projects can be grouped into three focus areas:

- *Establishing front lines of defense*. This includes projects intended to protect the perimeter of federal networks, such as consolidating connections and deploying intrusion detection and prevention systems.
- *Defending against full spectrum of threats*. This includes physical and cyber projects intended to protect national security and intelligence-related information and systems across the federal government.
- *Shaping the future environment*. The initiatives in this area are focused on expanding cybersecurity education and research and development efforts for future technologies and cybersecurity strategies.

As required by FISMA (both the 2002 and 2014 laws), NIST has developed standards and guidelines for agencies to develop, document and implement their required information security programs, select controls for systems,[9] and conduct risk-based cyber threat mitigation activities. For example, NIST's Special Publication 800-37 recommends cost-effectively reducing information security risks to an acceptable level and ensuring that information security is addressed throughout an information system's life cycle.[10] In addition, NIST Special Publication 800-94 establishes guidance for federal agencies to use when designing, implementing, and maintaining the systems they deploy to perform intrusion detection and prevention.[11]

[9] See, for example, NIST, Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication (SP) 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

[10] NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication (SP) 800-37, Revision 1 (Gaithersburg, Md.: Feb. 2010).

[11] NIST, *Guide to Intrusion Detection and Prevention Systems*, SP 800-94 (Gaithersburg, Md.: February 2007).

DHS's Actions Supporting Cybersecurity of the Federal Network Enterprise

DHS designated the National Protection and Programs Directorate to lead the national effort to strengthen the security and resilience of the nation's physical and cyber-critical infrastructure, including supporting federal agencies in securing their information systems and information. Specifically, the directorate is responsible for enhancing the security, resilience, and reliability of federal agencies in the protection of the ".gov" domain of the federal civilian government.

Within the National Protection and Programs Directorate, the Office of Cybersecurity and Communications, among other things, operates the National Cybersecurity and Communications Integration Center (NCCIC) that is to serve as a 24/7 cyber monitoring, incident response, and management center and as a national focal point of cyber and communications incident integration.[12] The US-CERT, one of several subcomponents of the NCCIC, is responsible for operating the NCPS, which provides intrusion detection and prevention capabilities to covered federal agencies. The Network Security Deployment (NSD) division of the Office of Cybersecurity and Communications is responsible for developing, deploying, and sustaining NCPS. For example, the division is to deliver NCPS intrusion detection capability directly to federal agencies through Trusted Internet Connection Access Providers or through Internet service providers at Managed Trusted Internet Protocol Service locations.[13]

[12] DHS has established an extensive privacy framework to ensure that none of the activities associated with NCPS are infringing on the privacy rights of individuals. Specific review of the privacy controls associated with the system was outside the scope of this review.

[13] In November 2007, OMB issued M-08-05 that announced the Trusted Internet Connections Initiative, which is intended to improve security by reducing and consolidating external network connections and by providing centralized monitoring at a select group of access providers. The DHS's Office of Cybersecurity and Communications was designated as the coordinator of the initiative. Agencies may serve as their own access provider, also referred to as a Trusted Internet Connection Access Provider or by obtaining services from another source. Agencies may choose one of four service options: (1) Single service (i.e. the agency provides services to its own bureaus and components only); (2) Multi-service (i.e. the agency provides services to its own bureaus and components as well as to other agencies); (3) Seeking service (i.e. the agency obtains services from a multi-service agency or through the General Services Administration-managed Networx program); or (4) Hybrid (i.e. the agency both provides services to its own bureaus and components and obtains additional services from a Networx provider.

National Cybersecurity Protection System

NCPS is an integrated system-of-systems that is intended to deliver a range of capabilities, including intrusion detection, intrusion prevention, analytics, and information sharing. The NCPS capabilities, operationally known as the Einstein program, are one of a number of tools and capabilities that assist in federal network defense. Originally created in 2003, NCPS is intended to aid DHS in its ability to help reduce and prevent computer network vulnerabilities across the federal government. Its analysts examine raw and summarized data from a wide variety of information sources to make determinations about potential attacks across the network traffic of participating federal agencies detected by NCPS. Table 3 provides an overview of the enhancements DHS has made to the original iteration of Einstein as well as the corresponding objective of NCPS the functionality supports.

Table 3: Overview of 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 executive branch 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-16-294

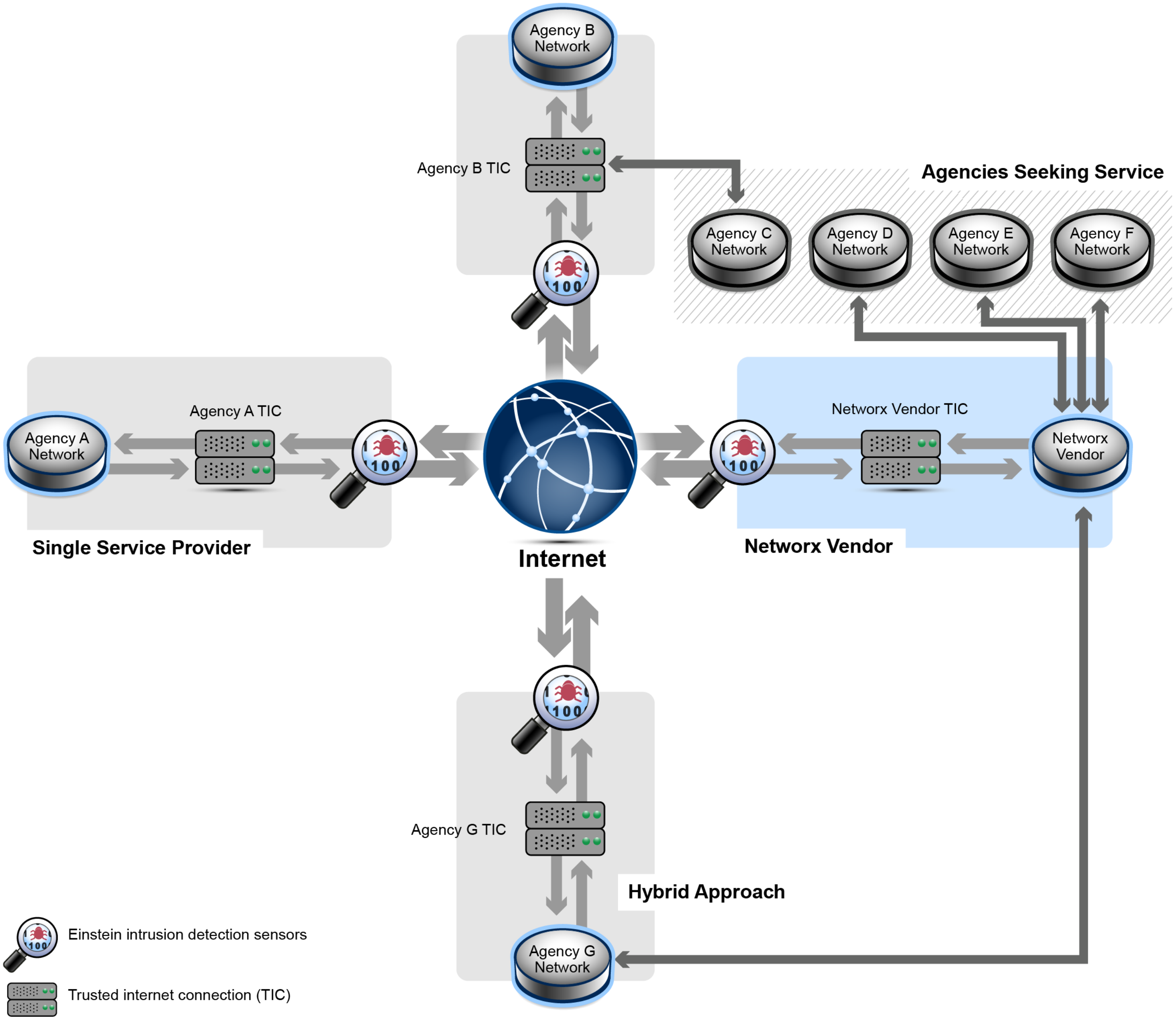
[a] The network traffic information includes source and destination Internet Protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

[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.

NCPS is intended to build successive layers of defense mechanisms into the federal government's information technology infrastructures. When NCPS intrusion detection sensors are deployed at a Trusted Internet Connection location, the system monitors inbound and outbound network traffic, with the goal of allowing US-CERT, using NCPS and its supporting processes, to monitor all traffic passing between the federal civilian networks and the Internet for malicious activity. Figure 1 illustrates how Trusted Internet Connection portals interact with the NCPS intrusion detection sensors and the Internet. For more detailed information about NCPS's development and functionality, see appendix II.

Figure 1: Interaction of Trusted Internet Connection and NCPS Intrusion Detection Sensors

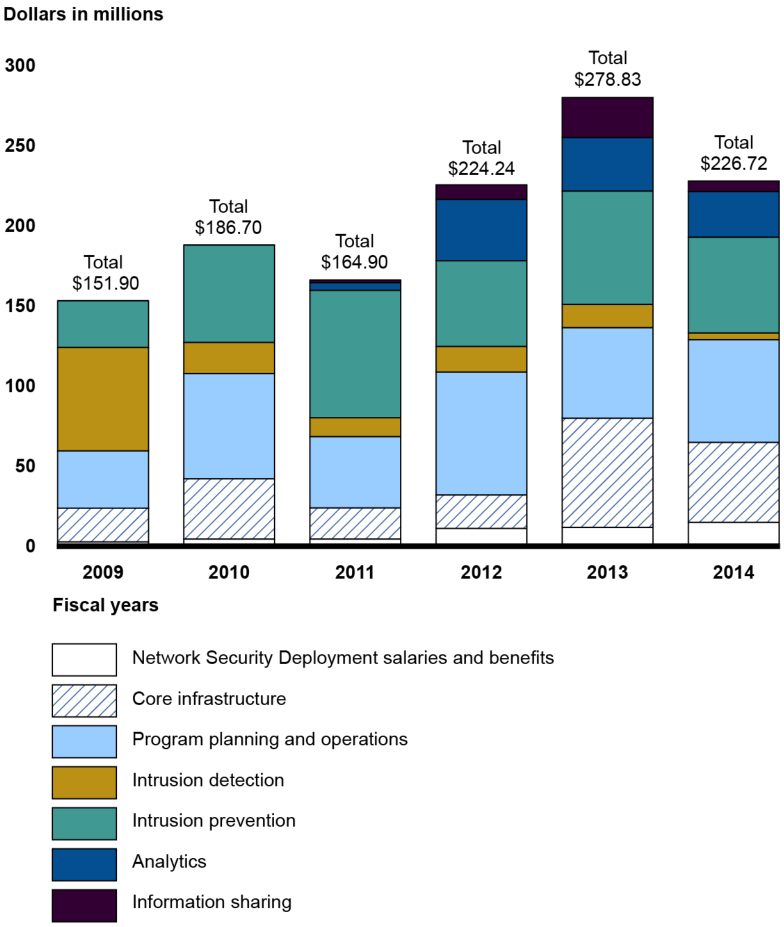


Source: GAO analysis of Department of Homeland Security data. | GAO-16-294

NCPS Expenditures through Fiscal Year 2014

As we reported in April 2015,[14] DHS spent over $1.2 billion on the NCPS system through fiscal year 2014. Figure 2 below depicts the funds spent for NCPS over the past 6 budget years.

Figure 2: NSD National Cybersecurity Protection System Expenditures to Date



Source: GAO analysis of unaudited Department of Homeland Security expenditure data. | GAO-16-294

[14] GAO, *Homeland Security Acquisitions: Major Program Assessments Reveal Actions Needed to Improve Accountability*, GAO-15-171SP (Washington, D.C.: April 22, 2015).

NSD plans to use the fiscal year 2015 funding to sustain currently deployed capabilities and expand intrusion prevention, information-sharing, and analytics capabilities of NCPS. As of April 2015, the projected total life-cycle cost of the program was approximately $5.7 billion, through fiscal year 2018.

NCPS Is Not Fully Satisfying All Intended System Objectives

The overarching objectives of NCPS are to provide functionality that supports intrusion detection, intrusion prevention, analytics, and information sharing. While NCPS's ability to detect and prevent intrusions, analyze network data, and share information is useful, its capabilities are limited. For example, NCPS detects signature-based anomalies, but does not employ other, more complex methodologies and cannot detect anomalies in certain types of traffic. Further, the intrusion prevention capabilities can currently mitigate threats to a limited subset of network traffic. Regarding NCPS's analytics function, DHS has deployed aspects of this capability and plans to develop more complex tools. However, information sharing, which is the fourth stated objective, has only recently been approved and funded for development; thus, current information sharing efforts are manual and largely ad hoc. In addition, although DHS established a variety of NCPS-related metrics, none provide insight into the value derived from the functions of the system. Developing such metrics poses a challenge for the agency, according to DHS officials. Until NCPS's intended capabilities are more fully developed, DHS will be hampered in its abilities to provide effective cybersecurity-related support to federal agencies.

NCPS Has Limited Ability to Detect Intrusions within Observed Network Traffic

NCPS's intrusion detection capability is intended to provide DHS with the ability to scan network traffic for signs of potentially malicious activity. Effective intrusion detection provides an organization with the ability to detect abnormalities within network traffic and can be accomplished through the use of multiple types of intrusion detection methodologies. In order to more comprehensively and accurately detect malicious activity, NIST recommends[15] using a combination of three detection methodologies: signature-based, anomaly-based, and stateful purpose analysis.

[15] NIST 800-94.

- Signature-based intrusion detection is able to detect malicious traffic by comparing current traffic to known patterns of malicious behavior, also referred to as signatures. This method is considered effective at detecting known threats and is the simplest form of intrusion detection, because it can only match against known patterns of malicious traffic.
- The anomaly-based and stateful purpose detection methodologies are more complex approaches, which involve comparing current network activity to predefined baselines of “normal behavior” to identify deviations which could be indicative of malicious activity. These approaches to intrusion detection are more effective than signature-based detection at identifying previously unknown threats, such as “zero-days,”[16] as well as variants to known threats and threats disguised by the use of evasion techniques.

NCPS uses only a signature-based methodology for detecting malicious activity. According to US-CERT officials, NCPS’s intrusion detection capability is supported by 228 intrusion detection sensors placed throughout the .gov network infrastructure. The sensors provide a flow of network traffic to be analyzed. Officials added that there are over 9,000 intrusion detection signatures deployed within NCPS, with approximately 2,300 that are enabled and being used to evaluate traffic at any given time. A majority of the signatures are available through commercially available products, though a portion is custom developed.

According to DHS documentation and NSD officials, NCPS was always intended to be a signature-based intrusion detection system, and thus it does not have the ability to employ multiple intrusion detection methodologies. Further, NSD and US-CERT officials stated that NCPS is just one of the many tools available to federal agencies to help enhance their cybersecurity posture. They stated that it is the responsibility of each agency to ensure their networks and information systems are secure while it is the responsibility of DHS to provide a baseline set of protections and government-wide situational awareness, as part of a defense-in-depth information security strategy.

By employing only signature-based intrusion detection, NCPS is unable to detect intrusions for which it does not have a valid or active signature

[16] A “zero day” is able to exploit an existing vulnerability in a product for which the vendor has not released an official fix or patch.

deployed. This limits the overall effectiveness of the program. Moreover, given that many federal agencies use commercially available signature-based intrusion detection systems to support their information security efforts, the addition of another signature-based intrusion detection system may do little to provide customer agencies with a baseline set of protections. DHS officials acknowledged that the intrusion detection systems used by many federal agencies likely have more signatures deployed than NCPS. Thus, the agencies' intrusion detection systems would be able to compare their network traffic against a larger set of potential exploits, such as exploits that US-CERT determined no longer needed to be scanned by NCPS. In other cases, US-CERT officials stated, some agencies do not possess their own robust intrusion detection capability and thus rely more on the intrusion detection functionality provided by NCPS.

Regarding zero-day exploits, US-CERT officials stated there is no way to identify them until they are announced. Once they are announced, US-CERT can develop a signature, as was the case with Adobe Flash exploits that were recently publicly announced.[17] While there are sources that can be used to buy zero day exploits, officials stated that DHS does not pay for zero days. Occasionally, US-CERT will receive notifications of exploits from partners before they go public, but these are mostly malware notifications. While we acknowledge the challenge of developing signatures for zero-day exploits, enhancing NCPS's current intrusion detection approach to include functionality that would support the development of a baseline of network behavioral analysis,[18] as described in NIST 800-94, would enhance DHS's ability to combat such threats.

NCPS Is Unable to Detect Exploits across All Types of Network Traffic

According to NIST, many intrusion detection products have the ability to detect attacks carried out through various types of network traffic, such as traffic related to network browsers, e-mail, and file transfer, as well as

[17] US-CERT issued an alert in July 2015 that identified newly discovered vulnerabilities associated with Adobe Flash. These vulnerabilities could allow a remote attacker to execute arbitrary code with system privileges. Based on the identification of these vulnerabilities, related signatures could then be developed to be part of the NCPS signature set.

[18] A network behavior analysis system examines network traffic or statistics on network traffic to identify unusual traffic flows, such as distributed denial of service attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems).

traffic related to supervisory control and data acquisition (SCADA) control systems.[19] In addition, intrusion detection systems should also have the ability to detect malicious activity across multiple layers of network protocols, including Internet Protocol Version 6 (IPv6).[20] Further, NIST states that some intrusion detection products have the ability to detect characteristics of encrypted traffic (i.e., whether encryption had been applied) but not evaluate the traffic itself. Adversaries will often use encryption to mask malicious traffic to help better facilitate the successful execution of cyber-exploits, such as zero-day attacks.

However, NCPS is not currently evaluating all types of network traffic. NSD and US-CERT officials stated there are currently no signatures deployed with NCPS that will detect threats embedded in certain types of network traffic.

US-CERT officials stated that they have not deployed signatures related to these additional types of network traffic for various reasons. They stated that NCPS customer departments and agencies have not been clear on the details of the specific types of network traffic present within their organizations or the amount of traffic allowed to pass through their network gateways. According to an NSD official, they initially collect such data and hold meetings with officials from customer departments and agencies to exchange technical information, but the departments and agencies are responsible for routing network traffic to the NCPS sensors and not required to keep DHS abreast of changes. In addition, US-CERT

[19] SCADA is one type of control system, which is a computer-based system used within many infrastructures and industries to monitor and control sensitive processes and physical functions. Control systems perform functions that range from simple to complex. They can be used to simply monitor processes--for example, the environmental conditions in a small office building--or to manage the complex activities of a municipal water system or a nuclear power plant. Control systems are vulnerable to cyber-attack from inside and outside the control system network.

[20] In September 2010, the federal chief information officer issued a memorandum for agency chief information officers stating that the federal government is committed to the operational deployment and use of IPv6, and in July 2012, the Federal Chief Information Officer Council Strategy and Planning Committee issued a roadmap toward IPv6 adoption within the government. The roadmap stated that though both IPv4 (the legacy version of IP) and IPv6 are being used on the Internet, IPv4 is, by far, still the dominate protocol because of its legacy deployment. However, IPv6 traffic growth is inevitable due to the current state of IPv4 address exhaustion, creating an extreme supply and demand curve and required to support communications between the U.S. government and its citizens and business partners worldwide.

officials stated that they have not conducted a detailed analysis of customer departments' and agencies' traffic to gain this understanding. Further, US-CERT officials stated that they were not equally concerned with the risk posed by all types of network traffic.

Without an ability to analyze all types of traffic, DHS is unable to detect threats embedded in such traffic and increases the risk that agencies could be negatively impacted by such threats.

Current NCPS Signatures Do Not Address Selected Common Vulnerabilities

According to NIST, signature-based intrusion detection systems depend on the quality of the signatures contained within them, and thus need to be updated to reflect new vulnerabilities and exploits that emerge.[21] Organizations can purchase signatures from commercial vendors, custom develop them, or obtain them from open sources. NIST maintains the National Vulnerability Database (NVD), which is an open source of information that can influence many information security activities, including the development of intrusion detection signatures. Federal agencies are encouraged to use the information contained within the database as part of their information security efforts.[22]

In addition, US-CERT has acknowledged the importance of incorporating the use of common vulnerabilities and exposures (CVE) information in information security activities. In April 2015 US-CERT issued an alert which stated that cyber threat adversaries continue to exploit unpatched software products from vendors such as Adobe, Microsoft, and Oracle. Vulnerabilities in these products are often a common vector for spear phishing attacks. The alert stated that as many as 85 percent of these attacks are preventable through the implementation of patches. Accordingly, the bulletin contained 30 of the top targeted vulnerabilities

[21] NIST 800-94.

[22] The NVD is the U.S. government repository of standards-based vulnerability management data. These data enable automation of vulnerability management, security measurement, and compliance. The NVD is built upon a list of common vulnerabilities and exposures (CVE), which is a free, publically available, open-source dictionary of information security vulnerabilities and exposures. According to NIST, the NVD contains the information contained within the common vulnerabilities and exposures dictionary augmented with additional analysis, a database, and a fine-grained search engine. The NVD is a superset of common vulnerabilities and exposures data, synchronized such that any updates to the common vulnerabilities appear immediately on the NVD. The goal of the NVD is to provide common names for publicly known cybersecurity issues by helping correlate data between different vulnerability or security tools, repositories, and services.

and associated CVE information that security officials could use to implement within their organizations.

However, the signatures supporting NCPS's intrusion detection capability only identify a portion of vulnerabilities associated with common software applications from vendors such as Adobe, Microsoft, and Oracle. Specifically, we found that NCPS had limited coverage[23] of vulnerabilities associated with 10 common client and server applications we evaluated.[24] At the time of our review, NCPS intrusion detection capability signatures provided:

- reasonable coverage for 1 vulnerability,[25]
- partial coverage for 7 vulnerabilities,[26] and
- no coverage for 2 vulnerabilities.[27]

Further, for the 12 advanced persistent threats[28] we evaluated, NCPS's intrusion detection capability had signatures that at the time of our review provided:

[23] We define coverage as the extent to which a signature would or would not provide NCPS with the means to detect the associated vulnerability.

[24] Under the traditional Internet client/server model, the access to information and services is accomplished by the interaction between users (clients) and servers—usually Web sites or portals. A client is defined as a requester of services, and a server is defined as the provider of services. Applications on both client and server machines would have vulnerabilities that are susceptible to potential exploitation, if not properly patched.

[25] We made a determination of reasonable coverage if DHS provided evidence that the particular signature(s) provided a sufficient means for NCPS to detect the associated vulnerability.

[26] We made a determination of partial coverage if DHS provided evidence indicating that the particular signature or combination of signatures provided NCPS with some but not all of the means to effectively detect a particular vulnerability.

[27] We made a determination of no coverage if DHS could provide no evidence for a particular signature or combination of signatures supported NCPS's ability to effectively detect a particular vulnerability.

- reasonable coverage for 8 advanced persistent threats, and
- partial coverage for 4 advanced persistent threats.

More specifically, for the five client applications we reviewed (Adobe Acrobat, Flash, Internet Explorer, Java, and Microsoft office), the NCPS intrusion detection signatures provided some degree of coverage for approximately 6 percent of the total vulnerabilities selected for review (i.e., 29 of 489), with coverage for specific applications ranging from 1.2 to 80 percent of vulnerabilities identified in CVE reports published during 2014.

Further, it is unknown how, if at all, US-CERT plans to leverage vulnerability data from other DHS sources to influence the development of intrusion detection signatures. For example, the Federal Network Resilience division is responsible for managing the Continuous Diagnostics and Mitigation program.[29] The vulnerability information garnered from this program could be used to develop signatures that would target exploits that are affecting many federal agencies. US-CERT officials stated that they plan to use this information to influence NCPS, but could not provide specific details as how they plan to accomplish this due to the relative immaturity of the Continuous Diagnostics and Mitigation program.

One reason that the signatures did not cover all identified vulnerabilities is that the current tool DHS uses to manage and track the status of intrusion detection signatures deployed within NCPS does not have the ability to

[28] According to NIST, an advanced persistent threat can be an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (1) pursues its objectives repeatedly over an extended period of time; (2) adapts to defenders' efforts to resist it; and (3) is determined to maintain the level of interaction needed to execute its objectives.

[29] According to DHS, the Continuous Diagnostics and Mitigation program is intended to provide federal agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These tools include sensors that perform automated searches for known cyber vulnerabilities, the results of which feed into a dashboard that alerts network managers. These alerts can be prioritized, enabling agencies to allocate resources based on risk. This information could be a source of valuable vulnerability information.

capture CVE information. US-CERT officials stated that when they developed the Signature Management System tool, they were not required to create a link between a signature and a published CVE data. However, US-CERT has acknowledged this deficiency and stated this is something it plans to address in the future.

In addition, US-CERT officials agreed with the results of our analysis of client vulnerabilities, but reiterated that the goal of NCPS was not to protect against all vulnerabilities. US-CERT officials stated that agencies with their own internal intrusion detection systems would likely be able to comprehensively address the common client vulnerabilities we selected. US-CERT officials stated that the overall intent of the system was to protect against nation-state level threat actors who often leverage "zero-day" exploits which may not have had a known mitigation or specific CVE assigned. Accordingly, officials stated, they must consider input from a variety of classified and unclassified sources, in addition to open source data such as CVEs, when developing their intrusion detection signatures. However, NCPS did not possess intrusion detection signatures that fully addressed all the advanced persistent threats we reviewed, which are often a type of exploit leveraged by nation-state actors.

US-CERT officials added that they must consider a variety of factors when deciding which specific signatures to deploy and the length of time they keep the signatures active. For example, the current version of the software managing the intrusion detection function does not allow for custom rules at each sensor. As a result, the signatures deployed must be uniform across all sensors and cannot be tailored to a specific agency. This adds an additional layer of complexity when deciding how long to deploy signatures. For example, a smaller agency may be unaware of a particular threat or associated signature, and thus could benefit from having that signature deployed longer than a larger agency, which may view it as potentially duplicative of signatures employed by its own internal intrusion detection tool. Officials stated that they expect this issue to be addressed when they upgrade to the next version of the software that manages the intrusion detection function.

We acknowledge that NCPS's intrusion detection capabilities draw on many sources of vulnerability information and it should not necessarily duplicate capabilities that agencies already possess. However, updating the tool used to manage NCPS signatures to draw on and more clearly link to publicly available, open-source repositories of vulnerability information, such as the NVD, and using data from the Continuous Diagnostic and Mitigation program as they become available as an input into the development and management of signatures could add value by minimizing the risk that known vulnerabilities will be exploited.

NCPS Intrusion Prevention Capability Is Limited, but Further Enhancements Are Planned

NCPS's ability to provide intrusion prevention is another key objective of the system. Intrusion prevention is an additional technique recommended by NIST in support of effective information system monitoring. When fully developed, NCPS will have the ability to proactively mitigate threats across multiple types of network traffic. This is important because malicious actors can propagate threats across multiple vectors and types of network traffic.

NCPS's intrusion prevention capability provides DHS with the ability to proactively address network-based threats before they can potentially cause harm to federal networks. This is accomplished by monitoring network traffic to and from a customer agency's network and taking some action to stop traffic (e.g., blocking an e-mail) that has characteristics matching pre-defined indicators of malicious traffic.[30]

NCPS has the ability to prevent intrusions in near real time, but is currently only able to proactively mitigate threats across a limited subset of network traffic (i.e., Domain Name System, or DNS, blocking and e-mail filtering) at a selected group of customer agencies. Consequently, there are other types of network traffic (e.g., web content), which are common vectors of attack not currently being analyzed for potentially malicious content.

NSD officials noted that initial capabilities for intrusion prevention were intended to be more robust, but were scaled back due to a change in the program's approach. Specifically, these officials stated that the original intent of the intrusion prevention deployment was to protect all types of network traffic with classified indicators. Further, the solution was supposed to provide government-furnished equipment to Internet service provider networks as the backbone of the intrusion prevention function of NCPS. However, NSD officials stated that, due to the excessive costs of operating and maintaining the original solution, the agency decided in

[30] 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 classified or unclassified.

May 2012 to change approaches. The new approach follows a managed service model, where the Internet service providers would receive classified indicators within their appropriate facilities and manage the prevention for their particular customer agencies. Because of this managed service model approach, NSD officials stated that the first set of prevention capabilities was based in part on the existing solutions provided by commercial service providers under the Defense Industrial Base Opt-In pilot (later renamed the Enhanced Cybersecurity Services).[31] Officials also added that another motivation for the new approach was to create a cybersecurity marketplace where the various Internet service providers would compete with each other to provide better cybersecurity solutions for federal customers.

DHS officials stated that they are developing prevention capabilities for other types of network traffic. Specifically, NSD officials stated that they plan to introduce the ability to filter web content by January 1, 2016. A review of a recent monthly report from one of the Internet service providers supporting NCPS intrusion prevention indicated that the contractor has begun work on web content filtering and provided DHS with a draft report on the indicators and overall process.

DHS Has Developed Aspects of the NCPS Analytics Capability

Another key objective of NCPS is to provide DHS with an analytics capability. NIST recommends that organizations take a variety of actions with respect to analytics, including

[31] Enhanced Cybersecurity Services is a program similar to NCPS that DHS is also responsible for administering. The program provides voluntary information sharing that is intended to assist U.S.-based public and private entities across all 16 critical infrastructure sectors defined by federal policy as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops cyber threat indicators based on this information and shares them with qualified Internet service providers, thus enabling them to better protect their customers. Enhanced Cybersecurity Services augments, but does not replace entities’ existing cybersecurity capabilities. The program does not involve government monitoring of private networks or communications. Under the program, information relating to threats and malware activities detected by the Internet service providers is not directly shared between the critical infrastructure Internet service provider customers and the government. However, when an Internet service provider customer voluntarily agrees, the provider may share limited and anonymized information with Enhanced Cybersecurity Services.

- analyzing and correlating audit records across different repositories to gain organization-wide situational awareness,
- correlating information from nontechnical sources with audit information to enhance organization-wide situational awareness,
- analyzing the characteristics of malicious code, and
- employing automated tools to support near real-time analysis.[32]

The functionality deployed in support of NCPS analytics capability developed to date is in accordance with recommended standards. For example, the security information and event management solution, which has been operational since February 2012, simplifies cyber analysis by providing a centralized platform in which the log data from similar events can be aggregated, thereby reducing duplication. The tool also facilitates analysts' ability to correlate related events that might otherwise go unnoticed and provides visualization capabilities, making it easier to see relationships. Additionally, NSD has established functionality that enables the analysis of the characteristics of malicious code. For example, the Packet Capture tool enables US-CERT analysts to see "inside" the packet, and inspect the payload to analyze a specific cyber threat. Further, the Digital Media Analysis Environment (Forensics) and Advanced Malware Analysis Center provide mechanisms to collect and contain information on cyber threats in a highly secure environment for evaluation by US-CERT analysts.

NSD and US-CERT officials stated that DHS initially focused funding and development efforts on analytical functions associated with supporting the intrusion detection and prevention functions of NCPS. However, the more complex analytics development is planned for later stages of system development. Specifically, DHS has enhancements planned through fiscal year 2018. These planned enhancements are intended to better facilitate the near real-time analysis of various data streams and advanced malware behavioral analysis, and to conduct forensic analysis in more collaborative way.

[32] NIST 800-53.

NCPS Information-Sharing Capability Is Not Fully Developed, and Selected Customer Agencies Did Not Always View Incident Notifications as Timely and Useful

Information sharing is a key control recommended by NIST in support of effective information system security.[33] Additionally, the presence of good information sharing, particularly the ability to effectively notify an affected entity of potentially malicious activity, is a key component of effective intrusion detection and prevention, and thus a key objective of NCPS. Further, NIST states that organizations should develop standard operating procedures to ensure that consistent and accurate information is available for reporting and management oversight. Also, US-CERT's Concept of Operations for NCPS establishes monitoring the status of mitigation actions and strategies as a requirement of the program.

NSD officials stated that the information-sharing capability has only recently been approved and funded for development, and thus current information-sharing efforts are manual and largely ad hoc. DHS first requested funding for the development of information-sharing capabilities in 2010, but NSD officials stated the effort was given a lower priority than the intrusion prevention capability and was not funded to begin planning activities until 2014. As a result, DHS has yet to develop a majority of planned functionality for the information-sharing capability of NCPS. Though the operational requirements for the NCPS information-sharing functionality were approved in November 2014, DHS did not formally authorize NSD to initiate development of the capability until August 2015. As a result no substantive actions have yet been taken to develop this capability.

Regarding the current information-sharing efforts, officials from the five customer agencies we reviewed stated that DHS is not always effectively communicating its intrusion detection notifications to customer agencies. Specifically, DHS officials provided evidence that they sent 74 incident notifications that they believed were related to NCPS to the five agencies in our review[34] during fiscal year 2014. However, evidence provided by the agencies showed that only 56 of these notifications had been received by the customer agencies. The five impacted agencies and DHS disagreed as to whether the other 20 incident notifications had been sent and received. Specifically, for 18 of 20 these notifications, DHS provided

[33] NIST 800-53.

[34] As noted previously, the five selected agencies were the Department of Energy, General Services Administration, National Science Foundation, Nuclear Regulatory Commission, and the Department of Veterans Affairs.

evidence that an e-mail may have been sent, but the agencies had no record of receiving the notifications. For the 2 additional notifications, one customer agency had a record of receiving them; however, DHS had no evidence of transmitting the e-mails.

For the 56 NCPS-related notifications that the five agencies acknowledged receiving, the agencies stated that

- 31 incidents notifications were timely and useful,
- 10 incidents notifications were not timely or useful,
- 7 incident notifications were identified by agency officials as false positives, and
- 7 incident notifications were not related to an NCPS intrusion-detection.[35]

Additionally, DHS did not always solicit, and agencies did not always provide, feedback on the notifications. Specifically:

- Of the 56 incident notifications mentioned above, DHS requested that the impacted agency provide feedback on 36 of them. Of these 36, the agencies stated that they provided feedback on 15 notifications, but did not provide feedback on 21.
- For an additional 10 notifications, officials from 3 of 5 agencies stated they provided feedback even though DHS had not explicitly requested follow-up action.
- For an additional 10 notifications, DHS did not request feedback and the customer agencies did not provide any.

As another channel for sharing information, US-CERT holds weekly calls with representatives of the security operation centers of various federal agencies. These calls provide a forum for the voluntary exchange of a variety of information security information, including NCPS-related information. Officials from the five customer agencies involved in our review expressed value in the information received from these discussions.

One reason DHS and agencies do not agree about whether notifications were received may be that DHS does not always explicitly ask for feedback or confirmation of receipt of the notification. Additionally,

[35] According to one of the five agencies, the remaining notification appeared to be duplicative of a previously sent notification. However, we were unable to verify this.

officials from one customer agency stated that DHS has no way of determining which of its analysts were responsible for transmitting a particular notification, so it is difficult to obtain context after a notification is sent.

US-CERT officials stated that standard operating procedures and a quality control procedure are being developed as part of the implementation of a new version of the incident management database. However, these procedures were not developed during the scope of our review, fiscal year 2014. In August 2015, US-CERT provided us with a draft standard operating procedure related to the incident notification process. The policy provides an overview of the types of questions a US-CERT analyst should ask a customer agency when transmitting a notification. However, the draft policy does not instruct them specifically to include a solicitation of feedback within the notification. Further, US-CERT could not provide any information regarding the timetable for when these procedures would take effect.

Regarding the usefulness of the notifications, two of the agencies in our review stated that because of the placement of the intrusion detection sensors on their networks, a significant amount of effort was required to evaluate the context of the DHS notifications. Thus, both agencies stated, and DHS agreed, the value of the notifications could be enhanced by giving US-CERT analysts access to the agencies' network diagrams, which could allow them to identify the specific location of the intrusion.

Officials from customer agencies stated that they did not provide feedback for a variety of reasons. For example, one agency stated that due to its federated nature, getting a response from the impacted entity within their agency was a challenge and could only be rectified by reaching out to site owners for every incident notification they receive. Consequently, officials stated, they typically only reached out when the notification had met the threshold of a security event. Officials from this agency stated that they had instituted a new standard operating procedure that requires the analyst processing the incident notification to reach out to DHS prior to closing it out. They added that this policy went into effect after fiscal year 2014 and did not impact the data set we reviewed. An additional agency stated that a request for feedback is not always clearly stated within the notification they receive from US-CERT.

Without verifying the receipt of intrusion detection notifications and soliciting feedback on their usefulness, DHS may be hindered in assessing the effectiveness of NCPS's current information-sharing capabilities.

Current Metrics Do Not Comprehensively Measure Effectiveness of NCPS

According to NIST,[36] a number of laws—including the Federal Information Security Management Act—cite performance measurement in general, and information security performance measurement in particular, as a requirement. Further, NIST 800-55 states that an information security measurement program provides a number of organizational and financial benefits, including increased accountability for information security performance, improved effectiveness of information security activities, demonstrated compliance with laws, and quantified inputs and allocation decisions. Further, effectiveness or efficiency measures are used to monitor if program-level processes and system-level security controls are implemented correctly, operating as intended, and meeting the desired outcome.

Metrics for NCPS, as provided by DHS, do not provide information about how well the system is enhancing government information security or the quality, efficiency and accuracy of supporting actions. DHS has established three department-wide NCPS-related performance metrics, as part of its Performance and Accountability report:

- Percentage of traffic monitored for cyber intrusions at civilian federal executive branch agencies: According to Executive Program Management Office and NSD officials, this measure assesses NCPS's intrusion detection capability by providing information on the scope of coverage for potentially malicious cyber-activity across participating civilian federal government agencies. During fiscal year 2014, DHS reported that approximately 88.5 percent of the total Internet traffic of 23 civilian, executive branch agencies was monitored by NCPS intrusion detection sensors. Though this metric provides insight into the amount of federal executive-branch traffic that NCPS is able to provide intrusion detection for, it does not provide insight into the quality or efficiency of the intrusion detection function for that traffic.
- Percentage of incidents detected by US-CERT that targeted agencies are notified of within 30 minutes: According to Executive Program

[36] NIST, *Special Publication Performance Measurement Guide for Information Security* 800-55 (Gaithersburg, Md.: July 2008).

Management Office and NSD officials, this is an additional measure of NCPS's intrusion detection capability. Specifically, DHS documentation stated that there were 297 cyber incidents identified on federal networks using the NCPS's intrusion detection capability in fiscal year 2014. The average time to notify impacted agencies was 18 minutes, with 87.2 percent (259 of 297) of notifications occurring within 30 minutes. While this metric provides insight into the speed at which DHS could share information related to detected incidents, it does not provide a measure for the accuracy or value of those notifications. Further, of 24 incident notifications for the five selected agencies that support this metric, DHS could not provide evidence that 12 of these notifications were sent. Without appropriately sharing the notifications with the affected agency, we are unsure how DHS classifies these 12 notifications as incidents.

- Percentage of known malicious cyber traffic prevented from causing harm at federal agencies: According to Executive Program Management Office and NSD officials, this measure assesses NCPS's intrusion prevention capability. Specifically, DHS documents stated that each currently deployed indicator of a malicious threat is paired with a countermeasure to prevent the malicious threat from harming those networks. In fiscal year 2014, 389 indicators were deployed amongst intrusion prevention sensors. Though this metric would track whether a particular countermeasure was engaging (i.e., if prevention occurred) it does not necessarily evaluate the effectiveness or efficiency of the intrusion prevention capability. DHS officials agreed with this observation and stated that the agency was in the process of retiring this metric and developing a new one that would better measure and evaluate the effectiveness of intrusion prevention.

Further, NSD has established key performance parameters that provide an indication of the system's ability to perform functions supporting NCPS's objectives. For example, the following measures were developed to track the performance of the intrusion detection function:

- Detect known cyber events through automated intrusion detection within 1 minute of event occurrence.
- Provide automated notification within the operations center that a cyber event took place within 1 minute of event detection.
- Aggregate and correlate detected cyber events for known indicators within 30 minutes of event notification.

While these are valuable for determining how NCPS is operating as a system, officials from the Executive Program Management Office and NSD agreed that they did not provide a qualitative or quantitative assessment of the system's ability to fulfill the aforementioned objectives. Further, as we reported in April 2015, a DHS acquisition official questioned whether the NCPS key performance parameters were defined properly.[37]

Regarding the system's benefits, NSD and US-CERT officials stated that the total amount of incident notifications sent to customer agencies does indicate that NCPS is providing value. However, as our analysis of a selected group of customer notifications from fiscal year 2014 indicates, customer agencies do not perceive every notification transmitted as valuable. Without the deployment of comprehensive measures, DHS cannot appropriately articulate the value provided by NCPS.

DHS Identified Future NCPS Needs, but Has Developed Limited Requirements

While DHS developed an executive road map for the intrusion detection, prevention, analytics, and information sharing objectives that describes future NCPS capabilities to be developed through fiscal year 2018, it has not defined requirements, as called for by OMB guidance and best practice, for two intrusion detection capabilities to be provided in fiscal year 2016. In addition, although DHS officials stated that they do consider threat information as part of the required risk-based approach for determining future capabilities to protect federal information systems, they do not consider specific vulnerabilities affecting agencies' networks and systems, as information on these is not currently available. The lack of vulnerability information prevents DHS from taking a full risk-based approach to designing future NCPS intrusion prevention capabilities.

[37] GAO-15-171SP.

DHS Identified Future Needs in Program Planning Documents, but Not All Future Capabilities Are Based on Appropriately Defined Requirements

OMB's Capital Programming Guide states that requirements should be developed to support program budgeting activities. The guidance also states that agencies should avoid "specification creep," where requirements become uncontrolled by defining requirements to meet future potential needs or incorporating emerging technology that would be "nice" to have. Further, a recognized best practice in requirements development from the Software Engineering Institute notes that requirements should be expressed in a way that can be used for design decisions.[38]

NSD maintains a road map that is used to track potential additional capabilities for NCPS's intrusion detection, intrusion prevention, analytics, and information-sharing objectives to be developed in future fiscal years, up to fiscal year 2018. For each NCPS objective, the Executive Road Map identifies the current state of operations ("as-is") and the desired state of operations ("target"). According to NSD officials, this road map facilitates discussions with senior DHS management, and is revised at several points in the fiscal year.

The road map identifies technology and techniques that may increase the department's ability to perform activities to support the four objectives. For example, DHS plans to begin work on a "web gateway proxy scan encryption" capability in fiscal year 2016. DHS also plans to seek funding for a wireless network protection capability in fiscal year 2018, which may add an additional type of intrusion detection and prevention technology described in guidance issued by NIST.[39]

Requirements have not been fully defined for all items in the road map. Specifically, two capabilities DHS stated will be provided in fiscal year 2016—expanding the intrusion detection capability to identify malware present on customer agency internal networks and identifying malicious traffic entering and exiting cloud-based service provider services—are based on requirements that have not been fully defined.

NSD officials stated that these capabilities were based upon the requirement to detect intrusion attempts in near real time across the

[38] Software Engineering Institute, *Capability Maturity Model® Integration for Development (CMMI-DEV)*, Version 1.3 (Pittsburgh, Pa.: November 2010).

[39] NIST 800-94.

federal government. They added that identifying malware on customer agency internal networks and malicious traffic entering and exiting cloud-based service providers is a logical expansion of responding to the cyber threat, and the program office needs flexibility to adapt to the threat. However, these capabilities could represent a significant departure from the version of NCPS currently deployed and envisioned in the governance documents. Specifically, the technical nature of cloud computing—where customer agency data may be stored and accessed by multiple physical sites—and the number of cloud service providers that could be used by customer agencies may require a different infrastructure deployment methodology than the existing NCPS sensor deployments at Internet service providers and at customer agency locations. Further, while the Executive Road Map indicates that NCPS will detect malware on customer agency internal networks using log data from DHS's Continuous Diagnostics and Mitigation program, it is unclear how DHS plans to accomplish this.

Until it fully defines requirements for these two capabilities, DHS increases the risk that it will invest in functionality that does not effectively support information security efforts at the customer agencies and across the federal government.

Decisions Regarding Future NCPS Intrusion Prevention Capabilities Incorporate Some Elements of a Risk-Based Approach

The Federal Information Security Modernization Act of 2014 and guidance issued by NIST call for a risk-based approach to protecting federal systems. According to NIST's *Guide for Conducting Risk Assessments*, information security risk is assessed by considering the threats posed to the federal government, the vulnerabilities (or weaknesses) in information systems, the impact (or harm) that could occur given the potential for threats exploiting vulnerabilities, and the likelihood that threats would use the exploits to allow harm to occur.[40]

DHS has incorporated selected elements of a risk-based approach when considering the next capabilities of the NCPS intrusion prevention objective. Specifically, NSD coordinated and leveraged threat information from the National Security Agency and the National Cybersecurity and Communications Integration Center, along with information provided by

[40] NIST, *Guide for Conducting Risk Assessments,* Special Publication 800-30 Revision 1 (Gaithersburg, Md.: September 2012).

the Internet service providers, to develop a list of countermeasures that DHS believed would be reasonable to implement.

NSD officials stated that decisions regarding existing and upcoming countermeasures were made based on the capabilities of the Internet service providers. Specifically, the e-mail and DNS countermeasures were used as the first countermeasures for the NCPS intrusion prevention capability because they were already deployed at Internet service providers as part of the Enhanced Cybersecurity Services program.

However, NSD did not consider and does not currently have access to vulnerability information for the agency information systems it is helping to protect. NSD officials stated that vulnerability data about customer agency information systems and networks are difficult to obtain. For example, agency information security reports required under the Federal Information Security Modernization Act of 2014 do not contain vulnerability information that NSD could use to inform future capabilities. Also, NSD officials stated—and the Executive Road Map confirmed—that DHS's Continuous Diagnostics and Mitigation program may provide additional vulnerability information that could be valuable in determining future capabilities. However, at this time the program is relatively immature and NSD had not developed processes and procedures on how to use this vulnerability information to inform decisions on future capabilities at the time of our review.

Further, DHS also has a separate program to collect vulnerability information on federal executive branch agency systems and networks that could be useful for determining future NCPS intrusion prevention capabilities. In an October 2014 memo, OMB directed DHS to scan Internet-accessible addresses and public-facing segments of federal civilian agency systems for vulnerabilities on an ongoing basis, and report to OMB on the identification and mitigation of vulnerabilities across federal agency information systems.[41] However, NSD did not provide details—including processes and procedures—of how this information could be used to inform future NCPS intrusion prevention capabilities.

[41] OMB, *Memorandum for Heads of Executive Departments and Agencies: Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, OMB-15-01 (Washington, D.C.: Oct. 3, 2014).

Until the department develops processes and procedures for using such vulnerability information, DHS will not be able to adopt an effective risk-based approach for planning future NCPS intrusion prevention capabilities.

NCPS Adoption Varied across the Agencies

OMB Memorandum M-08-05 established the requirement for almost all federal executive branch agencies to implement the intrusion detection capabilities (within Einstein 2) of NCPS.[42] In July 2015, the White House noted that deployment of the NCPS intrusion prevention capabilities was to be accelerated, with DHS awarding a contract to provide intrusion prevention services for all federal civilian agencies by the end of 2015.

Agencies have had mixed results in adopting NCPS capabilities. According to DHS program documentation, all 23 of the non-defense CFO Act agencies had routed traffic to NCPS intrusion detection sensors. However, NSD documents indicated that only 5 of the 23 agencies were receiving intrusion prevention services. Further, NSD documents showed that for 3 of these 5 agencies, adoption of intrusion prevention services for e-mail was limited—only 1 agency appeared to have fully adopted intrusion prevention for e-mail service, another agency had adopted intrusion prevention for only one part of its network e-mail, and a third agency was just beginning to adopt the e-mail service.

Further, four of the five selected agencies in our review reported that not all of their traffic was being sent to NCPS intrusion detection sensors. In addition, two of the selected agencies reported that they had adopted the DNS intrusion prevention service, and only one had completed the adoption process for its e-mail service. See table 4 below for a summary of NCPS intrusion detection and prevention adoption at the selected five agencies.

[42] As previously stated, OMB M-08-05 announced the Trusted Internet Connection Initiative, which included Einstein. The Department of Defense is not required to implement Einstein. For more information, see GAO*, Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies*, GAO-10-237 (Washington, D.C.: Mar. 12, 2010) and Department of Homeland Security Office of Inspector General*, Implementation Status of Einstein 3 Accelerated*, OIG-14-452 (Washington, D.C.: Mar. 24, 2014).

Table 4: NCPS Adoption at Selected Agencies

		Intrusion prevention	
Agency	Intrusion detection	Outbound DNS	Inbound e-mail
Agency 1	Yes	Yes	No
Agency 2	Partial	No	No
Agency 3	Partial	No	No
Agency 4	Partial	Yes	Yes
Agency 5	Partial	No	No

Source: GAO analysis of DHS and selected agency information. | GAO-16-294

Officials from NSD, the selected agencies in our review, and the Internet service providers identified several policy and implementation challenges to adopt the NCPS intrusion prevention capabilities, along with efforts to address these challenges:

- Approval of memoranda of agreement (MOA): An MOA is required in order to establish NCPS service for an agency. Among other things, the MOA identifies responsibilities for both DHS and the customer agency (including interactions with Internet service providers), as well as identifies points of contact for the respective organizations. Sixteen of the 23 non-defense CFO Act agencies had an MOA in place with DHS to provide intrusion prevention services.

  Three of the five agencies in our review were in the process of approving an MOA for intrusion prevention services and cited barriers to approving the agreement. Specifically, two of these agencies did not sign an agreement because their Internet service providers had not been capable of providing NCPS intrusion prevention services. NSD officials stated that they are in the process of accelerating the availability of Internet service providers to those agencies which are not currently provided NCPS intrusion prevention capabilities. Officials from the third agency stated that there were questions whether existing law protecting sensitive information in its possession prohibited participation in NCPS intrusion prevention or not. In July 2015, officials from this agency stated that, working with DHS, it had agreed to adopt some NCPS intrusion prevention capabilities.

- Agency capabilities and concerns: NSD officials noted that the ability to meet DHS security requirements (e.g., encrypted tunnels) to use the intrusion prevention capabilities varies from agency to agency. NSD officials also stated that because each agency has unique network infrastructures, implementation must be specific to that agency. Further, NSD officials added that agencies are generally concerned about interfering with any mission-critical applications, such as e-mail. Also, while chief information officers usually sign the MOA, NSD officials noted that network operators within the agency can be unaware of the agreement, which can pose a potential barrier to full deployment. To address these issues, NSD staff stated that they work with agencies to tailor implementation and explain details of the prevention capabilities to reassure them that business operations will not be impeded. Additionally, officials from one agency in our review that had adopted the DNS intrusion prevention capability initially hesitated to adopt the e-mail capability due to records management concerns. Agency officials stated in July 2015 that they are in the process of working with DHS to adopt the e-mail intrusion prevention capability.

- Viability of solution for cloud e-mail: Officials from one agency in our review stated that they obtain e-mail services from cloud providers, and added that they hesitate to participate in NCPS intrusion prevention e-mail capability because there is currently no solution that is easily implemented. Officials from another agency in the process of signing an MOA stated that they also use cloud service providers for e-mail. This agency will also not be able to implement the e-mail intrusion prevention capability. NSD has noted the challenges associated with implementing a cloud solution, but plans to refine this capability over time. However, as we previously stated, the plans to initiate development efforts on a cloud solution during fiscal year 2016 are not based on fully developed requirements.

- Development and operational challenges at Internet service providers: NSD and two of the Internet service providers noted a challenge with designing, developing, and operating a classified infrastructure on unclassified network traffic. For example, the complex and changing security requirements of one of DHS's partners who provides threat information created delays in the service providers' ability to deliver intrusion prevention capabilities. In addition, obtaining and retaining personnel with appropriate security clearances posed a challenge for the Internet service providers. NSD has acknowledged the inherent complexity of using classified information to address cyber risks in non-classified network traffic and has ongoing efforts to work with the Internet service providers to address this.

Further, NCPS faces additional implementation challenges in ensuring that agency traffic is sent to the intrusion detection sensors. Specifically, four of the five agencies in our review cited several challenges in routing all of their traffic through NCPS intrusion detection sensors, including capacity limitations of the sensors, agreements with external business partners that use direct network connections, interagency network connections that do not route through Internet gateways, use of encrypted communications mechanisms, and backup network circuits that are not used regularly. NSD officials stated that agencies are responsible for routing their traffic to the intrusion detection sensors, and DHS does not have a role in that aspect of NCPS implementation.

NCPS also faces a challenge in implementing a portion of the intrusion detection capability and all of the intrusion prevention capability when routing traffic through sensors at the Internet service providers.[43] Of the five agencies in our review, four depend on their Internet service provider to receive NCPS intrusion detection services (through the Managed Trusted Internet Protocol Service program) and/or intrusion prevention services. Two of these four agencies had taken steps to securely route traffic to the sensors, while one agency did not implement an authentication mechanism to ensure that network routes received by their router were legitimate. The other agency stated that its Internet service provider managed its routing configurations and did not provide evidence for us to verify if secure routing configurations were in place.

This occurred in part because NSD did not provide guidance to customer agencies on how to securely route their information to the Internet service providers. NSD officials stated that providing network routing guidance to customer agencies is not the role of DHS. Rather, they believe that is best handled by the customer agency and their Internet service provider. However, without providing network routing guidance, NSD has no assurance the traffic they see constitutes all or only a subset of the traffic the customer agencies intend to send. Further, by not providing routing guidance, NSD has less assurance that customer agency traffic will actually be picked up at the sensors, since the routing may bypass those sensors, reducing the effectiveness of NCPS.

[43] Customer agencies requiring their Internet service provider to perform NCPS activities (such as with NCPS intrusion detection services provided through the Managed Trusted Internet Protocol Service or any of the NCPS intrusion prevention capabilities) must configure their border gateways to communicate the appropriate traffic—including DNS and e-mail traffic for the NCPS intrusion prevention capabilities—to the providers in a secure manner.

Conclusions

DHS has devoted significant resources to developing and deploying NCPS, with the goal of strengthening agencies' ability to detect and prevent intrusions on their networks, as well as the capability for analyzing network activity and sharing information between DHS and agencies. The system's intrusion detection capabilities are the most fully developed of the four system objectives, and they provide the ability to detect known malicious patterns of activity on agency networks. However, without the ability to effectively detect intrusions across multiple types of traffic or provide other types of detection capabilities, such as anomaly-based and stateful purpose detection, NCPS is limited in its ability to identify potential threats. In addition, without making use of publicly available, open-source repositories to enhance the system's signatures and data available from its Continuous Diagnostics and Mitigation program, DHS may not be providing the ability to detect attacks that exploit known vulnerabilities.

The system's intrusion prevention capability is less fully developed, with limited deployment across different types of network traffic, such as content from websites, limiting its ability to prevent malicious code from penetrating agencies' networks.

Further, NCPS's support of a number of analytics capabilities, and ongoing efforts to enhance these, should provide DHS and agencies with improved ability to analyze potentially malicious traffic in a timely and efficient manner. However, DHS's sharing of information with agencies has not always been effective, with disagreement among agencies about the number of notifications sent and received and their usefulness. Finalizing the incident notification process, to include the solicitation of feedback from customer agencies, could help ensure that DHS is effectively communicating information that helps agencies strengthen their security posture. Another step that could assist in ensuring the effectiveness of NCPS is developing metrics that measure the quality, efficiency, and accuracy of the services it provides.

DHS has continued to plan for future capabilities of the system, but without clearly defined requirements, it risks investing in functionality that does not effectively support agency information security. Moreover, to ensure a risk-based approach is being pursued to select future NCPS capabilities, information about vulnerabilities on agency networks could be a valuable input.

The effectiveness of NCPS further depends on its adoption by agencies. While the adoption of the intrusion detection capabilities is widespread among the 23 agencies required to use NCPS, the implementation of intrusion prevention capabilities is more limited due to policy and implementation challenges that DHS is working to overcome. However, addressing a lack of guidance for routing network traffic through NCPS sensors could help better ensure a wider and more effective use of NCPS capabilities.

Recommendations for Executive Action

We recommend the Secretary of Homeland Security direct:

- NSD to determine the feasibility of enhancing NCPS's current intrusion detection approach to include functionality that would detect deviations from normal network behavior baselines;
- NSD to determine the feasibility of developing enhancements to current intrusion detection capabilities to facilitate the scanning of traffic not currently scanned by NCPS;
- US-CERT to update the tool it uses to manage and deploy intrusion detection signatures to include the ability to more clearly link signatures to publicly available, open-source data repositories;
- US-CERT to consider the viability of using vulnerability information, such as data from the Continuous Diagnostics and Mitigation program as it becomes available, as an input into the development and management of intrusion detection signatures;
- US-CERT to develop a timetable for finalizing the incident notification process, to ensure that customer agencies are being sent notifications of potential incidents, which clearly solicit feedback on the usefulness and timeliness of the notification;
- The Office of Cybersecurity and Communications to develop metrics that clearly measure the effectiveness of NCPS's efforts, including the quality, efficiency, and accuracy of supporting actions related to detecting and preventing intrusions, providing analytic services, and sharing cyber-related information;
- The Office of Cybersecurity and Communications to develop clearly defined requirements for detecting threats on agency internal networks and at cloud service providers to help better ensure effective support of information security activities;
- NSD to develop processes and procedures for using vulnerability information, such as data from the Continuous Diagnostics and Mitigation program as it becomes available, to help ensure DHS is using a risk-based approach for the selection/development of future NCPS intrusion prevention capabilities; and
- NSD to work with their customer 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.

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of Homeland Security, Energy, and Veterans Affairs; the General Services Administration; the Nuclear Regulatory Commission; and the National Science Foundation for their review and comment. In written comments signed by the Director, Departmental GAO-OIG Liaison Office, DHS concurred with each of our nine recommendations. DHS also provided details about steps that it plans to take to address eight of the nine recommendations, including estimated time frames for completion. If effectively implemented, these actions should help address the weaknesses we identified in the NCPS program. Regarding our recommendation to develop clearly defined requirements for detecting threats on agency internal networks and at cloud service providers, the Director asked that we consider it resolved and closed because a formal requirements working group and requirements management process had been developed. We will review the evidence and determine if these actions address the recommendation. DHS's written comments are reprinted in appendix III.

Officials from DHS also provided technical comments via e-mail, which we incorporated as appropriate. Officials from the Departments of Energy and Veterans Affairs, General Services Administration, Nuclear Regulatory Commission, and the National Science Foundation stated that they had no comments.

We are sending copies of this report to the appropriate congressional committees, the departments and agencies in our review, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati

Nabajyoti Barkakati, Ph.D.
Director, Center for Technology and Engineering

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine the extent to which (1) the National Cybersecurity Protection System (NCPS) meets stated objectives, (2) the Department of Homeland Security (DHS) has designed requirements for future stages of the system, and (3) federal agencies have adopted the system.

To determine the extent to which NCPS meets stated objectives, we compared four of the overarching capabilities of the system (intrusion detection, intrusion prevention, analytics, and information sharing) to leading federal practices, including the National Institute of Standards and Technology's Special Publication 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations; Special Publication 800-55: Performance Measurement Guide for Information Security*, and Special Publication 800-94: *Guide to Intrusion Detection and Prevention Systems (IDPS).* We also examined program information and documents, as well as interviewed DHS officials within the Office of Cybersecurity and Communications responsible for designing, developing, maintaining, and operating NCPS.

For the information-sharing objective we examined NCPS-related incident notifications DHS stated were sent by the United States Computer Emergency Readiness Team in fiscal year 2014 to five selected Chief Financial Officers Act agencies: the Departments of Energy and Veterans Affairs, the General Services Administration, the National Science Foundation, and the Nuclear Regulatory Commission. These agencies were selected based on information provided by DHS regarding the relative number of NCPS-related incident notifications sent to the agencies (one with a higher amount of notifications, two with around the median amount of notifications, and two with the fewest amount of notifications) and NCPS capabilities received. We also interviewed information security staff from each of these agencies and collected information regarding each agency's perceived usefulness and timeliness of the incident notifications, along with any feedback provided in response to the notification.

To evaluate the intrusion detection signatures deployed, we selected 10 common vulnerabilities from 2014 commonly affecting client and server applications and determined the extent to which the NCPS signatures provided reasonable coverage for the vulnerability the signature was intended to mitigate. Additionally, we conducted a similar evaluation for the signatures associated with a selection of 12 common advanced persistent threats from 2014. Further we evaluated the number of intrusion detection signatures DHS had issued for each client vulnerability during fiscal year 2014 and compared them to the number of signatures from publicly available repositories, such as common vulnerabilities and exposures (CVE) published for each corresponding category of vulnerability during the same period. We then determined the percentage of DHS coverage by comparing the number of signatures DHS had that addressed each of the vulnerabilities to the total number of CVEs released in 2014 for that category.

To determine the extent to which DHS has designed requirements for future stages of the system, we reviewed NCPS program planning documentation and interviewed program officials in order to identify how future capabilities are planned. We compared this information to federal guidance for planning and requirements development found in the Office of Management and Budget's *Capital Programming Guide*. In addition, for all new capabilities identified for funding in DHS's fiscal year 2016 funding request (such as expanding information sharing, streaming and near-real-time analytics, and deploying intrusion detection sensors at Internet service providers' traffic aggregation sites), we determined if formalized requirements supporting these capabilities had been documented and approved in program documentation. Further, we determined if plans for future capabilities to address NCPS's intrusion prevention objective were determined using a risk-based approach, including a consideration of threat, vulnerability, impact, and likelihood.

To determine the extent to which federal agencies have adopted NCPS, we reviewed policy issued by the Office of Management and Budget and DHS documentation (such as memoranda of agreement) for the 23 non-defense agencies identified in the Chief Financial Officers Act. We also discussed any challenges to adoption with DHS officials. To gain a better understanding of how federal agencies adopt the system, including the amount of traffic and any challenges or limitations associated with adoption, we interviewed officials from the five Chief Financial Officers Act agencies identified previously and reviewed agency network documentation. We also interviewed officials from the three Internet service providers currently participating in NCPS to obtain their perspective on agency adoption of the system.

We conducted this performance audit from June 2014 to January 2016 in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Overview of the National Cybersecurity Protection System's Development and Functionality

The National Cybersecurity Protection System (NCPS), operationally known as the Einstein program, is an integrated system-of-systems that is intended to deliver a range of capabilities, including intrusion detection, intrusion prevention, analytics, and information sharing.

Intrusion Detection Capability

The sensors deployed to support the 2003 version of NCPS, or Einstein 1, collect network flow records of data entering and exiting participating agencies' networks, which are to be analyzed by U.S. Computer Emergency Readiness Team (US-CERT) analysts and tools to detect certain types of malicious activity.[1] If the system detects malicious activity, US-CERT analysts are to coordinate with the appropriate agencies to support the mitigation of those threats and vulnerabilities. US-CERT also is to use the information from the sensors to create analyses of cross-governmental trends that offer agencies an aggregate picture of external threats against the federal government's networks.

In 2009, the Department of Homeland Security (DHS) incorporated network intrusion detection technology into the capabilities of the initial version of the system, enabling NCPS to monitor Einstein 1 network data from participating federal agencies for specific predefined patterns of known malicious activity, referred to as signatures. The NCPS intrusion detection capability, or Einstein 2, is to use signatures derived from numerous sources, such as commercial and public computer security information, incidents reported to US-CERT, information from federal partners, and independent US-CERT in-depth analysis.[2] When NCPS's intrusion detection function detects traffic consistent with malicious patterns denoted by a particular signature, it provides US-CERT analysts with a notification. The analyst is then to investigate the detection to determine if it was in fact an incident and provide mitigation support to the affected agency, as appropriate.

[1] Network flow records, also referred to as netflow, are records of communications made to an organization's IT systems. The records identify the source and destination Internet Protocol addresses used in the communication, the source and destination ports, the time the communication occurred, and the protocol used to communicate.

[2] Signatures are specific machine readable patterns of network traffic that could negatively affect the integrity, confidentiality, or availability of computer networks, systems, and information. For example, a specific signature might identify a known computer virus that is designed to delete files from a computer without authorization.

Intrusion Prevention Capability

In 2013, DHS's Network Security Deployment division (NSD) began deployment of an initial operational capability of the intrusion prevention function, operationally known as Einstein 3A, which is intended to support DHS's ability to actively defend .gov network traffic. One of the major components supporting the capability is the "Nest," which is a classified facility located at each of the participating Internet service providers that is responsible for off-ramping (i.e., routing traffic to the Nest from the agency) and on-ramping (i.e., routing traffic from the Nest back to the Internet) .gov traffic. DHS shares specific indicators of malicious activity with Internet service providers, who then configure the indicators into signatures for testing and implementation and match patterns against established indicators based on known or suspected malicious traffic traveling to or from the participating agencies.[3] Table 5 below highlights additional intrusion prevention functions currently available in NCPS.

Table 5: National Cybersecurity Protection System Intrusion Prevention Capabilities

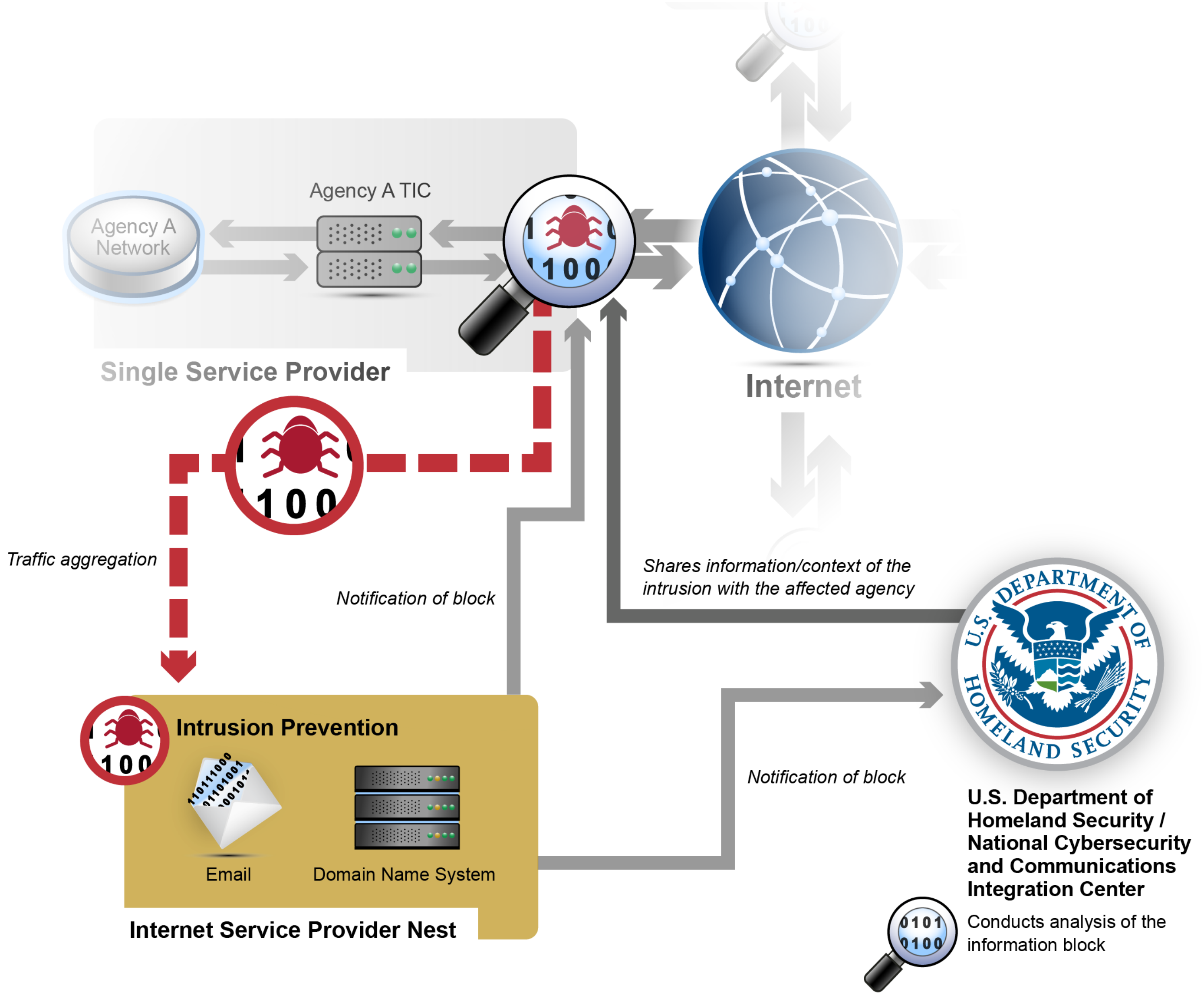
Capability	Description
Malicious traffic blocking	Blocks malicious traffic from entering or leaving federal civilian executive branch agency networks. This capability is managed by Internet service providers, who administer intrusion prevention and threat-based decision making using DHS-developed indicators of malicious cyber activity to develop signatures.
Domain name server blocking	Prevents malware installed on .gov networks from communicating with known malicious sources by redirecting the network connection away from the malicious sources to "safe servers" thus preventing further malicious activity by the installed malware.
E-mail filtering	Scans and potentially quarantines e-mail destined for .gov networks for malicious attachments before they are delivered to .gov end-users.

Source: GAO analysis of DHS NCPS program documentation. | GAO-16-294

Once fully deployed across the government, NCPS is intended to leverage available information from commercial and government sources to apply in-line protection measures to a wide set of federal network traffic protocols. When a signature detects a known or suspected cyber threat, NCPS is supposed to act on that threat to stop malicious traffic and prevent harm to the intended targets. Figure 3 provides an overview of how NCPS intrusion prevention capability is designed to work.

[3] Pattern matching is a technique in automated data analysis, usually performed on a computer, by which a group of characteristic properties of an unknown object is compared with comparable groups of characteristics of a set of known objects, to discover the identity or proper classification of the unknown object.

Figure 3: Overview of How NCPS Intrusion Prevention Capability Is Designed to Work


Agency A TIC
Agency A Network
Single Service Provider
Internet
Traffic aggregation
Notification of block
Shares information/context of the intrusion with the affected agency
Intrusion Prevention
Email
Domain Name System
Internet Service Provider Nest
Notification of block
U.S. Department of Homeland Security / National Cybersecurity and Communications Integration Center
Conducts analysis of the information block

Source: GAO analysis of Department of Homeland Security data. | GAO-16-294

Analytics Capability

NCPS's analytic capability is intended to capture, organize, and analyze data collected from NCPS sensors and other data feeds. Table 6 below highlights key analytics functions currently available in NCPS.

Table 6: National Cybersecurity Protection System Analytics Capabilities

Capability	Description
Analytics	Compiles and analyzes information about cyber activity and reports on current and potential cybersecurity threats and vulnerabilities.
Advanced malware analysis center	Provides a segregated, closed, computer network system that is used to analyze computer network vulnerabilities and threats. The corrective action information is then published in vulnerability or malware reports.
Security information and event management	Provides an end-to end solution for data collection, aggregation, correlation, and visualization through an integrated suite of hardware, operating systems, and software.
Aggregation	Normalizes the data collected to make them uniform and easier to analyze.
Visualization tools	Enables the analyst to rapidly comprehend the current situation.

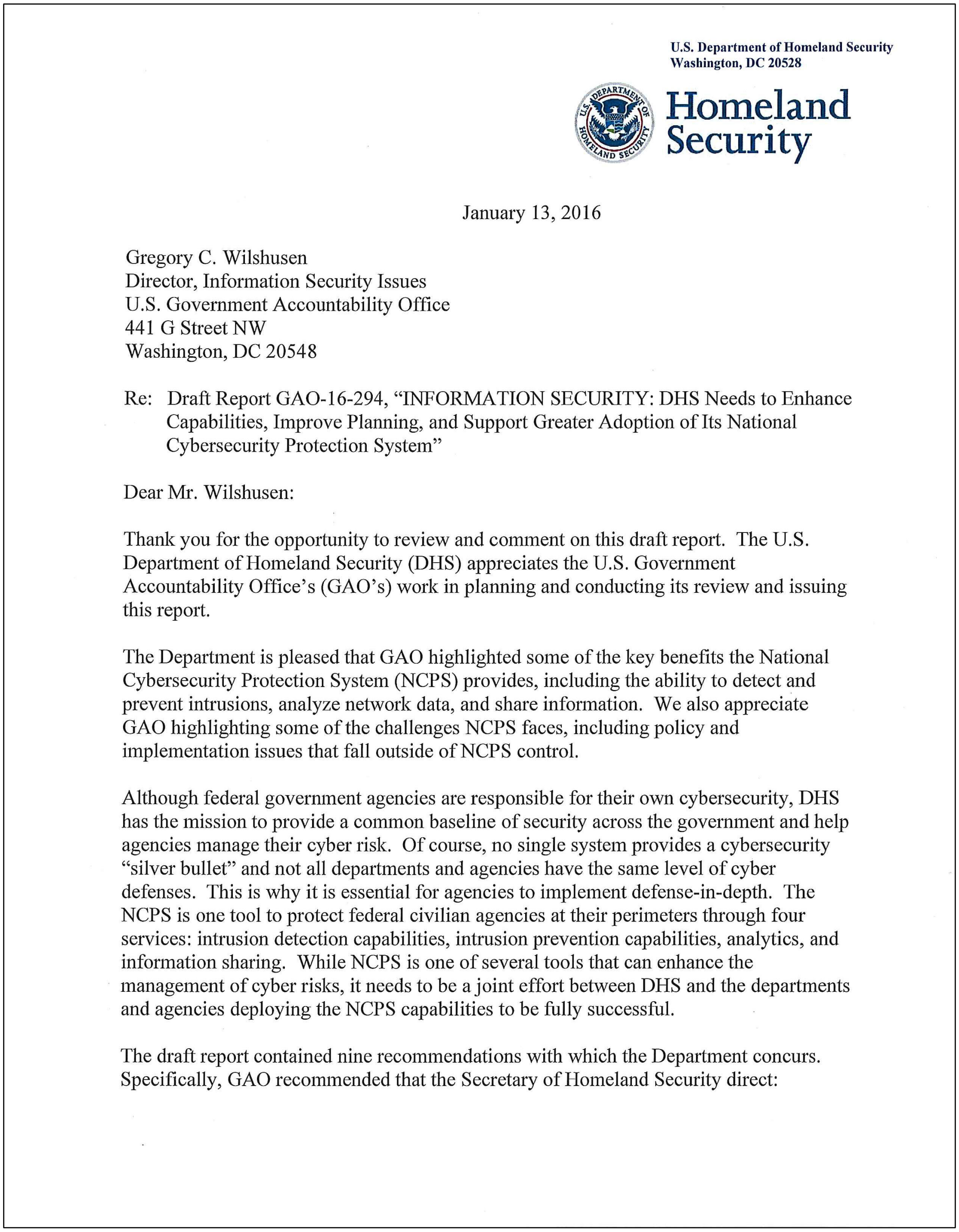
Source: GAO analysis of DHS NCPS program documentation. | GAO-16-294

These capabilities are expected to enable US-CERT to fuse information and correlate malicious network activities across participating federal executive branch agencies to achieve situational awareness of high-profile cyber threats. US-CERT is responsible for sharing situational awareness about current and potential cybersecurity threats and vulnerabilities with federal agencies, state and local governments, private sector partners, infrastructure owners and operators, and the public.

Information-Sharing Capability

NCPS's information-sharing capability is intended to enable enhanced sharing of information between DHS and its partners through real-time or near-real-time response; collaboration and coordination; and analysis of network intrusion attempts, suspicious intrusion activity, and analytical best practices. When fully developed, NCPS information sharing is intended to promote the rapid exchange of appropriate cyber threat and cyber incident information among NCCIC cybersecurity analysts and their cybersecurity partners, at multiple classification levels. Further, the capabilities are intended reduce time required to respond to incidents with better coordination and collaboration, and improved efficiencies with more automated information sharing and exposure of analysis capabilities.

Appendix III: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

January 13, 2016

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Re: Draft Report GAO-16-294, "INFORMATION SECURITY: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System"

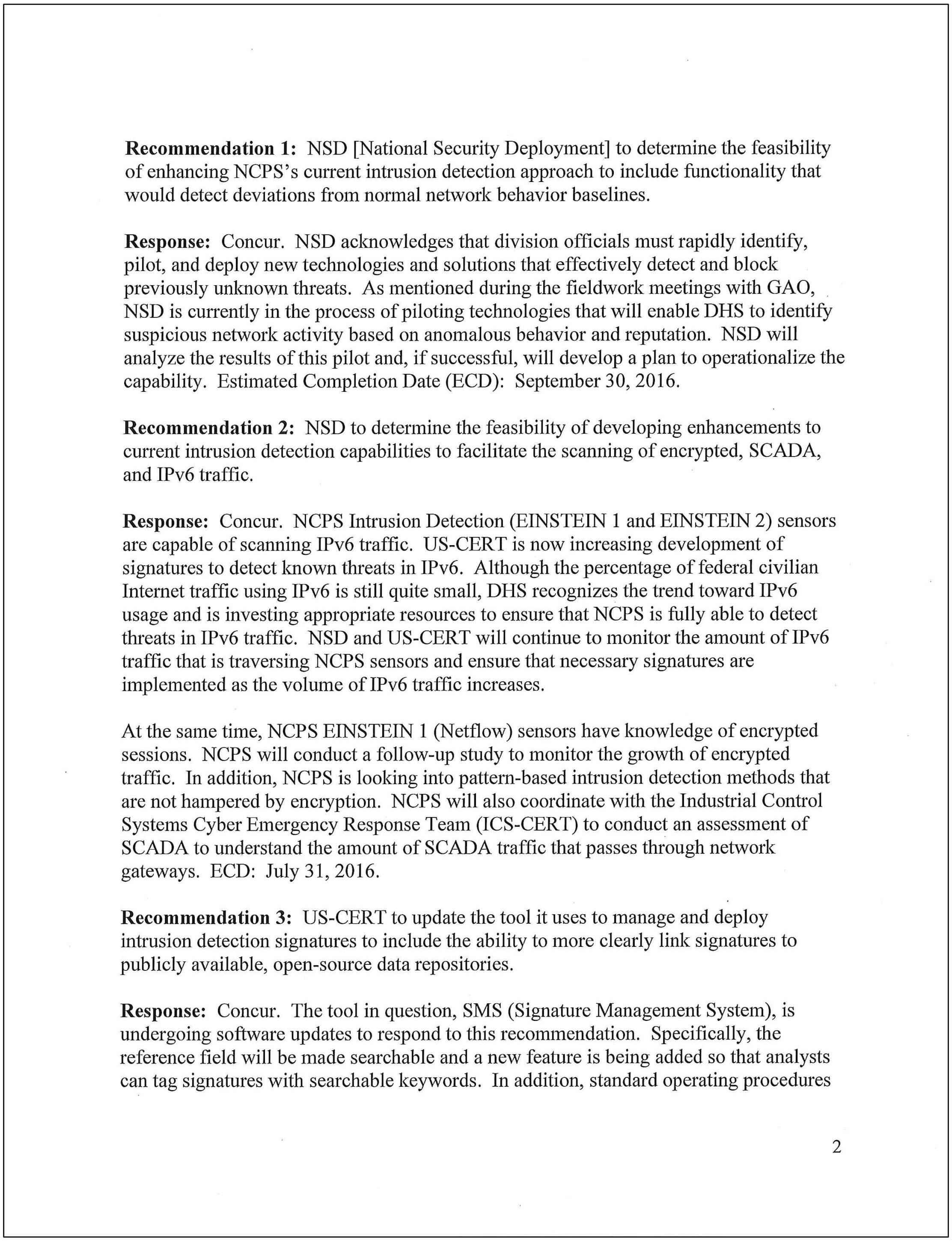
Dear Mr. Wilshusen:

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

The Department is pleased that GAO highlighted some of the key benefits the National Cybersecurity Protection System (NCPS) provides, including the ability to detect and prevent intrusions, analyze network data, and share information. We also appreciate GAO highlighting some of the challenges NCPS faces, including policy and implementation issues that fall outside of NCPS control.

Although federal government agencies are responsible for their own cybersecurity, DHS has the mission to provide a common baseline of security across the government and help agencies manage their cyber risk. Of course, no single system provides a cybersecurity "silver bullet" and not all departments and agencies have the same level of cyber defenses. This is why it is essential for agencies to implement defense-in-depth. The NCPS is one tool to protect federal civilian agencies at their perimeters through four services: intrusion detection capabilities, intrusion prevention capabilities, analytics, and information sharing. While NCPS is one of several tools that can enhance the management of cyber risks, it needs to be a joint effort between DHS and the departments and agencies deploying the NCPS capabilities to be fully successful.

The draft report contained nine recommendations with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct:



Recommendation 1: NSD [National Security Deployment] to determine the feasibility of enhancing NCPS's current intrusion detection approach to include functionality that would detect deviations from normal network behavior baselines.

Response: Concur. NSD acknowledges that division officials must rapidly identify, pilot, and deploy new technologies and solutions that effectively detect and block previously unknown threats. As mentioned during the fieldwork meetings with GAO, NSD is currently in the process of piloting technologies that will enable DHS to identify suspicious network activity based on anomalous behavior and reputation. NSD will analyze the results of this pilot and, if successful, will develop a plan to operationalize the capability. Estimated Completion Date (ECD): September 30, 2016.

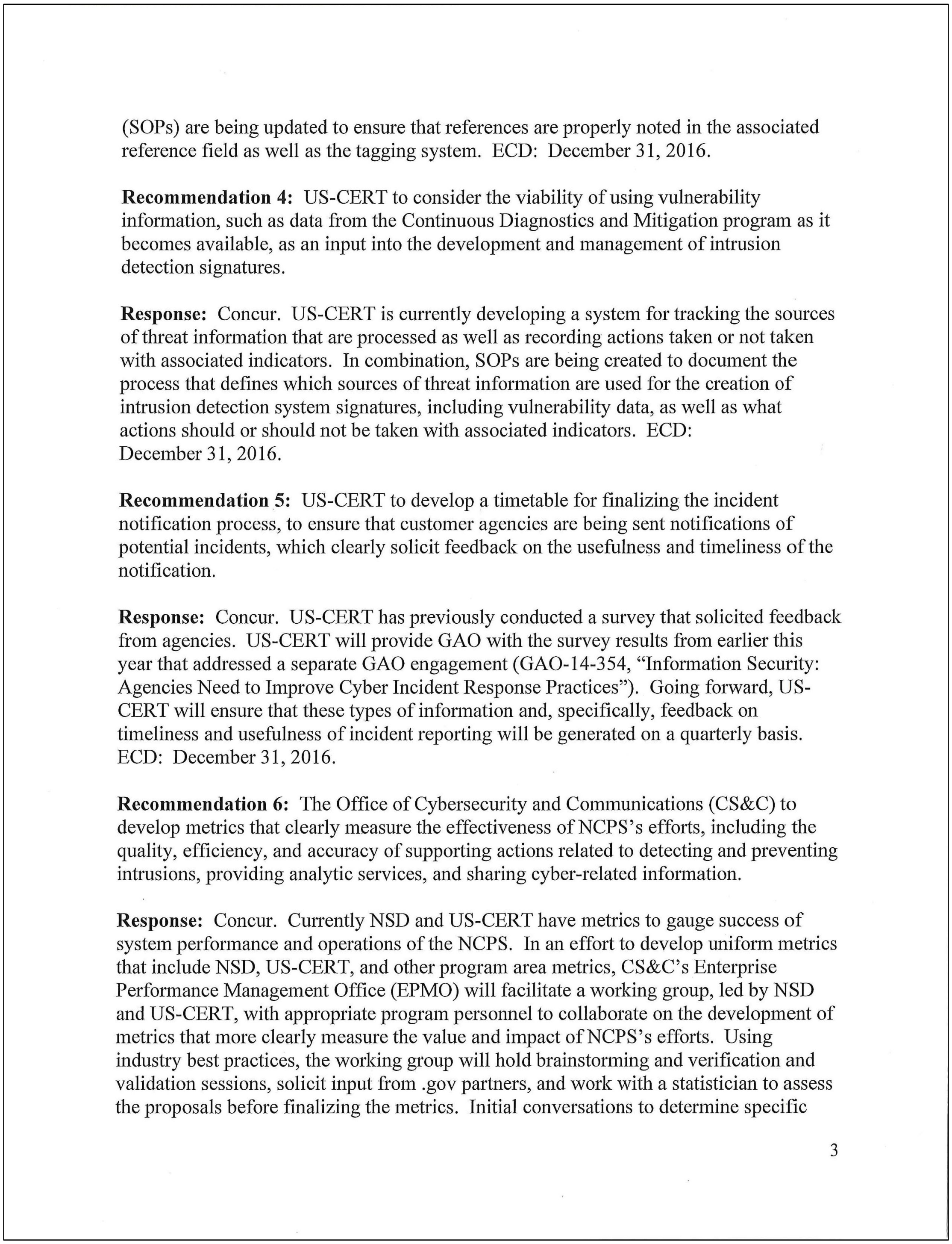
Recommendation 2: NSD to determine the feasibility of developing enhancements to current intrusion detection capabilities to facilitate the scanning of encrypted, SCADA, and IPv6 traffic.

Response: Concur. NCPS Intrusion Detection (EINSTEIN 1 and EINSTEIN 2) sensors are capable of scanning IPv6 traffic. US-CERT is now increasing development of signatures to detect known threats in IPv6. Although the percentage of federal civilian Internet traffic using IPv6 is still quite small, DHS recognizes the trend toward IPv6 usage and is investing appropriate resources to ensure that NCPS is fully able to detect threats in IPv6 traffic. NSD and US-CERT will continue to monitor the amount of IPv6 traffic that is traversing NCPS sensors and ensure that necessary signatures are implemented as the volume of IPv6 traffic increases.

At the same time, NCPS EINSTEIN 1 (Netflow) sensors have knowledge of encrypted sessions. NCPS will conduct a follow-up study to monitor the growth of encrypted traffic. In addition, NCPS is looking into pattern-based intrusion detection methods that are not hampered by encryption. NCPS will also coordinate with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to conduct an assessment of SCADA to understand the amount of SCADA traffic that passes through network gateways. ECD: July 31, 2016.

Recommendation 3: US-CERT to update the tool it uses to manage and deploy intrusion detection signatures to include the ability to more clearly link signatures to publicly available, open-source data repositories.

Response: Concur. The tool in question, SMS (Signature Management System), is undergoing software updates to respond to this recommendation. Specifically, the reference field will be made searchable and a new feature is being added so that analysts can tag signatures with searchable keywords. In addition, standard operating procedures



(SOPs) are being updated to ensure that references are properly noted in the associated reference field as well as the tagging system. ECD: December 31, 2016.

Recommendation 4: US-CERT to consider the viability of using vulnerability information, such as data from the Continuous Diagnostics and Mitigation program as it becomes available, as an input into the development and management of intrusion detection signatures.

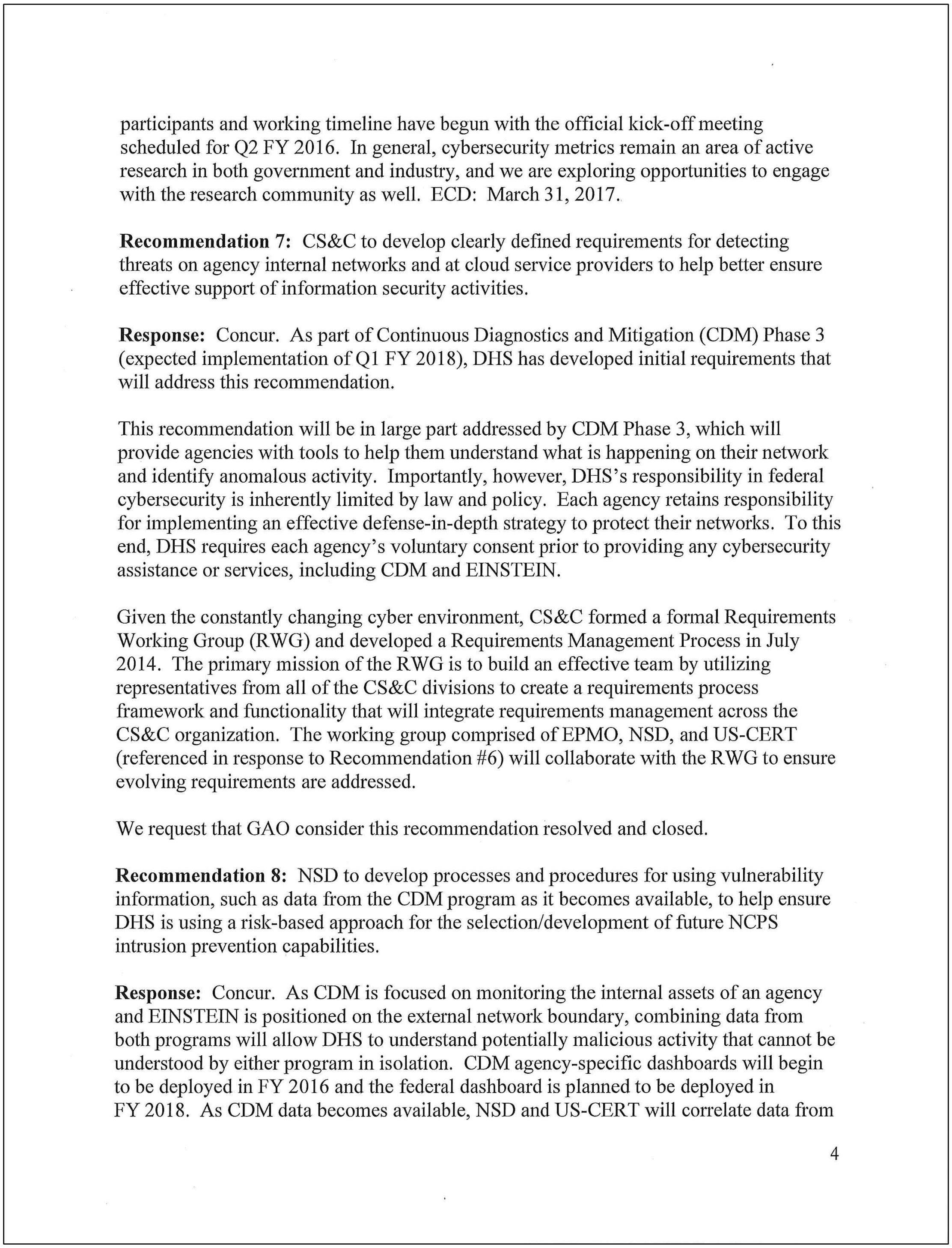
Response: Concur. US-CERT is currently developing a system for tracking the sources of threat information that are processed as well as recording actions taken or not taken with associated indicators. In combination, SOPs are being created to document the process that defines which sources of threat information are used for the creation of intrusion detection system signatures, including vulnerability data, as well as what actions should or should not be taken with associated indicators. ECD: December 31, 2016.

Recommendation 5: US-CERT to develop a timetable for finalizing the incident notification process, to ensure that customer agencies are being sent notifications of potential incidents, which clearly solicit feedback on the usefulness and timeliness of the notification.

Response: Concur. US-CERT has previously conducted a survey that solicited feedback from agencies. US-CERT will provide GAO with the survey results from earlier this year that addressed a separate GAO engagement (GAO-14-354, "Information Security: Agencies Need to Improve Cyber Incident Response Practices"). Going forward, US-CERT will ensure that these types of information and, specifically, feedback on timeliness and usefulness of incident reporting will be generated on a quarterly basis. ECD: December 31, 2016.

Recommendation 6: The Office of Cybersecurity and Communications (CS&C) to develop metrics that clearly measure the effectiveness of NCPS's efforts, including the quality, efficiency, and accuracy of supporting actions related to detecting and preventing intrusions, providing analytic services, and sharing cyber-related information.

Response: Concur. Currently NSD and US-CERT have metrics to gauge success of system performance and operations of the NCPS. In an effort to develop uniform metrics that include NSD, US-CERT, and other program area metrics, CS&C's Enterprise Performance Management Office (EPMO) will facilitate a working group, led by NSD and US-CERT, with appropriate program personnel to collaborate on the development of metrics that more clearly measure the value and impact of NCPS's efforts. Using industry best practices, the working group will hold brainstorming and verification and validation sessions, solicit input from .gov partners, and work with a statistician to assess the proposals before finalizing the metrics. Initial conversations to determine specific



participants and working timeline have begun with the official kick-off meeting scheduled for Q2 FY 2016. In general, cybersecurity metrics remain an area of active research in both government and industry, and we are exploring opportunities to engage with the research community as well. ECD: March 31, 2017.

Recommendation 7: CS&C to develop clearly defined requirements for detecting threats on agency internal networks and at cloud service providers to help better ensure effective support of information security activities.

Response: Concur. As part of Continuous Diagnostics and Mitigation (CDM) Phase 3 (expected implementation of Q1 FY 2018), DHS has developed initial requirements that will address this recommendation.

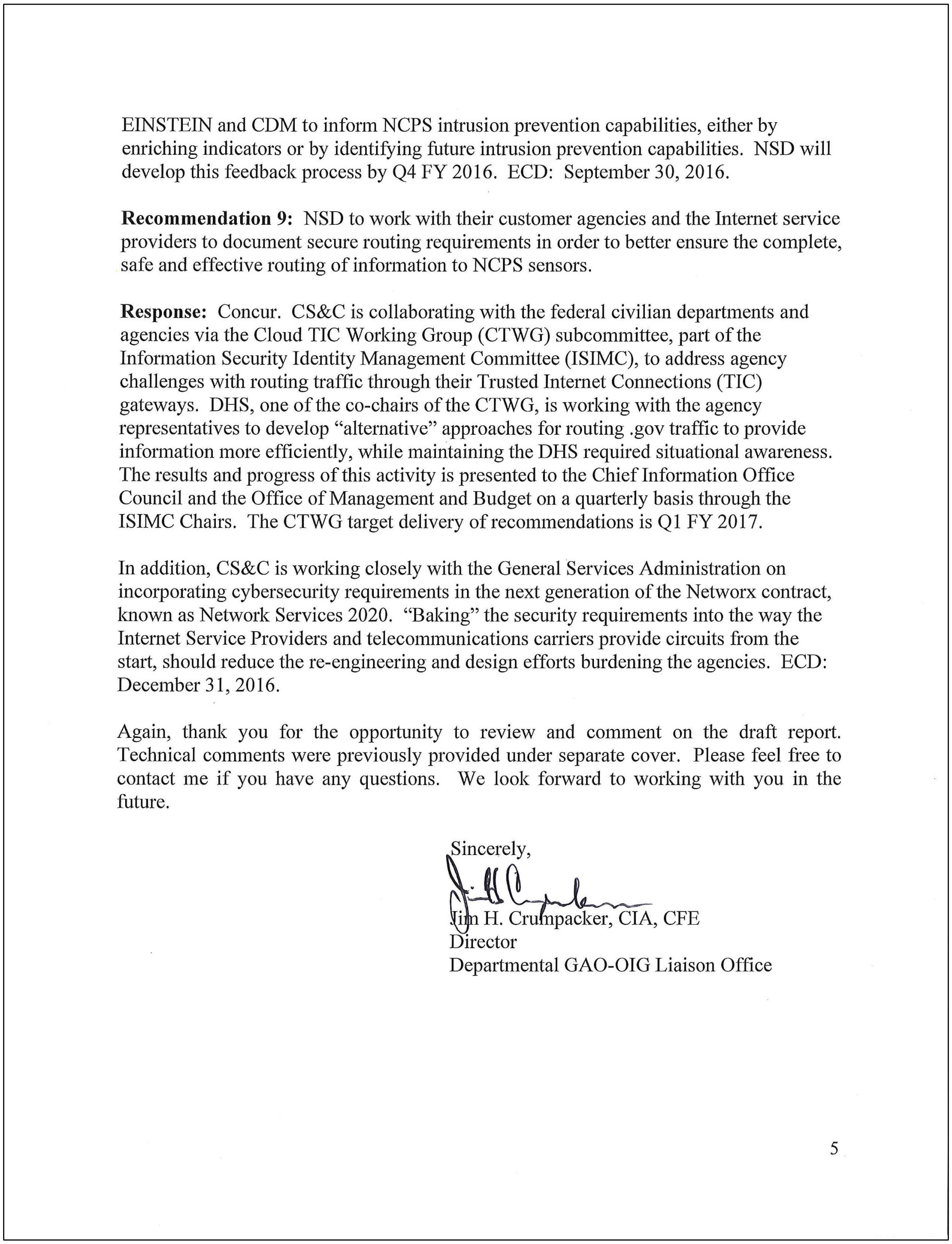
This recommendation will be in large part addressed by CDM Phase 3, which will provide agencies with tools to help them understand what is happening on their network and identify anomalous activity. Importantly, however, DHS's responsibility in federal cybersecurity is inherently limited by law and policy. Each agency retains responsibility for implementing an effective defense-in-depth strategy to protect their networks. To this end, DHS requires each agency's voluntary consent prior to providing any cybersecurity assistance or services, including CDM and EINSTEIN.

Given the constantly changing cyber environment, CS&C formed a formal Requirements Working Group (RWG) and developed a Requirements Management Process in July 2014. The primary mission of the RWG is to build an effective team by utilizing representatives from all of the CS&C divisions to create a requirements process framework and functionality that will integrate requirements management across the CS&C organization. The working group comprised of EPMO, NSD, and US-CERT (referenced in response to Recommendation #6) will collaborate with the RWG to ensure evolving requirements are addressed.

We request that GAO consider this recommendation resolved and closed.

Recommendation 8: NSD to develop processes and procedures for using vulnerability information, such as data from the CDM program as it becomes available, to help ensure DHS is using a risk-based approach for the selection/development of future NCPS intrusion prevention capabilities.

Response: Concur. As CDM is focused on monitoring the internal assets of an agency and EINSTEIN is positioned on the external network boundary, combining data from both programs will allow DHS to understand potentially malicious activity that cannot be understood by either program in isolation. CDM agency-specific dashboards will begin to be deployed in FY 2016 and the federal dashboard is planned to be deployed in FY 2018. As CDM data becomes available, NSD and US-CERT will correlate data from



EINSTEIN and CDM to inform NCPS intrusion prevention capabilities, either by enriching indicators or by identifying future intrusion prevention capabilities. NSD will develop this feedback process by Q4 FY 2016. ECD: September 30, 2016.

Recommendation 9: NSD to work with their customer 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.

Response: Concur. CS&C is collaborating with the federal civilian departments and agencies via the Cloud TIC Working Group (CTWG) subcommittee, part of the Information Security Identity Management Committee (ISIMC), to address agency challenges with routing traffic through their Trusted Internet Connections (TIC) gateways. DHS, one of the co-chairs of the CTWG, is working with the agency representatives to develop "alternative" approaches for routing .gov traffic to provide information more efficiently, while maintaining the DHS required situational awareness. The results and progress of this activity is presented to the Chief Information Office Council and the Office of Management and Budget on a quarterly basis through the ISIMC Chairs. The CTWG target delivery of recommendations is Q1 FY 2017.

In addition, CS&C is working closely with the General Services Administration on incorporating cybersecurity requirements in the next generation of the Networx contract, known as Network Services 2020. "Baking" the security requirements into the way the Internet Service Providers and telecommunications carriers provide circuits from the start, should reduce the re-engineering and design efforts burdening the agencies. ECD: December 31, 2016.

Again, thank you for the opportunity to review and comment on the draft report. Technical comments were previously 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.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov
Nabajyoti Barkakati, Ph.D., at (202) 512-4499 or barkakatin@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Lon C. Chin, Michael W. Gilmore, Harold Lewis, Christopher Warweg (assistant directors); Andrew Banister, Bradley Becker, Christopher Businsky, Kush K. Malhotra, Lee McCracken, and David Plocher made key contributions to this report.

(100476)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548