United States Government Accountability Office

Report to Congressional Requesters

CYBERSECURITY

DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program

Accessible Version

August 2020

GAO-20-598

August 2020

CYBERSECURITY

DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program

GAO Highlights

Highlights of GAO-20-598, a report to congressional requesters

Why GAO Did This Study

In 2013, DHS established the CDM program to strengthen the cybersecurity of government networks and systems by providing tools to agencies to continuously monitor their networks. The program, with estimated costs of about $10.9 billion, intends to provide capabilities for agencies to identify, prioritize, and mitigate cybersecurity vulnerabilities.

GAO was asked to review agencies' continuous monitoring practices. This report (1) examines the extent to which selected agencies have effectively implemented key CDM program requirements and (2) describes challenges agencies identified in implementing the requirements and steps DHS has taken to address these challenges.

GAO selected three agencies based on reported acquisition of CDM tools. GAO evaluated the agencies' implementation of CDM asset management capabilities, conducted semi-structured interviews with agency officials, and examined DHS actions.

What GAO Recommends

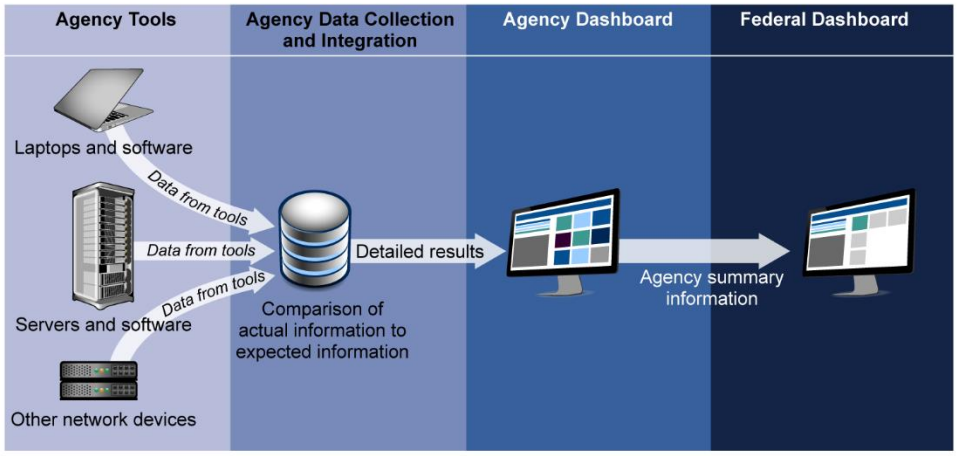
GAO is making six recommendations to DHS, including to ensure that contractors provide unique hardware identifiers; and nine recommendations to the three selected agencies, including to compare configurations to benchmarks. DHS and the selected agencies concurred with the recommendations.

View GAO-20-598. For more information, contact Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov.

What GAO Found

Selected agencies—the Federal Aviation Administration, Indian Health Services, and Small Business Administration—had generally deployed tools intended to provide cybersecurity data to support the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program. As depicted in the figure, the program relies on automated tools to identify hardware and software residing on agency networks. This information is aggregated and compared to expected outcomes, such as whether actual device configuration settings meet federal benchmarks. The information is then displayed on an agency dashboard and federal dashboard.

Continuous Diagnostics and Mitigation Program Data Flow from Agencies to the Federal Dashboard



Source: GAO analysis of Department of Homeland Security data. | GAO-20-598

However, while agencies reported that the program improved their network awareness, none of the three agencies had effectively implemented all key CDM program requirements. For example, the three agencies had not fully implemented requirements for managing their hardware. This was due in part to contractors, who install and troubleshoot the tools, not always providing unique identifying information. Accordingly, CDM tools did not provide an accurate count of the hardware on their networks. In addition, although most agencies implemented requirements for managing software, they were not consistently comparing configuration settings on their networks to federal core benchmarks intended to maintain a standard level of security.

The agencies identified various challenges to implementing the program, including overcoming resource limitations and not being able to resolve problems directly with contractors. DHS had taken numerous steps to help manage these challenges, including tracking risks of insufficient resources, providing forums for agencies to raise concerns, and allowing agencies to provide feedback to DHS on contractor performance.

Contents

Figures

Abbreviations

AWARE	agency-wide adaptive risk enumeration
CDM	continuous diagnostics and mitigation
CISA	Cybersecurity and Infrastructure Security Agency
DEFEND	Dynamic and Evolving Enterprise Network Defense
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FISMA	*Federal Information Security Modernization Act*
GSA	General Services Administration
HHS	Department of Health and Human Services
IHS	Indian Health Service
OMB	Office of Management and Budget
PMO	program management office
SBA	Small Business Administration

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

August 18, 2020

Congressional Requesters

Federal agencies rely heavily on information technology systems to carry out their missions, making the security of these systems vital due to the sensitive and essential data they contain. Moreover, these systems face increasing risks, from not only insider threats, but also from external threats of malicious attackers. As such, maintaining rigorous information security programs that provide timely, relevant, and accurate information is imperative.

One aspect of a rigorous information security program is continuously monitoring networks and systems to identify and manage risks. Toward this end, the Department of Homeland Security (DHS) developed the Continuous Diagnostics and Mitigation (CDM) program to strengthen the cybersecurity of government networks and systems by providing tools to agencies to support continuous monitoring of their networks.[1]

The CDM program includes capabilities intended to help agencies identify cybersecurity risks on an ongoing basis, use CDM information to prioritize the risks based on potential impacts, and then mitigate the most significant vulnerabilities first.[2] Each capability relies on several underlying tools, with associated requirements.

To establish the CDM program, in August 2013, DHS, in partnership with the General Services Administration (GSA), implemented a contracting vehicle intended to provide a government-wide set of continuous monitoring tools and services at a reduced cost to participating agencies.

[1]The CDM program uses hardware and software products (also referred to as tools) that have been installed on an agency's network. These tools automate the detection of hardware and software present on a network.

[2]Prioritization is a key component of risk-based protection and becomes necessary when requirements cannot be fully satisfied or when resources do not allow agencies to mitigate all risks within a reasonable time frame. See National Institute of Standards and Technology, *Special Publication 800-30: Guide for Conducting Risk Assessments* (Gaithersburg, MD: September 2012).

As of January 2020, DHS estimated that the total costs of the CDM program through 2031 would be $10.9 billion.[3]

You asked us to review the extent to which agencies are following applicable federal guidance for continuous monitoring programs. The CDM program provides a means for agencies to implement continuous monitoring. Our specific objectives for this review were to (1) examine the extent to which selected agencies have effectively implemented key CDM program requirements and (2) describe challenges, if any, that agencies have identified in implementing the requirements and steps DHS has taken to address these challenges.

To address the first objective, we initially identified all of the agencies participating in the CDM program using program information provided by DHS. We then sorted the agencies based on the number of hardware devices connected to their unclassified network(s), as reported by each agency in its fiscal year 2018 annual *Federal Information Security Modernization Act* (FISMA) report to Congress.[4] Specifically, we organized the agencies into three groups—those agencies with up to 26,000 connected devices, those agencies with 26,000 to 190,000 connected devices, and those agencies with more than 190,000 connected devices.[5]

We then assigned each agency a score to reflect its average acquisition status—that is, where each agency was in the process of acquiring CDM tools as of November 2018. To determine this score, we assigned points

[3]The $10.9 billion estimate includes costs for DHS to manage the CDM program and costs for agencies to operate and maintain tools.

[4]The *Federal Information Security Modernization Act of 2014* (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect. We included the 27 agencies that were both (1) associated with CDM contract awards in 2017 and 2018 and (2) required to issue an annual FISMA report.

[5]We chose these ranges because doing so resulted in three groups of nine agencies each.

to agencies dependent upon whether DHS reported that agencies had completed acquisition of tools supporting the CDM program or not.[6]

We assessed the reliability of the tool acquisition data by (1) interviewing DHS officials to understand the purpose of the data and context surrounding its collection and (2) reviewing the completeness of the data. We determined the data to be reliable for the purpose of selecting agencies for our review.

Using the assigned scores, we then selected one agency from each of the three groups of agencies, based on the tool acquisition status. Specifically, from each group, we chose the agency that we determined to have the highest calculated score, indicating that the agency was farther along in the acquisition process. The three agencies that resulted from our selections were the Department of Health and Human Services (HHS), the Department of Transportation (DOT), and the Small Business Administration (SBA).[7]

Because HHS and DOT have component-level agencies, we then selected one component-level agency within each of these departments. We selected the component agency with the highest calculated tool acquisition status score, applying a similar approach as for the department-level agencies.[8] The resulting component-level agencies that we selected were the Indian Health Service (IHS) within HHS and the

[6]DHS provided data on the acquisition status of tools supporting the CDM program at each participating agency. We focused on the tools supporting four CDM capabilities. For each capability, we assigned a score of 1 if the acquisition process had been completed for the capability and a 0 if the tool acquisition process had not been started or was in progress. For example, we assigned a score of four if an agency had completed the acquisition process for all four capabilities. If an agency had component organizations, we averaged the scores of the agency and its components to compute an overall score for the agency.

[7]During the course of our field work, SBA was in the process of implementing a pilot project with DHS for an alternative cloud-based solution for CDM. We did not include this effort in the scope of our review because it was ongoing at the time.

[8]In cases where multiple component agencies had the same score, we selected the component agency that reported the most agency-operated high-impact systems in its fiscal year 2018 FISMA report. A “high impact” system is an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a *Federal Information Processing Standard Publication 199* potential impact value of high. A potential impact value is high if the loss of confidentiality, integrity, or availability of a system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Federal Aviation Administration (FAA) within DOT. Overall, our final agency selections for reviewing the extent that agencies had implemented CDM program requirements were FAA, IHS, and SBA.

We next reviewed DHS's *Continuous Diagnostics and Mitigation (CDM) Technical Capabilities Volume Two Requirements Catalog*[9] to identify the functional and operational requirements defined by the CDM Program Management Office (PMO)[10] for the underlying tools that support capabilities within the asset management area of the CDM program. Asset management includes four capabilities: the ability to manage (1) hardware, (2) software, (3) configuration settings, and (4) vulnerabilities.[11] We chose to focus on the asset management program area because this area was to be the initial phase of CDM implementation; thus, agencies would be expected to be farther along with this area of implementation.[12] From the functional and operational requirements, we selected those that we considered to be key requirements due to their importance in implementing CDM.

We then reviewed the tools that FAA, IHS, and SBA had deployed for implementing the four capabilities associated with the asset management program area. We evaluated whether each agency had configured and used these tools in a manner that met the selected functional and operational requirements for the four capabilities. We also interviewed agency CDM program staff to gain an understanding of each agency's operating environment and CDM implementation status.

These agencies may have had other monitoring tools in place in addition to the tools associated with the CDM program. However, evaluating other agency tools was not within the scope of this review; we focused solely on those tools that the agencies had deployed to directly support the

[9]Department of Homeland Security, *Continuous Diagnostics and Mitigation (CDM) Technical Capabilities Volume Two Requirements Catalog* (Washington, D.C.: May 11, 2018).

[10]The CDM Program Management Office exists within DHS's Cybersecurity and Infrastructure Security Agency.

[11]Asset management is one of four CDM program areas.

[12]Three other CDM program areas—identity and access management, network security management, and data protection management—were to be implemented later. However, in 2018, the CDM Program Management Office changed its position on phased implementation of the areas and decided that agencies could implement the capabilities associated with each of the four program areas concurrently.

CDM program. The results of our work are specific to the selected agencies and, therefore, are not generalizable to federal agencies as a whole.

To address the second objective, we conducted semi-structured interviews[13] with knowledgeable officials at selected agencies. In addition to the three agencies we examined for our first objective and the two associated departments, we selected three additional agencies, for a total of eight agencies.

To identify the three additional agencies, we performed a selection process similar to that used for the first objective, but chose agencies that had the lowest calculated tool acquisition status scores. The additional agencies resulting from this process were the Department of Justice, the Federal Deposit Insurance Corporation, and the Federal Communications Commission. These three agencies and FAA, DOT, IHS, HHS, and SBA made up our total selection of agencies.[14]

Our semi-structured interviews consisted of questions regarding the interactions between each agency and DHS, the Office of Management and Budget (OMB), and the agency's CDM integrator.[15] These interviews also included questions regarding the acquisition, installation and configuration, and usage and maintenance of the tools associated with the four capabilities within the CDM asset management program area. We used these questions to facilitate a conversation with the CDM program staff at each agency regarding what went well and what did not go well during CDM program implementation and what agencies might do differently.

Using the information collected during the semi-structured interviews with agency officials, we performed a content analysis to formulate a list of

[13]A semi-structured interview methodology generally involves asking a set of questions of multiple interviewees. We used a semi-structured interview format with both closed- and open-ended questions. The intent of our open-ended questions was to engage the agency officials in a conversation about the topics discussed.

[14]As of December 2019, the Federal Communications Commission had participated in an assessment of their operating environment, but had not formally begun participation in the CDM program. Because of this, we included only the information from the commission that was applicable to our engagement, based on our judgment.

[15]Integrators are private-sector organizations (i.e., contractors) selected by the General Services Administration to install and configure CDM tools on the agency's network.

challenges associated with implementing the CDM program requirements.[16] The list of challenges reflected the experiences and views of only those agencies that participated in the semi-structured interviews and, therefore, are not generalizable to federal agencies as a whole. Regardless of this limitation, the solicited perspectives provided insight into the experiences and views of the selected agencies.

We discussed the results of our content analysis with each of the agencies in our review in order to confirm our characterization of the challenges and to determine whether any agencies had identified additional challenges. We also discussed the identified challenges with the CDM PMO at DHS to understand if that office had taken any actions to manage the identified challenges. In addition, we reviewed relevant CDM documentation that described how DHS intended to manage the identified challenges.

We conducted this performance audit from February 2019 through August 2020 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.

Background

DHS established CDM to support government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity. The objectives of the CDM program are to:

- reduce the agency threat surface,[17]
- increase visibility into the cybersecurity posture of agencies,

[16]To perform the content analysis, two analysts independently summarized the transcripts from our semi-structured interviews. These analysts then used the summaries to reach consensus on recurring themes that described challenges to agencies implementing CDM program requirements.

[17]A threat surface consists of all hardware and software that may be exposed to compromise due to insecure configurations or known vulnerabilities. Keeping threat surfaces as small as possible is a basic security measure.

- improve an agency's ability to respond to cybersecurity issues, and
- streamline FISMA reporting.[18]

The program is intended to allow federal agencies to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at both the individual agency and federal levels.

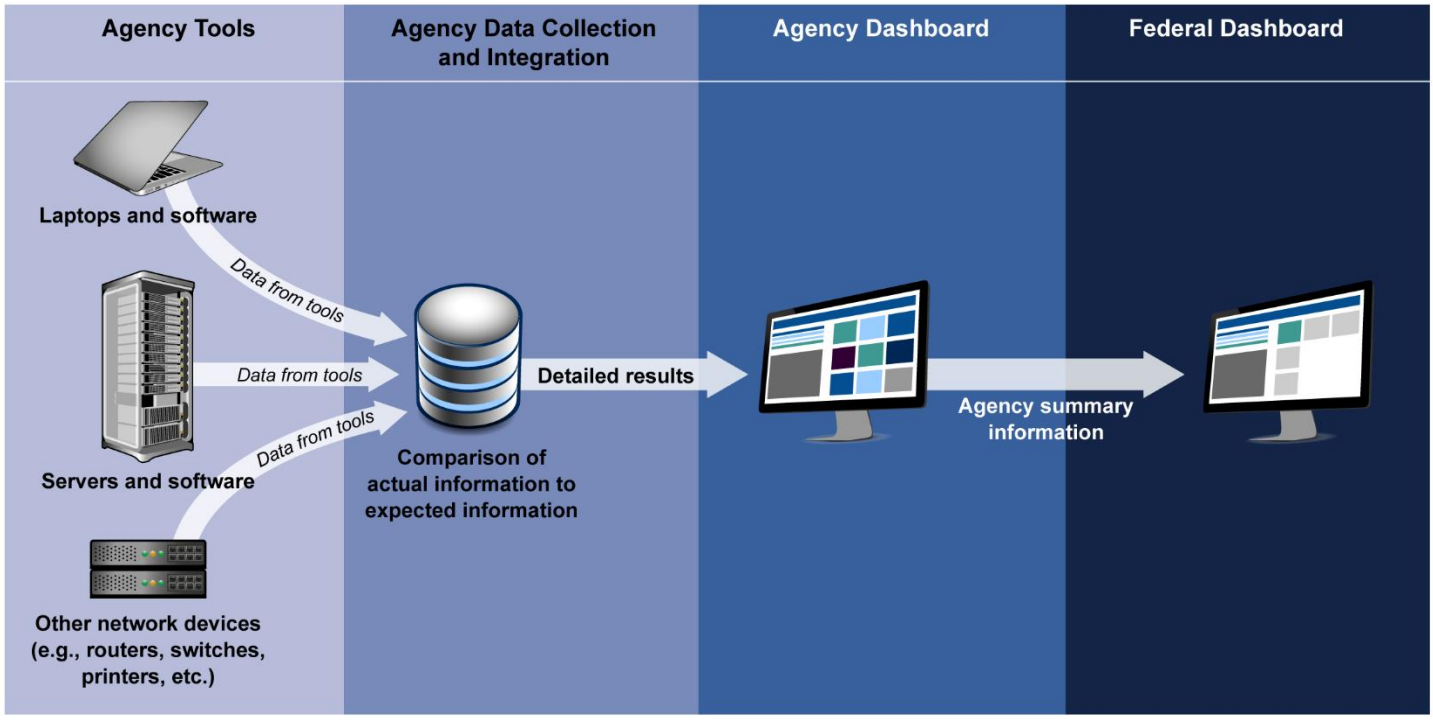
As depicted in figure 1, automated tools send information they have collected about hardware devices, including any associated software, connected to an agency's network to a collection point that compares the information with expected outcomes, such as whether actual device configuration settings meet agency or federal core benchmarks.[19] The results of these comparisons are then sent to an electronic visual display at an agency, referred to as the agency dashboard. The agency dashboard summarizes the information and sends it to a federal dashboard that is managed by DHS's Cybersecurity and Infrastructure Security Agency (CISA).[20] The federal dashboard includes summary information about the security of agencies' networks.

[18]FISMA requires agencies to report annually to OMB, DHS, certain congressional committees, and the Comptroller General on the adequacy and effectiveness of their information security policies and procedures. OMB and DHS work with interagency partners to develop the Chief Information Officer FISMA metrics, which are intended to be used by the agencies, OMB, and DHS to track agencies' progress in implementing cybersecurity capabilities. Further, FISMA requires OMB to report annually, in consultation with DHS, on the effectiveness of agency information security policies and practices.

[19]Federal core configuration benchmarks contain instructions or procedures for configuring hardware or software products to maintain a standard level of security. However, based on business needs and risk acceptance strategies, agencies may alter the federal benchmarks. These agency-specific variations represent the desired state of configuration settings for hardware and software on an agency's network.

[20]The Cybersecurity and Infrastructure Security Agency works with each federal civilian department and agency to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats.

Figure 1: Continuous Diagnostics and Mitigation Program Data Flow

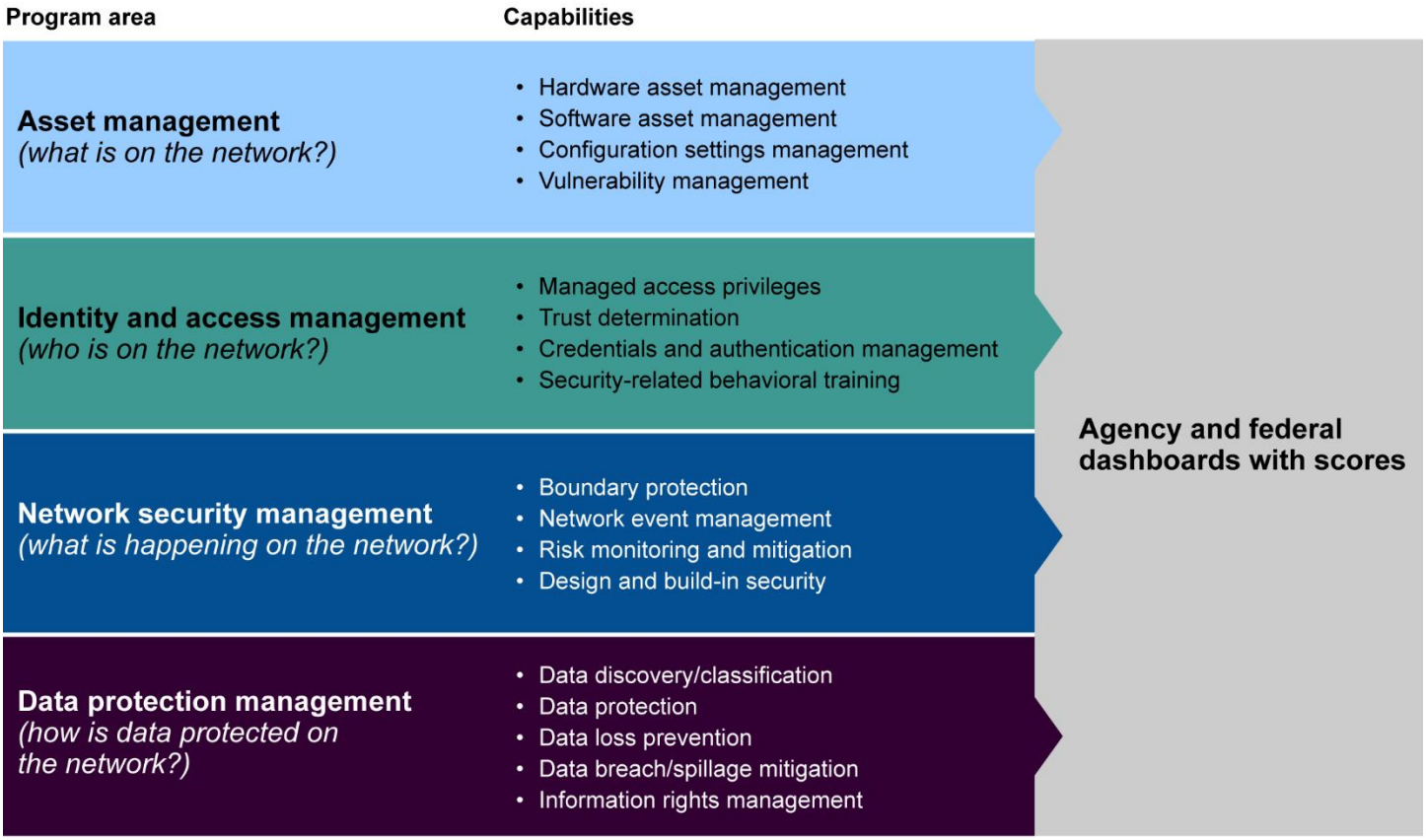


Source: GAO analysis of Department of Homeland Security data. | GAO-20-598

CDM Consists of Program Areas, Dashboards, and Risk Scores

DHS organized CDM into four program areas: asset management, identity and access management, network and security management, and data protection. The department further subdivided each program area into capabilities intended to support each area. Each of these program areas is to feed data to agency and federal dashboards, which include risk scores. Figure 2 depicts the CDM program areas with their associated capabilities.

Figure 2: Continuous Diagnostics and Mitigation Program Areas and Their Associated Capabilities



Source: GAO analysis of Department of Homeland Security data. | GAO-20-598

The asset management area, which is the focus of our review, involves managing what is on an agency's network. Specifically, this area requires identifying all hardware and software present on the network and addressing whether the agency has authorized the hardware to be on the network. In addition, it requires the tracking and management of software, configuration settings, and known vulnerabilities present on the network. Table 1 describes the tools used to provide the four capabilities associated with the asset management program area. Appendix I further summarizes the three other CDM program areas: identity and access management, network and security management, and data protection.

Table 1: Tools Associated with the Four Continuous Diagnostics and Mitigation Program Asset Management Capabilities

Capability	Purpose of tools	Examples of tools
Hardware asset management is to identify all hardware on the agency's network. It is the foundational capability for asset management; all other capabilities depend on its successful implementation.	To identify and collect inventory information for the hardware connected to an agency's network.	• Scanning tools that continuously or periodically examine network infrastructure to detect hardware devices • Tools that monitor outgoing and incoming network data for device identification
Software asset management is to ensure that software and associated objects are identified and authorized.	To scan and manage the software installed on hardware.	• Software version scanning tools to detect unauthorized or outdated versions of software • License management tools to control where and how software products are able to run
Configuration settings management is to identify misconfigurations that may be susceptible to exploitation.	To ensure that the hardware connected to an agency's network and the software on that hardware is configured in accordance with configuration benchmarks.	• Configuration assessment tools to automate the deployment of specific configuration standards on an agency's network • Continuous evaluation assessment tools to regularly scan configuration settings on an agency's network • Common configuration scoring system tools to measure the severity of software configuration issues on devices connected to a network
Vulnerability management is to ensure that known vulnerabilities are identified and prioritized for mitigation.	To ensure that agencies are regularly scanning their networks for vulnerabilities that may be introduced to their networks by the hardware connected to them.	• Vulnerability scanners to detect vulnerabilities in an agency's hardware and software • Web application scanners to detect vulnerabilities in web applications running on an agency's network • Database scanners to detect vulnerabilities in databases on an agency's network

Source: GAO analysis of Department of Homeland Security documentation. | GAO-20-598

The CDM program provides agencies and CISA with dashboard views of the data collected by the CDM tools, as well as a common scoring system to help officials understand their agency's security posture.

Agency CDM dashboards and the DHS federal CDM dashboard. The CDM program provides each agency with a dashboard that receives, aggregates, and displays information from the CDM tools installed on its network. The agency dashboard is to produce alerts to notify dashboard users of critical issues requiring immediate attention. As noted previously, agency dashboards send data to a federal CDM dashboard maintained by CISA. The federal dashboard is to display summary information for

each agency's cybersecurity posture. OMB requires agencies to meet federal dashboard reporting requirements.[21]

Agency-wide adaptive risk enumeration (AWARE) scores. DHS established AWARE scores to provide a standardized method to compare the security status of agencies' networks across federal civilian agencies. Agency dashboards calculate several types of AWARE scores based on parameters and formulas, using data collected by an agency's CDM tools. Such data includes unauthorized hardware, configuration settings, and vulnerabilities. For example, for vulnerabilities detected on a given hardware device, the calculation of the score related to vulnerabilities considers vulnerability type, how long the vulnerability has existed, whether the vulnerability occurs on a high-impact system,[22] and other factors, including the impact a vulnerability could have on an agency.

Multiple Stakeholders Are Responsible for Implementing the CDM Program

The CDM program requires coordination among various stakeholders that are responsible for implementing the program. Each stakeholder has specific roles and responsibilities within the program.

DHS: FISMA specifies DHS's responsibilities for assisting federal agencies with securing their information and systems, including providing operational and technical assistance to agencies and monitoring agencies' implementation of information security policies and practices. To provide a common set of requirements in support of the implementation of the CDM capabilities described previously, DHS published a set of functional and operational requirements in its *Continuous Diagnostics and Mitigation (CDM) Technical Capabilities*

[21]Office of Management and Budget, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, OMB Memorandum M-20-04 (Washington, D.C.: Nov. 19, 2019).

[22]A "high impact" system is an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a *Federal Information Processing Standard Publication 199* potential impact value of high. A potential impact value is high if the loss of confidentiality, integrity, or availability of a system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Volume Two Requirements Catalog.[23] In addition, DHS (specifically the CDM PMO) signs agreements with each agency participating in the program to outline the responsibilities for each in implementing the CDM program requirements. The agreements require the PMO to, among other things, solicit feedback from participating agencies regarding their experiences in implementing the CDM program requirements. As the program's technical point of contact, the PMO is responsible for ensuring that the integrators—private-sector organizations selected by GSA to install and configure CDM tools on the agency's network—perform at an acceptable level.

GSA: GSA partnered with DHS to establish government-wide contracts to provide a consistent government-wide set of information security continuous monitoring tools and services to agencies. GSA is to provide oversight for the acquisition of CDM tools and services.

Integrators: As previously noted, integrators are private sector organizations selected by GSA to install and configure tools on an agency's network. Each integrator is to develop an implementation solution (in consultation with each participating federal agency and DHS) that supports the CDM functional and operational requirements.[24] The integrator is responsible for troubleshooting problems with the data that the tools send to the agency's CDM dashboard and the federal CDM dashboard.

Participating agencies:[25] The PMO emphasizes the importance of agency staff working closely with DHS and the integrators to ensure that CDM capabilities are properly implemented and achieve intended objectives. Each agency is required to evaluate integrator implementation

[23]Department of Homeland Security, *Continuous Diagnostics and Mitigation (CDM) Technical Capabilities Volume Two Requirements Catalog* (Washington, D.C.: May 11, 2018). DHS's *Continuous Diagnostics and Mitigation (CDM) Technical Capabilities Volume One Defining Actual and Desired States*, issued in July 2017, provides agencies with additional guidance on configuring CDM tools.

[24]The integrators, as of December 2019, were Booz Allen Hamilton, CACI International, CGI Federal, and ManTech International.

[25]To manage the implementation of CDM tools and services, the PMO organized participating agencies into multiple groups. The PMO grouped agencies based on, among other things, the toolsets used by each agency in order to leverage collective license procurement and demographics, such as network configuration. As of April 2020, there were six groups of agencies, with an integrator assigned to support each group.

plans, and operate and maintain the CDM tools once the integrator has installed and configured them.[26] While DHS covers the initial funding for implementation of the tools supporting the capabilities, agencies are responsible for funding the ongoing operations and maintenance of the tools.

Selected Agencies Did Not Effectively Implement All Key CDM Requirements for Managing Assets

FAA, IHS, and SBA—the three agencies selected for our review—had generally deployed CDM tools intended to support the four capabilities associated with the asset management program area across their networks and had installed agency dashboards to receive and display asset management information. However, these agencies had not effectively implemented several key CDM program requirements for the capabilities.[27]

Specifically, the three agencies had not fully implemented requirements for managing their hardware, although this capability is foundational to the success of the other three asset management capabilities. For example, agencies' hardware inventories were missing information and contained duplicate hardware information. In addition, although agencies generally implemented requirements for managing software, they were not consistently comparing configuration settings on their networks to federal core benchmarks and agency-specific variations. Further, although the three agencies were generally meeting program requirements for scanning their networks for vulnerabilities, their CDM tools did not include

[26]Agencies are responsible for operating and maintaining the tools that collect information about hardware and software detected on an agency's network. The integrator is responsible for maintaining the tools that compare this information with expected outcomes and the agency CDM dashboard.

[27]Agencies may have had other tools in place in addition to the tools associated with CDM. However, evaluating the effectiveness of the implementation of those tools was not within the scope of this review.

all required information.[28] Moreover, poor data quality caused, in part, by these shortcomings diminished the usefulness of the agencies' dashboards.

Agencies' Hardware Inventories Were Missing Information and Contained Duplicates

The hardware asset management capability is intended to lay the foundation for implementing all other asset management capabilities. It is intended to ensure that only authorized hardware is connected to agency networks. To implement this capability, the hardware management capability is to provide a single unique identifier for each hardware device on an agency network and periodically update hardware information.[29]

DHS also requires that agencies use CDM tools to record the authorization status of hardware on an agency's network. For the purpose of CDM, hardware is considered authorized when a specific hardware device is associated with a FISMA system.[30] DHS—in its role as liaison between agencies and integrators—is to ensure that agencies and integrators work to implement CDM requirements effectively.

The three selected agencies had deployed CDM tools for managing hardware and reported improvements in hardware tracking, including identifying previously unknown hardware on their networks. However, the

[28]According to officials in SBA's Office of the Chief Information Officer, the agency implemented a more accurate cloud-based solution that meets the CDM program objectives. In December 2016, SBA suggested the alternate solution to DHS and began a 90-day pilot in March 2019. SBA and CISA issued a report in November 2019 that stated that the pilot met the intent of the objectives of the CDM program and partially met the requirements associated with managing hardware, software, configuration settings, and vulnerabilities. The report that SBA provided us did not specify which requirements were partially met. As noted in our methodology, we did not include the pilot in the scope of our review because it was ongoing during the course of our work.

[29]DHS guidance states that agencies should strive to update CDM information at least every 72 hours, but provides flexibility to account for agency business needs.

[30]FISMA requires an agency to provide information security protections to secure information systems operated by the agency or by contractors on behalf of the agency commensurate with the risk and magnitude of harm resulting from compromise of (1) information collected by or on behalf of the agency and (2) information systems used or operated by the agency or by a contractor (or other organization) on behalf of the agency. For the purpose of this review, we refer to systems secured in this manner as FISMA systems. A FISMA system consists of hardware devices that support its operations. A hardware device is associated with a FISMA system when the CDM tools record which system the device supports.

agencies had not fully implemented key program requirements. Specifically:

Agencies' CDM tools provided multiple identifiers for hardware on agency networks. An identifier supports agency management of hardware by ensuring the agency can accurately track hardware on its network. To do so, each hardware device should have a single unique identifier.

However, the agencies' tools did not provide unique identifiers. For example, at one agency, its tools assigned at least two identifiers for approximately 40 percent of its hardware devices in one of its operating environments.

According to DHS's CDM PMO, integrators are ultimately responsible for the information that appears in the CDM tools. However, for its part, DHS had not ensured that integrators' solutions effectively provided unique identifiers for hardware. DHS was aware of the problem of single hardware devices having multiple identifiers and had issued guidance in March 2019 stating that agencies and integrators should work to resolve this shortcoming. However, as of April 2020, the shortcoming had not been resolved.

Until DHS ensures that integrators implement this guidance, the CDM tools will not provide a single unique identifier to each hardware device, and agencies will not have an accurate count of how many devices are connected to their networks. In addition, an agency's AWARE scores will be inaccurate. Further, incorrect information about the number of devices undermines CDM's goal of streamlining FISMA reporting because several FISMA metrics depend on accurate device counts.

Agencies effectively used CDM tools to periodically update hardware inventory information. The CDM tools used at all three agencies automatically updated information as new hardware connected to their networks. Therefore, the tools updated information in real time.

The three agencies had not used CDM tools to fully record required information about their authorized hardware inventory. The inventory information was not fully populated in the tools we reviewed. Specifically, at each agency,

- FAA had partially associated its hardware with FISMA systems in its CDM tools. Specifically, as of April 2020, the agency had used

CDM tools to associate most of the hardware on its network with six FISMA systems. However, the agency was still in the process of documenting the remainder of its hardware in a format that could be used by the CDM tools. Although FAA had approximately 200 systems in its inventory, agency CDM staff stated that, in addition to the hardware associated with six systems, they planned to associate the remaining hardware with approximately six additional systems, but had not specified a time frame for completing this effort. According to the staff, these 12 primary systems support the remaining systems and the agency's integrator designed the CDM tools to only record hardware for these primary systems, rather than potentially associating specific hardware devices with multiple systems that may use it. The staff also stated that the problem with multiple identifiers described above also negatively affected their ability to associate the devices with systems.

- IHS had not used CDM tools to associate hardware with FISMA systems. Although the agency had associated hardware with FISMA systems in agency documentation, this information was not in a format that could be readily integrated into the CDM tools. Therefore, the integrator had not recorded the data into the tools. Agency CDM staff reported that they would need to manually record this information in a format compatible with the tools, but they lacked the resources to perform this work. According to IHS's Chief Information Officer, the agency was working to resolve these resource issues but had not yet done so.
- SBA maintained a repository that associated hardware with FISMA systems on its network. The agency maintained this information manually outside of CDM, but also employed an automated process to import the information into the CDM tools. However, the tools did not include associated systems for all hardware. According to agency CDM staff, the agency was still in the process of associating systems with hardware. Nevertheless, SBA had not specified a time frame for completing this effort.

Further, DHS had not ensured agencies and integrators had incorporated this information into CDM. According to the CDM PMO, agencies and integrators both play a role in ensuring that hardware is associated with FISMA systems in the CDM tools.

Until agencies fully prepare hardware inventory information, such as the FISMA systems using its hardware, and maintain it in a format that can be readily incorporated into the CDM tools, their integrators will not be able

to record the information. In addition, until DHS, in its role as liaison between agencies and integrators, works with agency integrators to record this information, agencies will not be able to identify devices that are unauthorized in a timely manner. Without having complete hardware information in the CDM tools, agency and federal dashboards will not accurately portray an agency's security posture. Further, having unauthorized devices on a network increases the risk that an agency's network may be compromised.

Most Agencies Implemented Requirements for Managing Software

The software asset management capability is intended to ensure that agencies know what software is installed on hardware managed by the hardware asset management capability. DHS requires agencies to use CDM tools to uniquely identify all software present on an agency's network. DHS also requires agencies to update software information periodically. DHS—in its role as liaison between agencies and integrators—is to ensure that agencies and integrators work to implement CDM requirements effectively.

Two of the three selected agencies had implemented tools to manage software on their networks, but the third agency had not.

SBA had not deployed CDM tools for managing its software. SBA CDM officials stated that the agency had not implemented software asset management because the tools provided by the integrator caused agency devices to malfunction and crash. According to the CDM PMO, as of May 2020, the office was working with the agency and its integrator to implement an alternate solution that is expected to work in the agency's environment to support software asset management requirements, including uniquely identifying software and periodically updating software information. If implemented effectively, SBA should be able to manage its software within the CDM program and provide software information to its CDM agency dashboard.

The other two agencies, FAA and IHS, had deployed CDM tools for managing software and had implemented key requirements. Specifically:

FAA and IHS used CDM tools to provide unique identifiers for software. Therefore, the CDM tools uniquely identified software on agency devices, such as servers and workstations.

FAA and IHS had configured CDM tools to collect information on software periodically. Specifically, the two agencies had configured the tools to gather software information, such as software name and unique identifier. FAA collected this information at least every 3 days, while IHS collected it every 5 days.

Agencies Had Deployed Tools to Manage Configurations, but Did Not Effectively Implement Key Requirements

The configuration settings management capability is intended to ensure that hardware and software on an agency's network are configured in a secure manner. To implement configuration management, DHS requires that agencies document agency-specific variations from federal core configuration benchmarks for each type of hardware and software on their networks. Agencies are to base these variations on business needs and risk acceptance strategies.

Additionally, DHS requires agencies to use CDM tools to compare configurations against both federal core benchmarks and agency-specific variations. The agency dashboard uses the results of an agency's comparison of its configuration settings versus the federal core benchmarks to compute the federal AWARE score. DHS also requires agencies to update configuration scan results periodically.

Although FAA, IHS, and SBA had deployed CDM tools for managing configurations, they had not fully implemented key configuration management requirements. Specifically:

The three agencies documented agency-specific variations to a limited extent.

- FAA had documented agency-specific variations to the federal core configuration benchmarks for three operating systems on its network. However, agency officials stated that they had not defined variations for the remaining 16 operating systems. FAA CDM staff stated that a portion of the 16 systems were older operating systems and the agency was working to remove these older systems from its environment. As a result, the staff had not created agency-specific variations for these older systems. For the remainder of the 16 operating systems, the staff stated that documenting agency-specific variations was a low priority

because DHS used federal core benchmarks instead of agency-specific variations to calculate the federal AWARE score.

- IHS had documented Windows operating system variations in its CDM tool, but had not documented variations for other operating systems. IHS CDM staff stated that a lack of resources had prevented the agency from documenting other operating systems.
- According to SBA CDM staff, the agency used federal benchmarks as a baseline for documenting agency-specific variations in its CDM tool. However, we did not identify any agency-specific variations in the tool's files provided to us by SBA for its operating systems.

Agencies used CDM tools inconsistently when comparing configuration settings against both federal core benchmarks and agency-specific variations.

- FAA used CDM tools to compare configuration settings to federal core benchmarks for 14 operating systems on its network, but had not compared their settings to benchmarks for five other operating systems. In addition, the agency had not consistently compared configuration settings to agency-specific variations. For the agency-specific variations, FAA only compared settings for three operating systems on its network. As previously noted, documenting agency-specific variations was a low priority at FAA.
- Because IHS had documented its variations in its CDM tool, the tool compared configuration settings to agency-specific variations. However, the CDM tool did not compare settings to the federal core benchmarks. According to IHS CDM staff, the agency prioritized the comparison to its agency-specific variations because this information was more useful to the agency with its limited resources.
- SBA used its CDM tool to compare its configuration settings to federal core benchmarks, but not to agency-specific variations. As described above, although agency staff stated SBA had documented agency-specific variations in its CDM tool, we did not identify these variations during our review.

Agencies configured CDM tools to update configuration scan results according to defined schedules. Specifically, FAA had scheduled its CDM tool to scan across its network at least every 3 days. In addition, IHS configured its CDM tool to collect configuration scan results every 5 days and SBA had scheduled its CDM tool to scan weekly.

Although agencies updated their scan results according to schedules, by not documenting and comparing configuration settings to agency-specific variations for all operating systems in use, agencies will lack important configuration information. Such information is needed to ensure that agencies have configured their hardware and software in a manner that meets agency business needs and risk acceptance strategies. Additionally, if agencies do not compare their configuration settings to federal core configuration benchmarks consistently with CDM tools, DHS's ability to increase its visibility into the federal cybersecurity posture is likely to be diminished.

Agencies' Tools Did Not Fully Address a Requirement to Manage Vulnerabilities

The vulnerability management capability is intended to ensure that agencies are aware of known vulnerabilities that exist on hardware and software on their networks. To implement this capability, DHS requires agencies to use CDM tools to collect detected vulnerability information, such as the time a vulnerability is first detected and the time of its remediation. DHS also requires vulnerability scans to be performed periodically. In addition, DHS requires agencies to update the tools in a timely manner to detect newly discovered vulnerabilities.[31] DHS—in its role as liaison between agencies and integrators—is to ensure that agencies and integrators work to implement CDM requirements effectively.

Agencies had installed tools to manage vulnerabilities, but their tools did not fully address a key requirement. Specifically:

Agencies' CDM tools collected required information on the time a vulnerability was first detected, but had not collected the time a vulnerability was remediated. For each agency:

- FAA used CDM tools to collect information about the first time a vulnerability was detected but not the time it was remediated. Agency CDM staff stated that the integrator would need to make changes to how the CDM tools recorded vulnerability information.

[31]It is critical that vulnerability management tools be updated with new vulnerability definitions—tool readable files that contain information about known vulnerabilities—to provide protection against the most current known threats.

The staff further stated that the time of remediation information was unreliable.

- IHS used CDM tools to collect information about the first time a vulnerability was detected, but it did not collect information on the time that a vulnerability was remediated. IHS CDM staff stated that the agency lacked system storage necessary to retain vulnerability remediation information.
- SBA used CDM tools to collect information on the time a vulnerability was first detected but not the time it was remediated. Agency staff stated that the integrator's CDM solution did not provide a mechanism to capture this information.

According to DHS's CDM PMO, integrators are ultimately responsible for the information that appears in the CDM tools. However, DHS had not ensured that integrators had incorporated the time of remediation information. Until DHS works with the integrators to ensure that the time of remediation is included in the information collected by the CDM tools, agencies will not have up-to-date knowledge of their security posture and may waste resources addressing vulnerabilities that have already been remediated.

Agencies configured CDM tools to scan for vulnerabilities according to defined schedules. Specifically, FAA had scheduled a CDM tool to scan select servers at least weekly and other devices at least monthly. The agency also used another CDM tool for more frequent system monitoring and reporting every 15 minutes. In addition, IHS configured its CDM tool to scan for vulnerabilities twice per week and SBA configured its tool to scan weekly.

At least one agency had not updated its CDM tool in a timely manner.

- At the time of our meeting with the agency in September 2019, FAA's CDM tool was the most recent version and the agency was using current vulnerability definition files, enabling the tool to detect new vulnerabilities on its network.
- At the time of our site visit to IHS in July 2019, the agency had not updated its vulnerability scanning tool because the license for its CDM tool had expired a month earlier. However, the agency acquired a new license in October 2019 and then updated the tool to allow scans to detect vulnerabilities that were more recent.

- At the time of our site visit in November 2019, SBA's CDM tool was the most recent version and was using current vulnerability definition files, enabling the tool to detect new vulnerabilities on the agency's network.

Poor Data Quality Diminished the Usefulness of Dashboards and Risk Scores

DHS provides agencies with CDM dashboards, which are populated with information gathered by agency CDM tools for hardware, software, configuration settings, and vulnerabilities. These dashboards are intended to promote awareness of the current state of hardware, software, configurations of hardware and software, and vulnerabilities on an agency's network. Although agencies are not required to use their dashboards for monitoring, DHS intends that this information will provide agency decision makers with consistent, timely, and targeted information to support prioritizing and fixing the worst problems first. According to DHS, the quality of the information in the dashboards is fundamental to ensuring that stakeholders have the correct information to make informed risk management decisions.

In addition, DHS maintains a federal CDM dashboard to promote its own awareness of agency networks.[32] Agency dashboards are to provide summary-level CDM information to DHS's federal dashboard, including the federal AWARE scores for each agency. DHS plans to use agency summary information to monitor the overall security posture of the federal government. DHS guidance notes that incomplete asset management data will reduce the effectiveness of both the federal and local AWARE scores.

Although FAA, IHS, and SBA agency CDM dashboards were in place and DHS had received data from them for the federal dashboard, the agencies were not using the dashboards to make security-related decisions, primarily due to poor data quality and other reasons. For example, as stated previously, the three agencies had not fully implemented the hardware asset management capability, which affects the accuracy of the data in dashboards. Additionally, the accuracy of

[32]In late 2019, DHS awarded a contract for completely new agency and federal CDM dashboards. DHS CDM officials stated that this was due to widespread operational problems with agency dashboards. DHS intended to begin testing the new dashboard in spring 2020.

federal and local AWARE scores was questionable due to shortcomings in agencies' implementation of key CDM requirements. Specifically:

All three agencies had dashboards populated with CDM information, but did not use the dashboards to make security-related decisions.

- FAA had established an agency CDM dashboard and had populated it with CDM information. However, FAA CDM staff reported they were not able to use their agency CDM dashboard effectively to make decisions due to the poor quality of the information. The agency's hardware inventory was missing information and contained duplicates, which undermined the data quality of the other CDM capabilities because it did not have complete information for the devices on its network. Additionally, FAA had not fully implemented configuration management capabilities, which further degraded the quality of the dashboard information. Due to these shortcomings, the agency was unable to use the information in the dashboard to manage risk. Instead, according to agency CDM staff, FAA relied on information from other tools to manage risk for its network.
- IHS had populated a CDM dashboard with information, but did not use it to make security-related decisions. According to its staff, the agency was able to use information from the individual CDM tools supporting its dashboard to assist with risk-based decisions, but did not use aggregated information in its agency CDM dashboard. IHS had not fully implemented its hardware asset management capability, which undermined the quality of the information gathered by the other CDM tools along with the information presented in its agency CDM dashboard.
- SBA had established a dashboard and populated it with CDM information. However, SBA CDM staff stated that they did not use the CDM agency dashboard, but instead relied on cloud-based tools to make security-related decisions.[33] SBA employed many cloud-based systems, and agency officials reported that their cloud-based tools provided more useful information than the CDM dashboard. The agency also had not fully implemented hardware management capabilities, reducing the quality of its CDM dashboard information.

[33]Evaluating the effectiveness of the implementation of SBA's cloud-based tools was not within the scope of this review.

DHS received CDM data from all three agencies. DHS demonstrated that the federal dashboard contained data from all three agencies. For FAA and IHS, which were both part of larger departments, DHS maintained both department-level and agency-level data.[34]

AWARE scores did not accurately reflect the security posture of the three agencies. The CDM AWARE scores rely on quality data to provide an accurate account of an agency's security posture. Accordingly, the shortcomings previously described in the quality of the underlying data negatively impacted the quality of the data used to calculate AWARE scores for FAA, IHS, and SBA.

As the agencies and DHS address the technical issues associated with implementing key CDM program requirements for managing hardware, configuration settings, and vulnerabilities described earlier, the quality of the data provided to the agency CDM dashboard should improve. As the data quality improves, the agency AWARE scores will become more accurate and the agencies will be able to better use CDM data to identify and prioritize the most significant problems on their networks.

In addition, to address data quality shortcomings, DHS developed a data quality management plan to identify data quality issues and remediate root causes. The plan identifies roles and responsibilities for the CDM PMO, integrators, and agencies for ensuring the accuracy of various data types, such as the number of devices connected to an agency's network. DHS intends for the processes described in the plan to evolve over time as CDM solutions mature.

Selected Agencies Identified Challenges in Implementing the CDM Program Requirements and DHS Took Actions to Manage These Challenges

FISMA requires DHS to assist agencies in implementing their information security programs. Further, the CDM agreements signed by DHS and each agency participating in the program state that DHS is to, among

[34]We did not review the accuracy or currency of this data.

other things, request, receive, and analyze agency feedback related to CDM operations.

In addition to shortcomings in implementing key CDM requirements described previously, agencies faced additional challenges. All eight of the agencies selected for our review—including the three selected for our technical review—identified challenges related to implementing CDM program requirements. Such challenges included planning for personnel and funding resources, resolving issues with integrators, implementing the CDM program using an integrator's solution, and implementing the program when the expertise of integrator staff declined. The CDM PMO took various actions to help manage the challenges throughout the life of the program. For example:

Planning for personnel and funding resources. CDM officials at each agency stated that they had underestimated or did not fully plan for the time and resources required of agency personnel for implementing program requirements. For example, CDM officials at one agency said they did not know that internal agency staff, rather than their integrator, would need to install new hardware to support the CDM tools. Officials at another agency stated that, although they knew that internal resources would be required to support the program, they were uncertain about how to schedule the use of resources, resulting in an inability to properly plan for program implementation.

The CDM PMO was aware of the challenge associated with personnel and funding resources, and had learned about this challenge through, for example, discussions with agencies at periodic customer forums.[35] To manage this challenge, the PMO documented the risk associated with personnel and funding resources for participating agencies and defined a series of steps for resolving the risk. The steps for resolving the risk included engaging with OMB when agencies indicated they did not have sufficient funding to cover license costs associated with continued use of the CDM tools. As of May 2020, the PMO had not fully resolved the risk, but PMO officials stated that they were still monitoring it. By continuing to monitor the risk, the PMO may be more effectively positioned to manage the challenge associated with personnel and funding resources at agencies in the future.

[35]The PMO holds bimonthly customer advisory forums to provide a platform for agencies participating in the CDM program to discuss issues related to implementation of the program, including providing feedback to the PMO and sharing lessons learned.

Resolving issues with integrators. CDM officials at five of the selected agencies told us they did not have direct oversight of integrator installation and configuration of the CDM tools on the selected agencies' networks. Instead, agency CDM staff had to rely on the DHS PMO to resolve problems the agencies experienced with the integrator. In one case, according to agency CDM staff, an agency CDM lead and other staff were spending a significant amount of time coordinating and attending meetings with PMO staff and the integrator, which took time away from their other responsibilities.

DHS acknowledged that agencies had experienced challenges with resolving issues with integrators. PMO officials stated that the PMO put program managers in place to, among other things, address the challenge related to directly resolving issues with the integrator. The officials explained that each manager operated as a point of contact for specific agencies and had responsibilities that included regularly communicating with agency CDM staff to understand the types of issues the agency was facing in implementing CDM. By continuing to facilitate communication between agency CDM officials and the PMO through the use of program managers, DHS may be more effectively positioned to manage the challenge of resolving issues with integrators moving forward.

Implementing the CDM program using an integrator's solution. Officials at five agencies stated that implementation plans that were not tailored more specifically to each agency's network environment created implementation problems. These officials stated that a more tailored approach, rather than using solely the integrator's solution, could have helped to alleviate these problems. For example, at one of the five agencies, the agency was not able to implement a tool in its integrator's solution for managing software. As a result, this agency was not meeting key CDM program requirements for managing software using CDM tools.

DHS acknowledged that agencies could experience challenges with using an integrator's solution. CDM PMO officials stated that through communication channels, such as the customer forums and program managers for agencies, the CDM program had become more flexible to agency feedback over time, and could better position agencies to tailor an integrator's solution to their environments. For example, for the agency that was initially unable to implement a tool in its integrator's solution for managing software, DHS worked with the agency and its integrator to find an alternate solution, according to PMO officials.

In addition, to allow for a more tailored implementation beyond the integrator's solution, CDM contracts enabled the agencies to request services from their integrators in addition to the integrator's initial solution.[36] As of November 2019, seven of the eight selected agencies had requested additional services to support more targeted implementation of the CDM program within their operating environments. By continuing to provide avenues for agencies to share feedback regarding an integrator's solution and tailor the solution to their environments, DHS may be more effectively positioned to manage the challenge of implementing the CDM program using an integrator's solution as the program continues.

Implementing the program when the expertise of integrator staff declined. Although CDM officials at five agencies stated that initial integrator staff had extensive technical knowledge that supported their CDM implementations, the officials told us that this was not always the case with subsequent staff. For example, officials at one agency explained that the integrator's replacement staff did not always have the same level of expertise as the prior staff. The officials stated that these declines in expertise resulted in missed deadlines and a lack of progress on the implementation.

The PMO was collecting metrics on integrator performance from the participating agencies as part of the award fee structure in the CDM contracts.[37] These metrics provided agencies with the opportunity to evaluate the integrator from the perspectives of technical aptitude, project management, and cost management. For example, the metrics included measures of how quickly the integrator sourced and hired appropriately skilled personnel, and whether or not the integrator retained key

[36]In January 2018, agencies participating in the CDM program began using an acquisition strategy called CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) to implement the CDM program requirements. DEFEND includes a request for service option, which enables agencies to request that the integrators perform tasks beyond the integrators' CDM solution. A request for service is a document including deliverables and overall specifications used to request and identify suitable solutions for the requestor's needs. Under DEFEND, agencies are required to pay for any request for service deliverables. Agencies are responsible for funding any additional requests for services.

[37]Such contracts, broadly referred to as incentive contracts, offer contractors (in this case referred to as integrators) the opportunity to earn fees or profits based on their performance.

personnel. According to CDM PMO officials, DHS collected these metrics every month.

In addition, through CDM program managers and customer forums, the PMO provided additional avenues for agencies to escalate issues associated with integrator staff. PMO staff stated that, in the event that an agency raised an issue associated with integrator staff through one of the available channels, the PMO was able to work with both the agency and the integrator to resolve the issue and alleviate any problems caused by integrator staffing issues. By continuing to collect metrics on integrator performance and provide avenues for agency CDM staff to communicate issues to the PMO, DHS may be more effectively positioned to manage the challenge of implementing the program when expertise of integrator staff might decline due to issues such as staff turnover.

Conclusions

Selected agencies reported that the CDM program had helped improve their awareness of hardware on their networks. However, although the program has been in existence for several years, these agencies had only implemented the foundational capability for managing hardware to a limited extent, including not associating hardware devices with FISMA systems. In addition, while most agencies implemented requirements for managing software, all of them inconsistently implemented requirements for managing configuration settings. Moreover, poor data quality resulting from these implementation shortcomings diminished the usefulness of agency dashboards to support security-related decision making. Until agencies fully and effectively implement CDM program capabilities, including the foundational capability of managing hardware on their networks, agency and federal dashboards will not accurately reflect agencies' security posture. Part of the reason that agencies have not fully implemented key CDM requirements is that DHS had not ensured integrators had addressed shortcomings with integrators' CDM solutions for managing hardware and vulnerabilities. Although DHS has taken various actions to address challenges identified by agencies, without further assistance from DHS in helping agencies overcome implementation shortcomings, the program—costing billions of dollars—will likely not fully achieve expected benefits.

Recommendations for Executive Action

We are making a total of 15 recommendations, including six to the Department of Homeland Security and nine to selected agencies.

The Secretary of Homeland Security should ensure that integrators' solutions provide unique identifiers for hardware on selected agencies' networks. (Recommendation 1)

The Secretary of Homeland Security should ensure that FAA's system integrator records FISMA system information in the agency's CDM tools. (Recommendation 2)

The Secretary of Homeland Security should ensure that IHS's system integrator records FISMA system information in the agency's CDM tools. (Recommendation 3)

The Secretary of Homeland Security should ensure that FAA's system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools, including the time a vulnerability was remediated. (Recommendation 4)

The Secretary of Homeland Security should ensure that IHS's system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools, including the time a vulnerability was remediated. (Recommendation 5)

The Secretary of Homeland Security should ensure that SBA's system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools, including the time a vulnerability was remediated. (Recommendation 6)

The FAA Administrator should commit to a time frame to complete the agency's effort to associate hardware with its FISMA systems. (Recommendation 7)

The FAA Administrator should document agency-specific variations from federal core configuration benchmarks for each operating system on its network. (Recommendation 8)

The FAA Administrator should configure its CDM tools to compare configuration settings against federal core benchmarks and agency-specific variations applicable to its environment. (Recommendation 9)

The Director of IHS should document approved hardware inventory information by associating FISMA systems with the hardware on its network in a format that can be readily integrated into its CDM tools. (Recommendation 10)

The Director of IHS should document agency-specific variations from federal core configuration benchmarks for each operating system on its network. (Recommendation 11)

The Director of IHS should configure its CDM tools to compare configuration settings against federal core benchmarks applicable to its environment. (Recommendation 12)

The SBA Administrator should commit to a time frame to complete the agency's effort to associate hardware with its FISMA systems. (Recommendation 13)

The SBA Administrator should document agency-specific variations from federal core configuration benchmarks for each operating system on its network. (Recommendation 14)

The SBA Administrator should configure its CDM tools to compare configuration settings against agency-specific benchmarks applicable to its environment. (Recommendation 15)

Agency Comments and Our Evaluation

We requested comments on a draft of this report from DHS and the three selected agencies to which we made recommendations (FAA, IHS, and SBA), as well as five other agencies where we performed work to identify challenges to implementing CDM (DOT, HHS, the Department of Justice, Federal Communications Commission, and Federal Deposit Insurance Corporation) and OMB. In response, four agencies—DHS; DOT (on behalf of FAA); HHS (on behalf of IHS); and SBA—concurred with all of our recommendations. In addition, OMB provided comments on our draft report. The remaining three agencies (the Department of Justice, Federal Communications Commission, and Federal Deposit Insurance Corporation) stated via email that they had no comments.

In written comments, DHS concurred with our six recommendations to the department. DHS stated that the department remains committed to improving agencies' awareness of hardware on their networks and to mitigating challenges identified with implementing the CDM program. The department added that it plans to complete implementation of our recommendations in 2021. The department also provided technical comments, which we incorporated as appropriate. DHS's comments are reprinted in appendix II.

DOT provided written comments stating that it concurred with our three recommendations to FAA. The department noted that CDM is one of the top cybersecurity goals and objectives identified in FAA's cybersecurity strategy. It added that CDM is expected to improve FAA's ability to understand, manage, and mitigate security vulnerabilities, and reduce adversaries' ability to compromise the confidentiality, integrity, and availability of information and information systems. DOT's comments are reprinted in appendix III.

In its written comments, HHS stated that IHS concurred with our three recommendations to IHS. Further, HHS noted that IHS plans to take a phased approach to associate FISMA systems with hardware, document agency-specific variations to federal core benchmarks, and configure tools to compare configuration settings to federal benchmarks. It indicated that IHS plans to complete these efforts in 2023. HHS's comments are reprinted in appendix IV.

In written comments, SBA concurred with our three recommendations to the agency. In addition, the agency stated that it will continue its efforts to align hardware with FISMA systems and intends to work with DHS and its integrator, as appropriate, to address and implement the other two recommendations. SBA stated that it plans to implement our recommendation related to configuring its CDM tools to compare configuration settings to agency-specific benchmarks in 2021. SBA's comments are reprinted in appendix V.

Beyond the aforementioned comments, OMB's liaison provided comments via email on aspects of our report message. Specifically, OMB stated that we should place more emphasis on CDM data quality and suggested that we include in the report, a recommendation that integrators ensure that data quality standards are met.

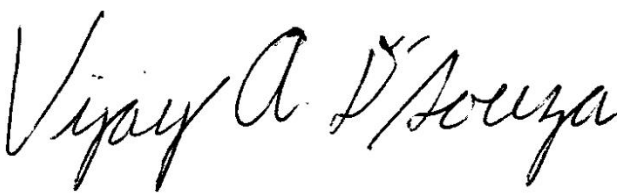
Our report notes that DHS developed a data quality management plan to identify data quality issues and remediate root causes. This plan identifies

roles and responsibilities for integrators to ensure the accuracy of various data. Our report also states that, as the agencies and DHS address the technical issues associated with implementing key CDM program requirements for managing hardware, configuration settings, and vulnerabilities, the quality of the data should improve. Based on DHS's plan and our recommendations that DHS ensure that integrators address various technical issues highlighted in our report, we do not believe that an additional recommendation related to integrators is warranted.

OMB also stated that our recommendations focused on the agencies evaluated, but that the shortcomings we identified potentially encompass the general government population. As a result, it said we should consider framing our recommendations to encompass uniform cybersecurity across the government. While we believe that the identified shortcomings may exist beyond the agencies selected for our review, as stated in our methodology, the results of our work are specific to the selected agencies and are not generalizable to federal agencies as a whole. Therefore, our recommendations are focused on the selected agencies discussed in our report.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of DHS, DOT, and HHS; the Attorney General at the Department of Justice; the Directors of CISA, IHS, and OMB; the Administrators of FAA and SBA; the Chairmen of the Federal Communications Commission and Federal Deposit Insurance Corporation; selected agencies' inspectors general; and other interested congressional 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 Vijay A. D'Souza at (202) 512-6240 or dsouzav@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 VI.



Vijay A. D'Souza
Director
Information Technology and Cybersecurity

List of Congressional Requesters

The Honorable Ron Johnson
Chairman
The Honorable Gary Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Thomas R. Carper
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
House of Representatives

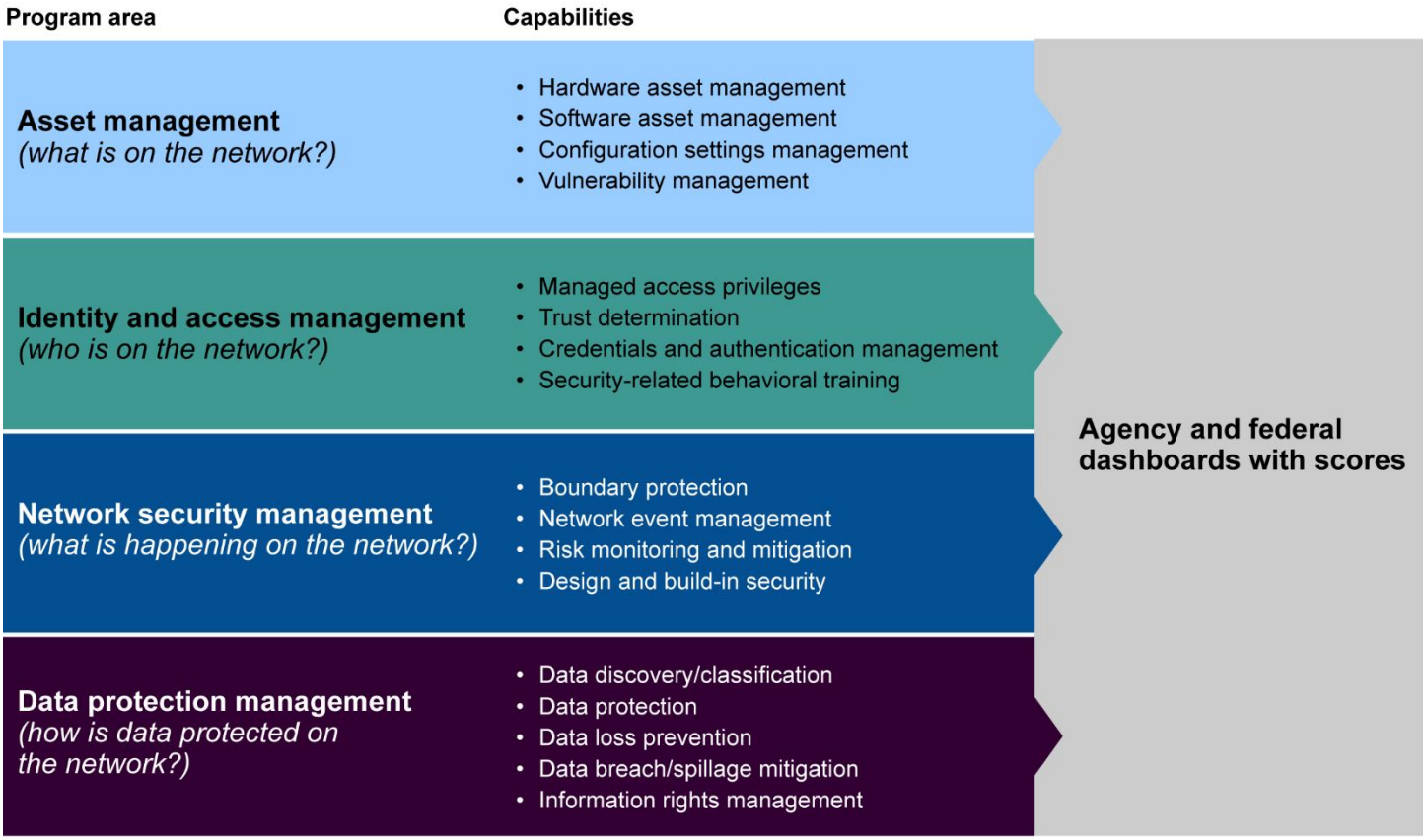
The Honorable Susan M. Collins
United States Senate

The Honorable Michael T. McCaul
House of Representatives

Appendix I: The Continuous Diagnostics and Mitigation (CDM) Program Consists of Four Program Areas

The Department of Homeland Security organized CDM into four program areas: asset management, identity and access management, network and security management, and data protection. The department further subdivided each program area into capabilities intended to support each area. Each of these program areas is to feed data to agency and federal dashboards, which include risk scores. Figure 3 depicts the CDM program areas with their associated capabilities.

Figure 3: Continuous Diagnostics and Mitigation Program Areas and Their Associated Capabilities



Source: GAO analysis of Department of Homeland Security data. | GAO-20-598

Asset management (What is on the network?): Managing what is on an agency's network requires identifying all hardware and software present on the network and addressing whether the agency has authorized the hardware to be on the network. In addition, it requires the tracking and management of software, configuration settings, and known vulnerabilities present on the network.

Identity and access management (Who is on the network?): Managing who is on an agency's network requires the control of user accounts on the network, as well as the access privileges associated with those accounts. The identity and access management program area consists of four capabilities:

- validating an individual's identity,

- verifying that the individual has the proper knowledge and training for the role they have been assigned and that their knowledge and training remains up-to-date,
- granting access to the systems by the individual based on the individual's established identity, and
- assigning privileges associated with the established identity.

Network security management (What is happening on the network?): Managing what is happening on an agency's network requires the control of network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. Network security management is intended to provide extensive and dynamic monitoring of the security controls on an agency's network. The program area includes:

- preparing for and responding to incidents and ensuring that software quality is integrated into the network and infrastructure,
- detecting internal actions and behaviors to determine who is doing what, and
- mitigating security incidents to prevent propagation throughout the network.

Data protection management (How is data protected on the network?): Managing how data is protected on an agency's network aims to, among other things:

- protect data at rest, in transit, and in use;
- prevent loss of data; and
- manage and mitigate data breaches.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

July 30, 2020

Vijay A. D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-20-598, "CYBERSECURITY: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program"

Dear Mr. D'Souza:

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

The Department is pleased with GAO's positive recognition that selected agencies had generally deployed tools intended to provide cybersecurity data to support DHS Continuous Diagnostics and Mitigation (CDM) program—an effort primarily led by DHS's Cybersecurity and Infrastructure Security Agency (CISA). DHS remains committed to improving agencies' awareness of hardware on their networks and mitigating challenges identified with implementing the CDM program.

The draft report contained 15 recommendations, including six for DHS with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2020.07.30 08:40:23 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-20-598

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Ensure integrators' solutions provide unique identifiers for hardware on selected agencies' networks.

Response: Concur. CISA's CDM Program Management Office (PMO) will conduct a detailed technical review of the design of each CDM Solution, with regard to unique identification (i.e., correlating and normalization) functionality, to verify existence and efficacy. Additionally, under the data quality activities, the CDM PMO will continuously evaluate the summary device counts for each agency for stability and accuracy, to validate that the unique identification function is operating within an acceptable tolerance, defined by CDM's Data Quality Management Plan. The CDM PMO will document and retain the results of these efforts for use by CDM program officials to help integrators improve their asset management functions. Estimated Completion Date (ECD): June 30, 2021.

Recommendation 2: Ensure that FAA's [Federal Aviation Administration] system integrator records FISMA [Federal Information Security Modernization Act] system information in the agency's CDM tools.

Response: Concur. The CDM Program's Portfolio Team will engage with the Department of Transportation (DOT) and FAA's system integrator to review the current FISMA inventory captured at the data integration layer, to better understand what remains to be captured. In addition, the CDM PMO will ensure that a method/process is in place to enable FAA to provide their FISMA inventory via a(n): 1) manual method receivable by the system integrator; or 2) automated mechanism (i.e., scheduled file exports or direct integration to the agency's Governance, Risk, and Compliance (GRC)) tool. Lastly, the CDM PMO will work with FAA to validate that all agreed-to FISMA systems are populated at the data integration layer, and that known assets are tagged and associated correctly. It is important to note, however, that these actions are highly dependent on FAA's ability to provide their FISMA inventory to the system integrator, as well as the requisite assets aligned to those respective systems, in a timely manner. ECD: June 30, 2021.

Recommendation 3: Ensure that the IHS's [Indian Health Service] system integrator records FISMA system information in the agency's CDM tools.

Response: Concur. The CDM Program's Portfolio Team will engage with the Department of Health and Human Services (HHS) and IHS's system integrator to review

3

the current FISMA inventory captured at the data integration layer, to better understand what remains to be captured. In addition, the CDM PMO will ensure that a method/process is in place to enable IHS to provide their FISMA inventory via a(n): 1) manual method receivable by the system integrator; or 2) automated mechanism (i.e., scheduled file exports or direct integration to the agency's GRC tool). Finally, the CDM PMO will work with IHS to validate that all agreed-to FISMA systems are populated at the data integration layer, and that known assets are tagged and associated correctly. It is important to note, however, that these actions are highly dependent on IHS's ability to provide their FISMA inventory to the system integrator, as well as the requisite assets aligned to those respective systems, in a timely manner. ECD: June 30, 2021.

Recommendation 4: Ensure that FAA's system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools, including the time a vulnerability was remediated.

Response: Concur. The CDM Portfolio Team will work with DOT and FAA to ensure: 1) FAA's system integrator provides a breakdown of the (captured vs. missing) vulnerability data fields including the "time vulnerability was remediated;" and 2) that FAA is presented with any configuration changes needed to collect missing vulnerability data. It is important to note, however, that system integrators have no purview over the FAA's vulnerability management tool, and in some cases the FAA will need to make configuration changes to ensure that CDM is being provided all the necessary vulnerability data needed. ECD: June 30, 2021.

Recommendation 5: Ensure that IHS's system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools including the time a vulnerability was remediated.

Response: Concur. The CDM Portfolio Team will work with HHS and IHS to ensure: 1) IHS's system integrator provides a breakdown of the (captured vs. missing) vulnerability data fields including the "time vulnerability was remediated;" and 2) that IHS is presented with any configuration changes needed to collect missing vulnerability data. It is important to note, however, that system integrators have no purview over the IHS's vulnerability management tool, and in some cases the IHS will need to make configuration changes to ensure that CDM is being provided all the necessary vulnerability data needed. ECD: June 30, 2021.

Recommendation 6: Ensure that SBA's [Small Business Administration] system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools, including the time a vulnerability was remediated.

Response: Concur. The CDM Portfolio Team will work with SBA to ensure: 1) SBA's system integrator provides a breakdown of the (captured vs. missing) vulnerability data

4

fields including the "time vulnerability was remediated;" and 2) that SBA is presented with any configuration changes needed to collect missing vulnerability data. It is important to note, however, that system integrators have no purview over the SBA vulnerability management tool, and in some cases the SBA will need to make configuration changes to ensure that CDM is being provided all the necessary vulnerability data needed. ECD: June 30, 2021.

5

Appendix III: Comments from the Department of Transportation

U.S. Department of Transportation

Assistant Secretary for Administration

1200 New Jersey Avenue SE
Washington, D.C. 20590

Office of the Secretary
of Transportation

July 17, 2020

Vijay A. D'Souza
Director, Information and Cybersecurity
U.S. Government Accountability Office (GAO)
441 G Street NW
Washington, DC 20548

Dear Mr. D'Souza:

Cybersecurity is a critical and pivotal component of accomplishing the FAA's mission to provide the safest and most efficient aerospace system in the world. Whether it is understanding aviation-specific threats and attacks, or mission support network attacks, the FAA has implemented cross organizational coordination to ensure the appropriate threat information is acted upon, defenses are in place, attacks are detected, and hygiene and remediation are performed. The FAA has ensured the agency's cybersecurity goals and objectives align with not only the FAA mission, but also with federal cybersecurity initiatives. Executing the strategic goals of the FAA in concert with federal initiatives will ensure the FAA focuses on the most critical cybersecurity issues in the most effective and efficient manner.

Continuous Diagnostics and Mitigation (CDM) implementation is one of the top cybersecurity goals and objectives identified within the FAA's Cybersecurity Strategy – *Improve understanding of Cybersecurity risk for FAA-owned, contracted and regulated systems.* The goal of CDM is to fortify the security and reliability of networks and systems through the increased use of automation. CDM will improve the FAA's ability to understand, manage, and mitigate security vulnerabilities, reducing adversaries' ability to compromise the confidentiality, integrity, and availability of the FAA's information and information systems.

Upon review of GAO's draft report, the FAA concurs with recommendations 7, 8, and 9 and will provide a detailed response to each recommendation within 180 days of the final report's issuance. The FAA appreciates the opportunity to respond to the GAO draft report. Please contact Madeline Chulumovich, Audit Relations and Program Improvement, at (202) 366-6512 with any questions.

Sincerely,

Keith Washington
Deputy Assistant Secretary for Administration

Appendix IV: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

July 27, 2020

Vijay A. D'Souza
Director, Information Technology & Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear D'Souza:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, *"Implementation of the Continuous Diagnostics and Mitigation (CDM) Program"* (Job Code 103327/GAO-20-598).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Sarah C. Arbes -S
Digitally signed by Sarah C. Arbes -S
Date: 2020.07.28 13:03:01 -04'00'

Sarah C. Arbes
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — CYBERSECURITY: DHS AND SELECTED AGENCIES NEED TO ADDRESS SHORTCOMINGS IN IMPLEMENTATION OF NETWORK MONITORING PROGRAM (GAO-20-598)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 10
The Director of IHS should document approved hardware inventory information by associating FISMA systems with the hardware on its network in a format that can be readily integrated in its CDM tools.

IHS Response
IHS concurs with GAO's recommendation. IHS is working on a phased project to reorganize its FISMA groups but requires dedicated resources to tag all hardware assets discovered by the CDM tools. The phased project will take approximately three years to complete.

Milestones	Duration - Completion Date
Re-organize FISMA boundaries and system groups.	18 Months – 1/21/2022
Configure CDM Tools to assign a unique ID to each network device. Classify each device and associate it with a FISMA system. Ensure 100% of network connected devices are inventoried.	12 Months – 1/21/2023
De-duplicate data to ensure each device only has a single identifier. Establish automated reporting to the CDM Dashboard. Identify unapproved hardware and take corrective action.	6 Months – 7/21/2023

Recommendation 11
The Director of IHS should document agency-specific variations from federal core configuration benchmarks for each operating system on its network.

IHS Response
IHS concurs with GAO's recommendation. IHS has applied DISA STIGS to newer Windows domain-joined operating systems only and will configure CDM tools to meet all requirements of the GAO findings. In order to identify misconfigurations from the defined DISA STIGS configuration benchmarks (non-IHS), IHS will configure the CDM compliance reporting application to scan for the variations from the defined DISA STIGs rather than the IHS approved baseline configuration. However, this will not be used to automate the deployment of the DISA STIGs configuration settings to IHS systems due to the potential negative impact to systems, applications, and medical devices used in the delivery of patient care. A larger portion of the 40,000+ devices on the IHS network is comprised of FDA-regulated Windows O/S-based medical devices. The IHS will develop a manual processes for reviewing and securing those devices. This resolution plan will take approximately three years to complete.

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — CYBERSECURITY: DHS AND SELECTED AGENCIES NEED TO ADDRESS SHORTCOMINGS IN IMPLEMENTATION OF NETWORK MONITORING PROGRAM (GAO-20-598)

Milestones	Duration - Completion Date
Create DISA STIG federal baseline scanning policies in CDM tools and scan managed devices for deviations to the baseline.	18 Months – 1/21/2022
Create agency-specific baseline policies and document deviations from the federal baseline. Document any approved exceptions to the agency baseline. Remediate or remove all non-compliant systems that do not have approved exceptions.	18 Months – 7/21/2023

Recommendation 12
The Director of IHS should configure its CDM tools to compare configuration settings against federal core benchmarks applicable to its environment.

IHS Response
IHS concurs with GAO's recommendation. IHS has applied DISA STIGS to newer Windows domain-joined operating systems only and will configure CDM tools to meet all requirements of the GAO findings. In order to identify misconfigurations from the defined DISA STIGS configuration benchmarks (non-IHS), IHS will configure the CDM compliance reporting application to scan for the variations from the defined DISA STIGs rather than the IHS approved baseline configuration. However, this will not be used to automate the deployment of the DISA STIGs configuration settings to IHS systems due to the potential negative impact to systems, applications, and medical devices used in the delivery of patient care. A larger portion of the 40,000+ devices on the IHS network is comprised of FDA-regulated Windows O/S-based medical devices. The IHS will develop a manual processes for reviewing and securing those devices. This resolution plan will take approximately three years to complete.

Milestones	Duration - Completion Date
Create DISA STIG federal baseline scanning policies in CDM tools and scan managed devices for deviations to the baseline.	18 Months – 1/21/2022
Create agency-specific baseline policies and document deviations from the federal baseline. Document any approved exceptions to the agency baseline. Remediate or remove all non-compliant systems that do not have approved exceptions.	18 Months – 7/21/2023

Appendix V: Comments from the Small Business Administration

July 27, 2020

Mr. Vijay A. D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. D'Souza:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled "DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program", GAO-20-598 (103327). The draft report examines the extent to which selected agencies have effectively implemented key CDM program requirements and describes challenges agencies identified in implementing the requirements and steps DHS has taken to address these challenges. Specifically, GAO selected three agencies based on reported acquisition of CDM tools. GAO evaluated the agencies' implementation of the CDM asset management capabilities, conducted semi-structured interviews with agency officials, and examined DHS actions.

SBA has reviewed the draft report and agrees with the three recommendations received.

Recommendation 13: The SBA Administrator should commit to a time frame to complete the agency's effort to associate hardware with its FISMA systems.

SBA Response: Concur. SBA is actively aligning FISMA systems with associated hardware and will continue these efforts during the rollout of DHS's new CDM environment.

Recommendation 14: The SBA Administrator should document agency-specific variations from federal core configuration benchmarks for each operating system on its network.

SBA Response: Concur. SBA will address and implement this recommendation during the rollout of DHS's new CDM environment in collaboration with DHS and the integrator.

Recommendation 15: The SBA Administrator should configure its CDM tools to compare configuration setting against agency-specific benchmarks applicable to its environment.

SBA Response: Concur. SBA will address and implement this recommendation during the rollout of DHS's new CDM environment in collaboration with DHS and the integrator. Estimated Completion Date: September 30, 2021.

Thank you for the opportunity to comment on this draft report. SBA does not have any technical comments currently. SBA appreciates GAO's consideration of our comments prior to publishing the final report.

Sincerely,

Keith A. Bluestein, Chief Information Officer
Small Business Administration

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contact

Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (Assistant Director), Daniel Swartz (Analyst-in-Charge), Edward Alexander, Jr., Christopher Businsky, Nancy Glover, Kevin Smith, Edward Varty, and Gregory C. Wilshusen made key contributions to this report. Amy Apostol, Melinda Cordero, Franklin Jackson, Ronald La Due Lake, Duc Ngo, and Adam Vodraska also provided valuable assistance.

Appendix VII: Accessible Data

Agency Comment Letters

Accessible Text for Appendix II Comments from the Department of Homeland Security

Page 1

July 30, 2020

Vijay A. D'Souza

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-20-598, "CYBERSECURITY: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program"

Dear Mr. D'Souza:

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

The Department is pleased with GAO's positive recognition that selected agencies had generally deployed tools intended to provide cybersecurity data to support DHS Continuous Diagnostics and Mitigation (CDM) program—an effort primarily led by DHS's Cybersecurity and Infrastructure Security Agency (CISA). DHS remains committed to

improving agencies' awareness of hardware on their networks and mitigating challenges identified with implementing the CDM program.

The draft report contained 15 recommendations, including six for DHS with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

Page 2

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations

Contained in GAO-20-598

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Ensure integrators' solutions provide unique identifiers for hardware on selected agencies' networks.

Response: Concur. CISA's CDM Program Management Office (PMO) will conduct a detailed technical review of the design of each CDM Solution, with regard to unique identification (i.e., correlating and normalization) functionality, to verify existence and efficacy. Additionally, under the data quality activities, the CDM PMO will continuously evaluate the summary device counts for each agency for stability and accuracy, to validate that the unique identification function is operating within an acceptable tolerance, defined by CDM's Data Quality Management Plan. The CDM

PMO will document and retain the results of these efforts for use by CDM program officials to help integrators improve their asset management functions. Estimated Completion Date (ECD): June 30, 2021.

Recommendation 2: Ensure that FAA's [Federal Aviation Administration] system integrator records FISMA [Federal Information Security Modernization Act] system information in the agency's CDM tools.

Response: Concur. The CDM Program's Portfolio Team will engage with the Department of Transportation (DOT) and FAA's system integrator to review the current FISMA inventory captured at the data integration layer, to better understand what remains to be captured. In addition, the CDM PMO will ensure that a method/process is in place to enable FAA to provide their FISMA inventory via a(n): 1) manual method receivable by the system integrator; or 2) automated mechanism (i.e., scheduled file exports or direct integration to the agency's Governance, Risk, and Compliance (GRC)) tool. Lastly, the CDM PMO will work with FAA to validate that all agreed-to FISMA systems are populated at the data integration layer, and that known assets are tagged and associated correctly. It is important to note, however, that these actions are highly dependent on FAA's ability to provide their FISMA inventory to the system integrator, as well as the requisite assets aligned to those respective systems, in a timely manner. ECD: June 30, 2021.

Recommendation 3: Ensure that the IHS's [Indian Health Service] system integrator records FISMA system information in the agency's CDM tools.

Response: Concur. The CDM Program's Portfolio Team will engage with the Department of Health and Human Services (HHS) and IHS's system integrator to review

Page 4

the current FISMA inventory captured at the data integration layer, to better understand what remains to be captured. In addition, the CDM PMO will ensure that a method/process is in place to enable IHS to provide their FISMA inventory via a(n): 1) manual method receivable by the system integrator; or 2) automated mechanism (i.e., scheduled file exports or direct integration to the agency's GRC tool). Finally, the CDM PMO will work with IHS to validate that all agreed-to FISMA systems are populated at the data integration layer, and that known assets are tagged and associated correctly. It is important to note, however, that these actions are highly dependent on IHS's ability to provide their FISMA

inventory to the system integrator, as well as the requisite assets aligned to those respective systems, in a timely manner. ECD: June 30, 2021.

Recommendation 4: Ensure that FAA's system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools, including the time a vulnerability was remediated.

Response: Concur. The CDM Portfolio Team will work with DOT and FAA to ensure: 1) FAA's system integrator provides a breakdown of the (captured vs. missing) vulnerability data fields including the "time vulnerability was remediated;" and 2) that FAA is presented with any configuration changes needed to collect missing vulnerability data. It is important to note, however, that system integrators have no purview over the FAA's vulnerability management tool, and in some cases the FAA will need to make configuration changes to ensure that CDM is being provided all the necessary vulnerability data needed. ECD: June 30, 2021.

Recommendation 5: Ensure that IHS's system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools including the time a vulnerability was remediated.

Response: Concur. The CDM Portfolio Team will work with HHS and IHS to ensure: 1) IHS's system integrator provides a breakdown of the (captured vs. missing) vulnerability data fields including the "time vulnerability was remediated;" and 2) that IHS is presented with any configuration changes needed to collect missing vulnerability data. It is important to note, however, that system integrators have no purview over the IHS's vulnerability management tool, and in some cases the IHS will need to make configuration changes to ensure that CDM is being provided all the necessary vulnerability data needed. ECD: June 30, 2021.

Recommendation 6: Ensure that SBA's [Small Business Administration] system integrator establishes a process to integrate all vulnerability information in the agency's CDM tools, including the time a vulnerability was remediated.

Response: Concur. The CDM Portfolio Team will work with SBA to ensure: 1) SBA's system integrator provides a breakdown of the (captured vs. missing) vulnerability data

Page 5

fields including the “time vulnerability was remediated;” and 2) that SBA is presented with any configuration changes needed to collect missing vulnerability data. It is important to note, however, that system integrators have no purview over the SBA vulnerability management tool, and in some cases the SBA will need to make configuration changes to ensure that CDM is being provided all the necessary vulnerability data needed. ECD: June 30, 2021.

Accessible Text for Appendix III Comments from the Department of Transportation

July 17, 2020

Vijay A. D’Souza

Director, Information and Cybersecurity

U.S. Government Accountability Office (GAO)

441 G Street NW

Washington, DC 20548

Dear Mr. D’Souza:

Cybersecurity is a critical and pivotal component of accomplishing the FAA’s mission to provide the safest and most efficient aerospace system in the world. Whether it is understanding aviation-specific threats and attacks, or mission support network attacks, the FAA has implemented cross organizational coordination to ensure the appropriate threat information is acted upon, defenses are in place, attacks are detected, and hygiene and remediation are performed. The FAA has ensured the agency’s cybersecurity goals and objectives align with not only the FAA mission, but also with federal cybersecurity initiatives. Executing the strategic goals of the FAA in concert with federal initiatives will ensure the FAA focuses on the most critical cybersecurity issues in the most effective and efficient manner.

Continuous Diagnostics and Mitigation (CDM) implementation is one of the top cybersecurity goals and objectives identified within the FAA’s

Cybersecurity Strategy – Improve understanding of Cybersecurity risk for FAA-owned, contracted and regulated systems. The goal of CDM is to fortify the security and reliability of networks and systems through the increased use of automation. CDM will improve the FAA's ability to understand, manage, and mitigate security vulnerabilities, reducing adversaries' ability to compromise the confidentiality, integrity, and availability of the FAA's information and information systems.

Upon review of GAO's draft report, the FAA concurs with recommendations 7, 8, and 9 and will provide a detailed response to each recommendation within 180 days of the final report's issuance. The FAA appreciates the opportunity to respond to the GAO draft report. Please contact Madeline Chulumovich, Audit Relations and Program Improvement, at (202) 366-6512 with any questions.

Sincerely,

Keith Washington

Deputy Assistant Secretary for Administration

Accessible Text for Appendix IV Comments from the Department of Health and Human Services

Page 1

July 27, 2020

Vijay A. D'Souza

Director, Information Technology & Cybersecurity

U.S. Government Accountability Office

441 G Street NW

Dear D'Souza:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "Implementation of the Continuous Diagnostics and Mitigation (CDM) Program" (Job Code 103327/GAO-20-598).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Sarah C. Arbes

Assistant Secretary for Legislation

Attachment

Page 2

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 10

The Director of IHS should document approved hardware inventory information by associating FISMA systems with the hardware on its network in a format that can be readily integrated in its CDM tools.

IHS Response

IHS concurs with GAO's recommendation. IHS is working on a phased project to reorganize its FISMA groups but requires dedicated resources to tag all hardware assets discovered by the CDM tools. The phased project will take approximately three years to complete.

Milestones	Duration - Completion Date
Re-organize FISMA boundaries and system groups.	18 Months – 1/21/2022
Configure CDM Tools to assign a unique ID to each network device. Classify each device and associate it with a FISMA system. Ensure 100% of network connected devices are inventoried.	12 Months – 1/21/2023
De-duplicate data to ensure each device only has a single identifier. Establish automated reporting to the CDM Dashboard. Identify unapproved hardware and take corrective action.	6 Months – 7/21/2023

Recommendation 11

The Director of IHS should document agency-specific variations from federal core configuration benchmarks for each operating system on its network.

IHS Response

IHS concurs with GAO's recommendation. IHS has applied DISA STIGS to newer Windows domain-joined operating systems only and will configure CDM tools to meet all requirements of the GAO findings. In order to identify misconfigurations from the defined DISA STIGS configuration benchmarks (non-IHS), IHS will configure the CDM compliance reporting application to scan for the variations from the defined DISA STIGs rather than the IHS approved baseline configuration. However, this will not be used to automate the deployment of the DISA STIGs configuration settings to IHS systems due to the potential negative impact to systems, applications, and medical devices used in the delivery of patient care. A larger portion of the 40,000+ devices on the IHS network is comprised of FDA-regulated Windows O/S-based medical devices. The IHS will develop a manual processes for reviewing and securing those devices. This resolution plan will take approximately three years to complete.

Page 3

Milestones	Duration - Completion Date
Create DISA STIG federal baseline scanning policies in CDM tools and scan managed devices for deviations to the baseline.	18 Months – 1/21/2022
Create agency-specific baseline policies and document deviations from the federal baseline. Document any approved exceptions to the agency baseline. Remediate or remove all non-compliant systems that do not have approved exceptions.	18 Months – 7/21/2023

Recommendation 12

The Director of IHS should configure its CDM tools to compare configuration settings against federal core benchmarks applicable to its environment.

IHS Response

IHS concurs with GAO's recommendation. IHS has applied DISA STIGS to newer Windows domain-joined operating systems only and will configure CDM tools to meet all requirements of the GAO findings. In order to identify misconfigurations from the defined DISA STIGS configuration benchmarks (non-IHS), IHS will configure the CDM compliance reporting application to scan for the variations from the defined DISA STIGs rather than the IHS approved baseline configuration. However, this will not be used to automate the deployment of the DISA STIGs configuration settings to IHS systems due to the potential negative impact to systems, applications, and medical devices used in the delivery of patient care. A larger portion of the 40,000+ devices on the IHS network is comprised of FDA-regulated Windows O/S-based medical devices. The IHS will develop a manual processes for reviewing and securing those devices. This resolution plan will take approximately three years to complete.

Milestones	Duration - Completion Date
Create DISA STIG federal baseline scanning policies in CDM tools and scan managed devices for deviations to the baseline.	18 Months – 1/21/2022
Create agency-specific baseline policies and document deviations from the federal baseline. Document any approved exceptions to the agency baseline. Remediate or remove all non-compliant systems that do not have approved exceptions.	18 Months – 7/21/2023

Accessible Text for Appendix V Comments from the Small Business Administration

Page 1

July 27, 2020

Mr. Vijay A. D'Souza

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office

441 G Street, N.W.

Washington, DC 20548

Dear Mr. D'Souza:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled "DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program", GAO- 20-598 (103327). The draft report examines the extent to which selected agencies have effectively implemented key CDM program requirements and describes challenges agencies identified in implementing the requirements and steps DHS has taken to address these challenges. Specifically, GAO selected three agencies based on reported acquisition of CDM tools. GAO evaluated the agencies' implementation of the CDM asset

management capabilities, conducted semi-structured interviews with agency officials, and examined DHS actions.

SBA has reviewed the draft report and agrees with the three recommendations received.

Recommendation 13: The SBA Administrator should commit to a time frame to complete the agency's effort to associate hardware with its FISMA systems.

SBA Response: Concur. SBA is actively aligning FISMA systems with associated hardware and will continue these efforts during the rollout of DHS's new CDM environment.

Recommendation 14: The SBA Administrator should document agency-specific variations from federal core configuration benchmarks for each operating system on its network.

SBA Response: Concur. SBA will address and implement this recommendation during the rollout of DHS's new CDM environment in collaboration with DHS and the integrator.

Recommendation 15: The SBA Administrator should configure its CDM tools to compare configuration setting against agency-specific benchmarks applicable to its environment.

SBA Response: Concur. SBA will address and implement this recommendation during the rollout of DHS's new CDM environment in collaboration with DHS and the integrator.

Estimated Completion Date: September 30, 2021.

Page 2

Thank you for the opportunity to comment on this draft report. SBA does not have any technical comments currently. SBA appreciates GAO's consideration of our comments prior to publishing the final report.

Sincerely,

Keith A. Bluestein, Chief Information Officer

Small Business Administration

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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

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, https://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 Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548