OFFICE OF INSPECTOR GENERAL

# DHS Has Made Limited Progress Implementing the Continuous Diagnostics and Mitigation Program

Homeland Security

June 1, 2021

OIG-21-38

**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

June 1, 2021

MEMORANDUM FOR: Thresa Lang, Ph.D.
Acting Chief Information Security Officer
Office of the Chief Information Security Officer

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2021.05.28 17:56:17 -04'00'

SUBJECT: *DHS Has Made Limited Progress Implementing the Continuous Diagnostics and Mitigation Program*

Attached for your action is our final report, *DHS Has Made Limited Progress Implementing the Continuous Diagnostics and Mitigation Program*. We incorporated the formal comments from DHS in the final report.

The report contains three recommendations aimed at improving the Continuous Diagnostics and Mitigation program. Your office concurred with all three recommendations. Based on information provided in the response to the draft report, we consider recommendations 1 through 3 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act of 1978, as amended,* we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

# DHS OIG HIGHLIGHTS

## *DHS Has Made Limited Progress Implementing the Continuous Diagnostics and Mitigation Program*

**June 1, 2021**

## Why We Did This Audit

In 2013, the Office of Management and Budget required Federal agencies to establish an Information Security Continuous Monitoring program to identify and respond to emerging cyber threats. DHS established the Continuous Diagnostics and Mitigation program to help agencies monitor and manage cybersecurity vulnerabilities. We conducted this audit to determine whether the program has strengthened the cybersecurity posture within the Department.

## What We Recommend

We made three recommendations for DHS to update its program plan, address vulnerabilities, and define patch management responsibilities.

**For Further Information:**
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

## What We Found

The Department of Homeland Security has not yet strengthened its cybersecurity posture by implementing a Continuous Diagnostics and Mitigation (CDM) program. DHS spent more than $180 million between 2013 and 2020 to design and build a department-wide continuous monitoring solution but faced setbacks. DHS initially planned to deploy its internal CDM solution in three phases by 2017 using a "One DHS" approach that restricted components to a standard set of common tools. After this attempt was unsuccessful, DHS adopted a new acquisition strategy in 2019, shifting to a capability-driven implementation approach, pushing the deadline to 2022, and allowing components to utilize existing tools to collect CDM data.

As of March 2020, DHS had developed an internal CDM dashboard, but reported less than half of the required asset management data. Efforts were still underway to automate and integrate the data collection process among components so DHS could report additional data, as required. DHS now needs to upgrade its dashboard to ensure sufficient processing capacity for component data. Until these capabilities are complete, the Department cannot leverage intended benefits of the dashboard to manage, prioritize, and respond to cyber risks in real time.

Additionally, we identified vulnerabilities on CDM servers and databases, which were due to DHS not clearly defining patch management responsibilities and not implementing required configuration settings. Consequently, databases and servers could be vulnerable to cybersecurity attack, and the integrity, confidentiality, and availability of the data could be at risk.

## DHS Response

DHS concurred with all three recommendations.

## Table of Contents



## Appendixes



## Abbreviations

| | |
|---|---|
| CDM | Continuous Diagnostics and Mitigation |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CMaaS | Continuous Monitoring as a Service |
| DEFEND | Dynamic and Evolving Federal Enterprise Network Defense |
| GAO | Government Accountability Office |
| ISCM | Information Security Continuous Monitoring |
| IT | information technology |
| OCIO | Office of the Chief Information Officer |
| OCISO | Office of the Chief Information Security Officer |
| OMB | Office of Management and Budget |
| OS | operating system |
| SSP | System Security Plan |

## Background

Federal agencies depend on computerized (cyber) information technology (IT) systems and electronic data for day-to-day operations to process, maintain, and report essential information. In the last several decades, advances in IT have introduced new cybersecurity risks across all industries. The security of these systems and data is vital to public confidence and the Nation's safety, prosperity, and well-being.

The Office of Management and Budget (OMB) sought to strengthen the Nation's cybersecurity posture by bolstering the processes and technologies used to detect cyber risks that may threaten an organization's IT environment. In 2013, OMB identified cybersecurity as a cross-agency priority goal and issued guidance for managing information security risk on a continuous basis.[1] Specifically, this guidance required that Federal agencies establish an Information Security Continuous Monitoring (ISCM) program to help identify and respond to emerging cyber threats. ISCM is the practice of maintaining ongoing awareness about information security risks, vulnerabilities, and threats to support organizational risk management decisions. By establishing ISCM, Federal agencies may collect information that informs and supports organizational risk management decisions and reduces threats to hardware and software assets. OMB also required Federal agencies to establish plans and set priorities to understand and manage cybersecurity risks.

In response to OMB's requirement, the Federal Chief Information Officer's Council and the Committee on National Security Systems established a Joint Continuous Monitoring Working Group (Working Group). The Working Group developed a concept of operations for monitoring information security and established guidance for stakeholders across the Federal government. The Working Group also issued guidance for agencies to implement continuous monitoring of security controls in a phased approach through fiscal year 2017.

### Federal Government-wide CDM Program

DHS established the Continuous Diagnostics and Mitigation (CDM) program in 2013 to carry out OMB's requirements for managing information security risk on a continuous basis. Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) manages the CDM program. DHS, in coordination with

[1] *Enhancing the Security of Federal Information and Information Systems*, OMB Memorandum M-14-03, Nov. 18, 2013.

OMB,[2] is to monitor the implementation of Federal departments' and agencies' ISCM strategies and programs.

The main goals of the CDM program are to improve cybersecurity capabilities, reduce threats, and streamline reporting. According to CISA, the CDM program objectives are to:

- reduce agency threat surface;
- increase visibility into the Federal cybersecurity posture;
- improve Federal cybersecurity response capabilities; and
- streamline *Federal Information Security Modernization Act of 2014* reporting.

To accomplish these objectives, the CDM program will rely on agency tools, software, and hardware to automate network monitoring and identify cyber risks. These tools include sensors that perform automated scans or searches for known cyber vulnerabilities. The data from the tools (e.g., scanning results) feed into an agency dashboard. As part of this process, the agency dashboard summarizes data, assigns risk scores, produces reports, and sends alerts to network managers about cyber risks.

Federal ISCM Dashboard Maintained by DHS

Developing a Federal ISCM Dashboard is a key component of the CDM program. The dashboard is meant to improve each agency's, and ultimately the Federal Government's, ability to identify and respond to cyber threats. CISA is responsible for building and deploying the Federal ISCM Dashboard that will consolidate and display summary information from each Federal agency. The ISCM dashboard should inform decisions about cybersecurity risks across the Federal government, with a focus on managing the highest priority and most serious risks. Managers can use data gathered from the Federal dashboard to develop guidance for agencies to improve risk-based decisions.

DHS is also responsible for driving the technical specifications and providing guidance to agencies for submitting security-related information to the Federal dashboard, as required by OMB.[3] As of 2013, OMB had identified four initial information security capability areas agencies must automate and report to

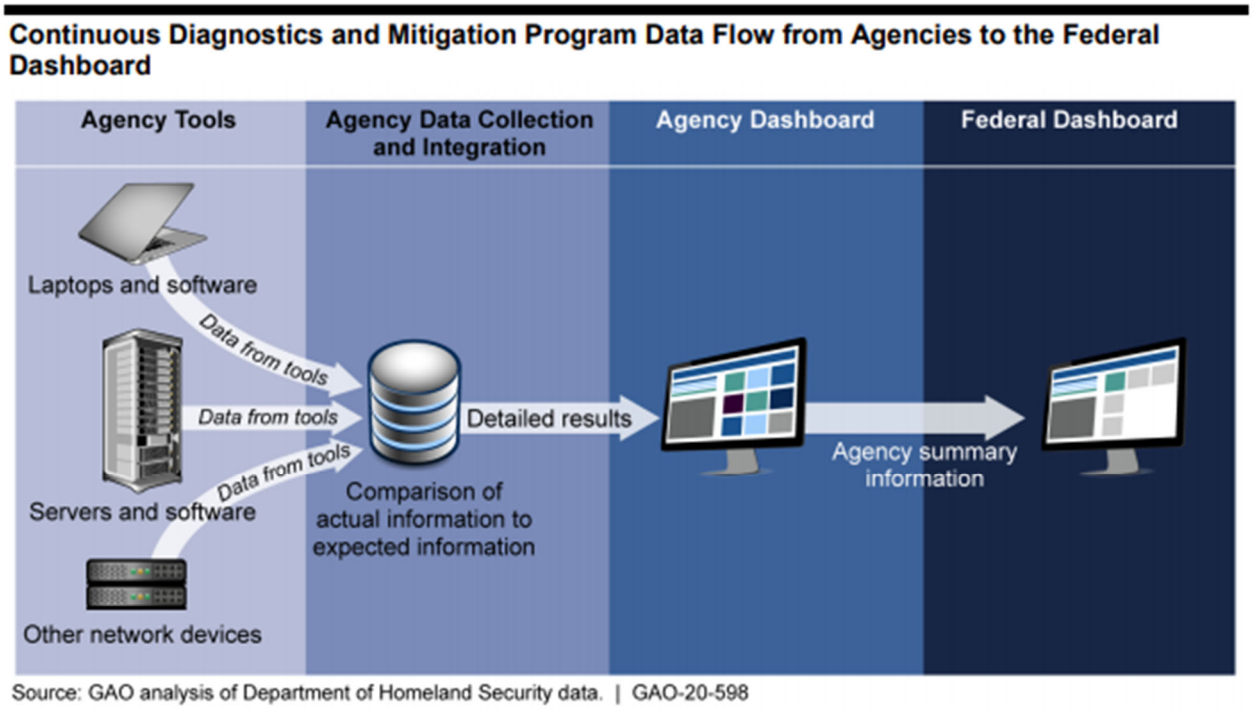
[2] *Enhancing the Security of Federal Information and Information Systems*, OMB Memorandum M-14-03, Nov. 18, 2013.
[3] According to OMB M-14-03, beginning in FY 2014, all agencies must submit security-related information to the ISCM dashboard for agency-level and Federal government-wide views.

DHS for integration on the Federal ISCM Dashboard. These four data elements were:

- Hardware Asset Management;
- Software Asset Management (including malware management);
- Configuration Setting Management; and
- Common Vulnerability Management.

Figure 1 illustrates the automated flow of information from the agency level to the Federal dashboard.

**Figure 1. CDM Program Data Flow**




## DHS' Internal CDM Program

While CISA leads the Federal CDM program, the DHS Office of the Chief Information Security Officer (OCISO) is responsible for department-level CDM activities, including developing DHS' CDM dashboard. The OCISO CDM Program Management Office leads these efforts. For example, the CDM Program Management Office establishes and maintains program management standards for all DHS components' adherence to the program. The CDM Program Management Office also guides DHS components on program details and collaborates with stakeholders, such as contractors, CISA, and the CDM Working Group.

**Prior Reports**

In December 2018, the Government Accountability Office (GAO) issued its report[4] on how agencies protect and secure Federal IT systems. Specifically, GAO audited the effectiveness of the Government's approach and strategy for securing its IT systems. GAO reported that DHS was in the process of enhancing CDM capabilities of Federal agencies to automate network monitoring for malicious activity. According to GAO, the Federal government-wide CDM program planned to:

- deploy Phase 1 tools by March 2019;
- deploy Phase 2 tools by September 2019; and
- achieve full operating capability of Phases 1, 2, and 3 by September 2022.[5]

GAO found that by June 2018, most agencies developing CDM capabilities had not fully implemented any of the CDM phases and the program was behind schedule. Further, officials at most agencies indicated the need for additional CDM training and guidance. CDM phase deployment delayed agency implementation, at least in part.

In August 2020, GAO reported[6] on DHS' oversight of the Federal government-wide CDM program. The report included information about how three specific agencies[7] implemented key CDM program requirements. GAO disclosed challenges the agencies identified in implementing the requirements, as well as the steps DHS took to address these challenges. GAO concluded that involvement in the CDM program improved network awareness of the three agencies. However, none of them had effectively implemented all key CDM program requirements. For example, none of the agencies had fully implemented requirements for managing their hardware.

We conducted our audit to determine the extent to which the CDM program strengthened the cybersecurity posture of the Department. We focused our audit on DHS' implementation of its internal CDM program, rather than its oversight of the Federal government-wide CDM program.

---

[4] *Agencies Need to Improve Implementation of Federal Approach to Security Systems and Protecting Against Intrusions*, GAO-19-105, Dec. 2018.
[5] A "Phase 4" conceptually existed at the time of GAO's audit, but it was not approved, and no tools were formally selected.
[6] *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-590, Aug. 2020.
[7] Federal Aviation Administration, Indian Health Services, and Small Business Administration.

## Results of Audit

DHS has not yet strengthened its cybersecurity posture by implementing a CDM program. DHS spent more than $180 million between 2013 and 2020 to design and build a department-wide continuous monitoring solution but faced setbacks. DHS initially planned to deploy its internal CDM solution in three phases by 2017 using a "One DHS" approach that restricted components to a standard set of common tools. After this attempt was unsuccessful, DHS adopted a new acquisition strategy in 2019, shifting to a capability-driven implementation approach, pushing the deadline to 2022, and allowing components to utilize existing tools to collect CDM data.

As of March 2020, DHS had developed an internal CDM dashboard but reported less than half of the required asset management data. Efforts were still underway to automate and integrate the data collection process among components so DHS could report additional data, as required. DHS now needs to upgrade its dashboard to ensure sufficient processing capacity for component data. Until these capabilities are complete, the Department cannot leverage intended benefits of the dashboard to manage, prioritize, and respond to cyber risks in real time.

Additionally, we identified several vulnerabilities on CDM servers and databases, which were due to DHS not clearly defining patch management responsibilities and not implementing required configuration settings. Consequently, databases and servers could be vulnerable to cybersecurity attack, and the integrity, confidentiality, and availability of the data could be at risk.

### DHS Faced Initial Challenges Completing Its CDM Program

DHS has not yet completed implementation of all required CDM capabilities across its components. In 2013, DHS began planning to design and deploy department-wide continuous monitoring tools and services in phases. The OCISO centered its initial program effort on a "One DHS" approach whereby components would be restricted to using a common set of security tools. However, the OCISO did not meet initial deadlines to complete the first three phases by December 2017 nor the subsequent deadline of June 2018. This was primarily because the "One DHS" approach did not work for the Department, which led the OCISO to abandon it in May 2019 and allow components to use a variety of tools, including their existing tools.

**Original Department-wide CDM Program Effort**

In November 2013, DHS began planning to design and deploy continuous monitoring tools and services to supply a full-scale CDM solution. In February 2015, Knowledge Consulting Group, Inc. received its original $29 million contract to design, build, and operate a continuous monitoring solution (i.e., dashboard) for DHS' CDM capability. The 2015 contract ended in 2018, by which time DHS had spent $38 million and the contractor had completed an initial version of the dashboard. However, the initial dashboard was not successful — the OCISO reported it crashed shortly after deployment. DHS was unable to identify the cause of this crash and could not recover the original dashboard.

DHS centered the 2013 department-wide deployment on the assumption that DHS components would be constrained to a common set of security tools for collecting and reporting data to the CDM dashboard. With this approach, DHS set out to follow OMB's original guidance to use standardized CDM solutions, or tools. In essence, OMB required agencies to standardize and deploy enterprise ISCM products and services instead of developing multiple, disparate services across agency bureaus and components.

The DHS Deputy Secretary supported this "One DHS" deployment of the CDM capability, encouraging components to use a common set of security tools. DHS anticipated that limiting CDM stakeholders to common tools would facilitate department-wide data gathering and analytics. The "One DHS" approach was also expected to decrease costs and improve efficiency by allowing for common training, acquisition, and licensing. Most importantly, DHS believed the use of common tools would ensure compatibility across component data in automating the data collection and reporting process.

However, DHS did not meet a series of early program deadlines. Despite DHS' planning efforts, the CDM program milestones shifted multiple times due to changes in CISA's broader Federal CDM program requirements. DHS based its original deployment plans on CISA's (and OMB's) phased, government-wide approach to deliver (1) asset, (2) user, and (3) network security management capabilities by 2017.[8] As such, CISA established the following initial program deployment milestones:

- Phase 1 capabilities by June 2016

[8] Phase 4, Data Protection Management, was introduced as early as May 2017 but was not part of the original contract.

- Phase 2 capabilities by September 2016
- Program full operating capability by June 2018; CISA later changed the date for the Federal CDM program to achieve full operating capability by December 2018.

DHS did not meet the deadlines for achieving full operating capability by 2018 under its "One-DHS" approach. DHS set an initial goal for components to populate the dashboard with asset management capability data by September 2019. However, components were not able to meet this target. Specifically, DHS did not, or could not, hold components accountable for the "One DHS" deployment requirements to use common tools that would ensure standardized security monitoring and data reporting capabilities. According to the DHS Chief Information Officer, many components wanted to use existing tools and did not want to change software or comply with the "One DHS" approach. In October 2018, OMB officially ended previous Federal guidance to use common tools to achieve CDM capabilities.[9] Ultimately, DHS spent $70 million on its initial CDM deployment approach.

**Second CDM Approach Established in 2018**

DHS' challenges in meeting the original CDM deadlines prompted significant changes to its deployment approach. In April 2018, DHS entered into a new, 6-year CDM contract known as Dynamic and Evolving Federal Enterprise Network Defense (DEFEND). The DEFEND contract was to support all phases of the CDM program and, once again, implement a common set of CDM tools and capabilities. In April 2018, DHS awarded $408 million to resolve CDM capability gaps, enhance existing capabilities, and complete new capabilities. The contractor, CACI, was to design, engineer, and deploy the Department's CDM cybersecurity tools and processes. DHS reported that in September 2018, CACI deployed the Department's current dashboard infrastructure.

In May 2019, DHS shifted away from its "One DHS" deployment approach.[10] With its second approach under the DEFEND contract, DHS began allowing components to use a variety of tools, including their existing tools, to collect CDM data. DEFEND also allowed components to procure tools directly from an approved product list. However, DHS did not establish a deadline for components to deploy replacement tools. As a result, some components removed the CDM tools provided by the Department under the "One DHS" deployment, but as of August 2020, some still had not replaced their tools. In

[9] OMB M-19-02 *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*.
[10] Continuous Diagnostics and Mitigation Phase 1 Tools Determination Memo, John A. Zangardi, DHS Chief Information Officer, May 4, 2019.

addition to DHS developing a second approach, CISA changed the Federal CDM program milestone date again, shifting the full operating capability milestone to September 2022.

With this second approach, the DHS CDM program organized its continuous monitoring capabilities into four categories:

1. *Asset Management Capability* – Management and control of devices, software, security configuration settings, and software vulnerabilities on the network. This included identifying hardware and software assets and recognizing known security vulnerabilities. During this phase, the components and agencies verify that assets have the correct security configuration settings to reduce risks and software vulnerabilities.

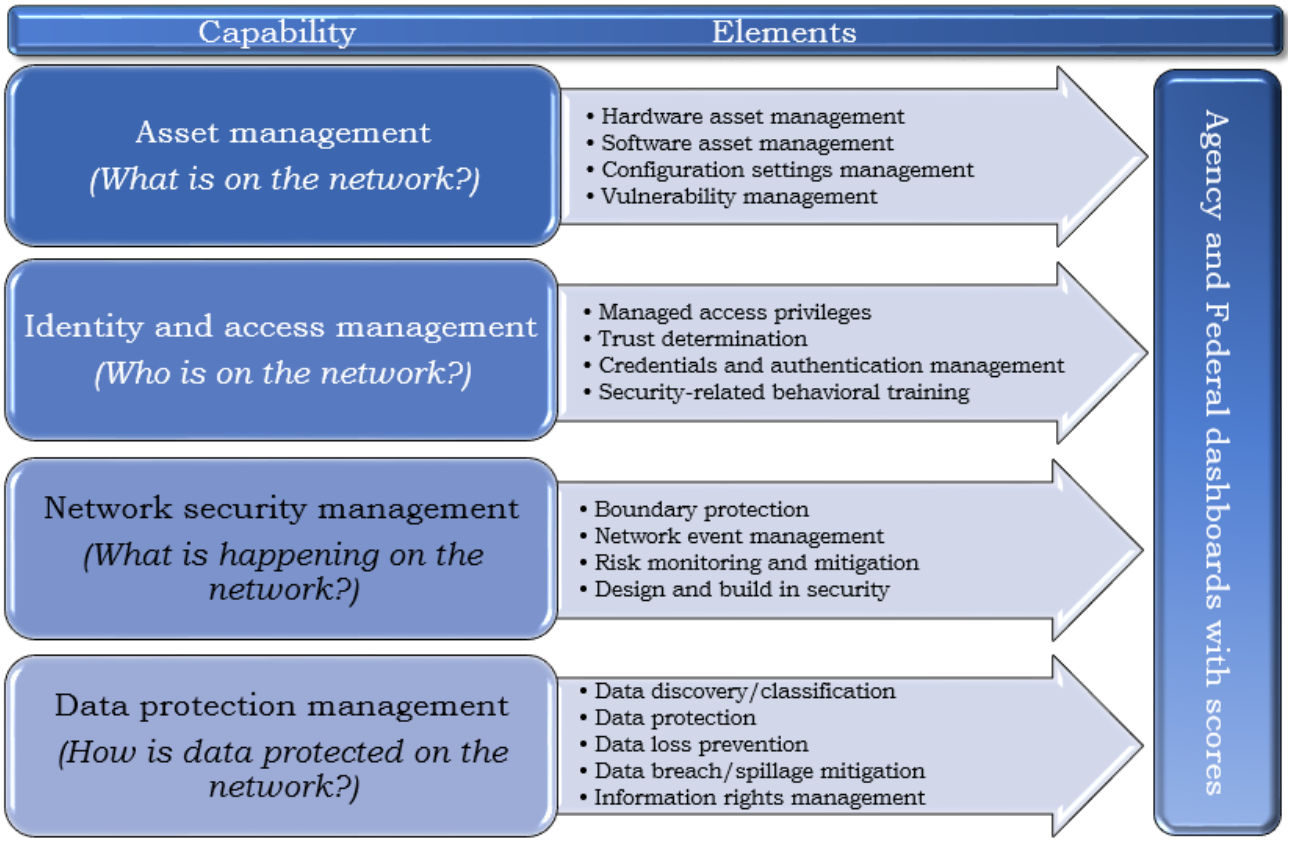
2. *Identity and Access Management Capability* – Management and control of who is on the network, whether they are authorized users, and validating user privileges. This phase included security related behavioral training, managing credentials and authentication, trust determination, and managing user access privileges.

3. *Network Security Management Capability* – Management of network, perimeter, host, and device components, along with data analytics and assessing user behavior and activities. The CDM program must operate, monitor, and improve security for data; conduct data analytics to identify network security incidents; and implement internal controls to identify, analyze, and document malicious or suspicious behavior on Government assets or networks.

4. *Data Protection Management Capability* – Management of data protection. Maintain and monitor the CDM program to protect the network using firewalls and encryption. Identify and mitigate cybersecurity risks on an ongoing basis. This includes data protection, loss prevention, breach mitigation, and information management.

When fully implemented by each DHS component, the Department should be able to synthesize and report on results across all four capabilities. That is, data elements from each capability area will feed into an enterprise dashboard. The dashboard will analyze the data and assign risk scores to measure the level of vulnerability, thereby providing situational awareness for the cybersecurity risk posture across the Department. Figure 2 shows the data elements from each of the four capabilities DHS intends to report to its agency dashboard.

**Figure 2. CDM Data Elements for the Capabilities DHS Reports to Dashboard**




*Source*: Office of Inspector General (OIG) analysis of CDM data

By the end of our audit fieldwork in Summer 2020, the CDM program was progressing once again despite the time, effort, and at least $38 million wasted on the initial failed approach. Overall, between 2013 and 2020, DHS spent $180 million to implement the CDM program. This included about $110 million on the DEFEND contract, plus about $70 million on tools and labor costs for contracts related to the old approach.

## Completed CDM Dashboard Has Not Yet Achieved Full Operational Capability

Although DHS deployed the Department's current dashboard in 2018, more work remains to be done by all components to fully automate the data collection process. As of March 2020, DHS components had provided less than half of the required asset management data to the Department's dashboard because efforts were still underway to integrate compatible CDM tools with the Department's dashboard. According to DHS, its current dashboard could not yet handle the required volume of data or report all data to the Federal dashboard as required. Until the DHS dashboard is fully functional, DHS cannot leverage the intended benefits of the dashboard to manage and respond to cybersecurity threats.

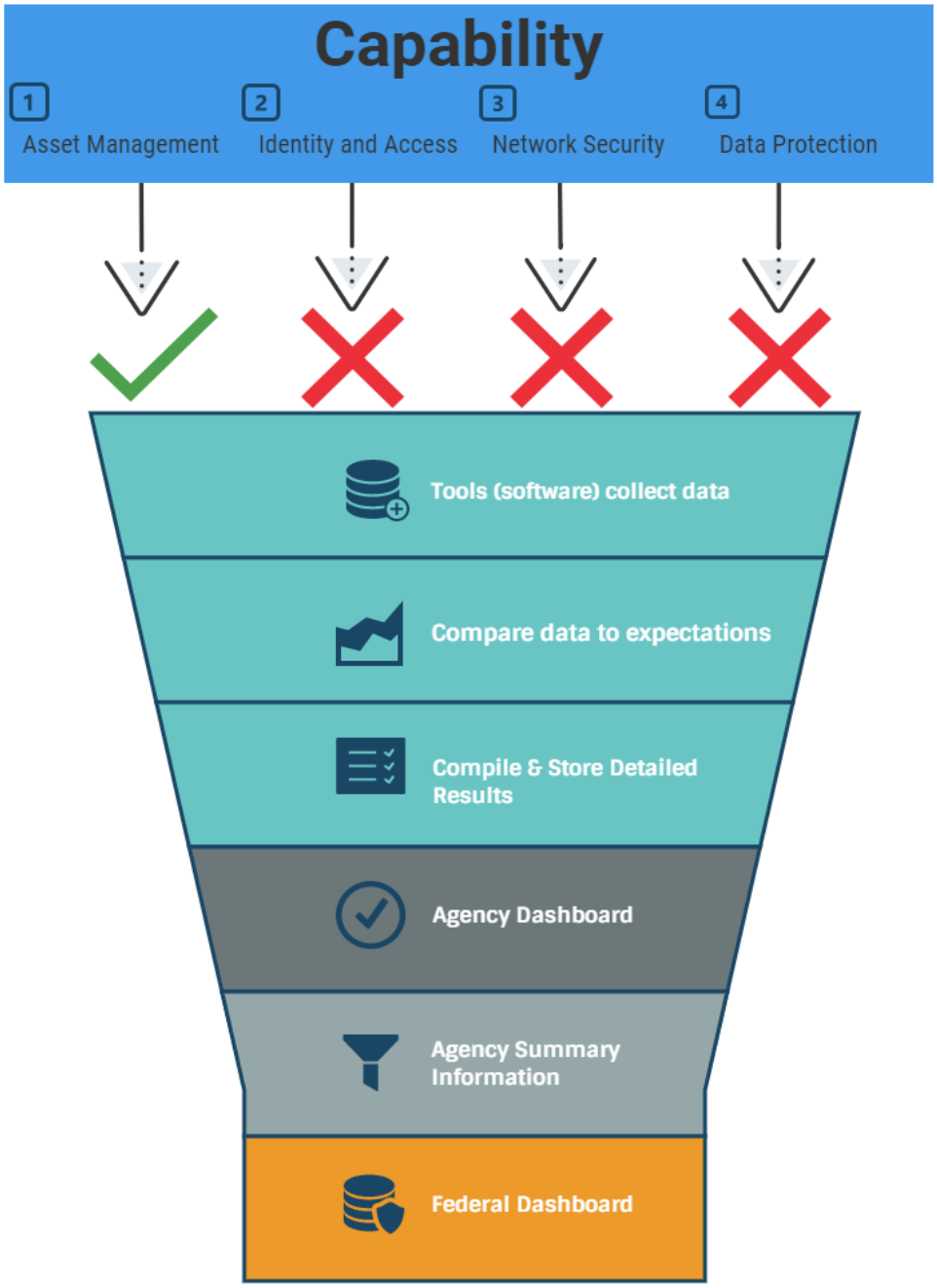
### Department-wide Dashboard Did Not Contain Complete Data

In 2018, the department-wide dashboard was operational, but it did not report all required data. As of March 2020, the dashboard contained less than half of the required data for asset management, which was only one of the four capability areas. Specifically, the dashboard contained the following partial asset management capability information:

- 40 percent of Hardware Assets
- 24 percent of Software Assets
- 18 percent of Configuration Settings
- 16 percent of Vulnerability Management

Figure 3 shows what CDM program data flowed to the dashboards.

**Figure 3. CDM Program Data Flow**




*Source:* OIG analysis of CDM process

For the dashboard to be accurate and useful, the underlying information must be complete, accurate, and timely. For example, a fully functional dashboard would need to collect information on each of the four CDM capability areas, not just one.

**Additional Component Tools and Processing Capacity Needed for Full Dashboard Functionality**

DHS' dashboard remained incomplete because it did not yet have a concerted way to collect and integrate data from components. As previously stated, with the shift away from the "One DHS" approach in May 2019, some components used their existing tools, while others opted to procure tools different from those on the approved product list.[11] OCISO officials stated that while the new approach ensured flexibility and generated more buy-in and participation from components, allowing disparate CDM tools added complexity. By the conclusion of our audit in summer 2020, each participating component was still working with CACI to normalize and integrate its data into the dashboard.

DHS expected the process of establishing uniform and integrated data would take additional time. In the interim, DHS depended on a cybersecurity tool called Tenable to show some progress reporting data. DHS needed a suite of tools but relied on this software, even though it knew Tenable alone could only provide some, but not all, needed capability.

Additionally, according to a Department official, the existing platform did not have adequate capacity to process the high volume of DHS' data from its numerous components. This occurred because the dashboard was developed with software that could not handle the data volume. To address this concern, DHS planned to build a new agency dashboard on a more robust platform. Officials expect the new dashboard platform will meet increased demand. The new platform will also provide better performance, visualization, and data analytics. At the conclusion of our audit, the Department had not finalized its implementation plans and schedule, but some DHS officials expected the new agency dashboard would be operational by early 2021.

[11] DHS requires each component to work with the DEFEND contractor to ensure its tools meet CDM requirements and that the data can be integrated into the Department's dashboard.

**DHS Has Not Yet Achieved CDM Benefits to Monitor Security Risks**

The primary goal of the CDM program was to improve cybersecurity capabilities, reduce threats, and streamline reporting. However, after 7 years, and spending $180 million, the Department has not yet gained the full benefits of the CDM program to manage and respond to cybersecurity threats. These benefits centered on completion of a department-wide dashboard that would provide a comprehensive view of vulnerabilities and improve internal control assessments. DHS projected dashboard benefits will include:

- maintaining an accurate picture of an organization's security risk posture;
- having visibility into Department and component assets;
- leveraging use of automated data feeds to measure security;
- ensuring effectiveness of security controls; and
- prioritizing mitigation and remediation of cybersecurity vulnerabilities.

Incomplete component data in the Department's dashboard limits its ability to gain intended benefits. For example, without complete data in the dashboard, DHS cannot leverage automated data feeds to measure security, proactively prioritize and address department-wide system vulnerabilities, and develop department-wide vulnerability solutions. DHS and its components also cannot achieve unified, cost-effective program efficiencies. Consequently, DHS and its components cannot ensure effective security controls. Until the DHS dashboard is complete, DHS remains hindered in its ability to submit complete and accurate data to the Federal dashboard.

## DHS CDM Servers and Databases Contained System Vulnerabilities

As part of our audit, we identified critical and high-risk vulnerabilities on CDM IT assets that needed corrective actions. This occurred because DHS headquarters had not fully defined patch management responsibilities or implemented required configuration settings. As a result, databases and servers could be vulnerable to attacks and the confidentiality, availability, or integrity of the data remain at risk.

**Patch Management Issues on CDM Servers and Databases**

DHS policy requires that components conduct vulnerability testing, promptly install patches, and eliminate or disable unnecessary services.[12] Patch management involves acquiring, testing, and installing fixes, known as patches, to address known vulnerabilities or deficiencies in a system's software or operating system (OS).

We determined that the Department implemented a patch management program that was generally effective to reduce IT asset vulnerabilities. However, we identified three critical and eight high-risk vulnerabilities[13] on CDM OSs and databases that needed corrective actions. Of the 11 vulnerabilities, 10 occurred multiple times on multiple systems. According to officials, the vulnerabilities were due to DHS not adequately defining the contractor's and data center's distinct responsibilities in installing patches. Table 1 shows the IT assets we tested, along with our results.

**Table 1. CDM IT Asset Vulnerabilities**

| IT Asset Type* | IT Assets Tested | Critical Vulnerabilities | High-Risk Vulnerabilities |
|---|---|---|---|
| OS 1 | 20 | 0 | 1 |
| OS 2 | 6 | 0 | 1 |
| OS 3 | 21 | 3 | 1 |
| Databases | 4 | 0 | 5 |
| **Total** | 51 | 3 | 8 |

*Source*: OIG analysis of IT assets.
*Names of asset types removed for security purposes

These vulnerabilities place the availability, confidentiality, and integrity of CDM data at risk. Specifically, these 11 unique vulnerabilities could subject the Department's CDM IT assets and data to cyberattacks, allowing an attacker to access, disable, or steal information from the server or database. The systems could also be subject to unauthorized access, including access to unauthorized resources or functionality. Ultimately, such exploitation could pose substantial risks to mission-critical DHS operations.

[12] DHS *Sensitive Systems Policy Directive 4300A*, Version 13.1, Section 4.8.3.d, Hardware and Software, July 27, 2017.
[13] Vulnerabilities are classified as low, medium, high, or critical risk, measured by the level of concern warranted.

**System Configuration Issues on CDM Servers**

DHS was not on track to ensure CDM servers complied with a required system configuration deadline. DHS required components to use specific OS configurations by November 7, 2019.[14] We tested the settings on three CDM IT asset types on November 6 and 7, 2019, and found that DHS had not implemented the required configuration settings. Specifically, the average percentage of non-compliance across the three IT asset types ranged from 9 to 46 percent for the 47 servers tested. Table 2 shows compliance by IT asset type and the number of servers tested.

**Table 2. CDM Server Configuration Management Compliance Rate**

| IT Asset Type* | Number of Servers Tested | Compliance Range (Percent) | Average Compliance (Percent) | Average Non-Compliance (Percent) |
|---|---|---|---|---|
| OS 1 | 20 | 71–89 | 87 | 13 |
| OS 2 | 6 | 90–92 | 91 | 9 |
| OS 3 | 21 | 42–84 | 54 | 46 |
| **Total** | 47 | - | - | - |

*Source*: OIG analysis of IT assets
*Names of assets removed for security purposes

DHS had not yet fully implemented required configuration settings although DHS officials said they had prioritized updating the highest risk configuration settings for risk mitigation. If DHS does not update its OS configuration settings, servers may remain vulnerable to operational disruptions and potential attack.

## Recommendations

**Recommendation 1:** We recommend the Chief Information Security Officer update the Department's Continuous Diagnostics and Mitigation program plan to demonstrate how OCISO will transition the agency dashboard to a scalable platform, ensure components use tools that meet requirements, set appropriate deadlines, and integrate component data.

[14] Interim Policy Memorandum: *DHS Information System Configuration Standards*, June 25, 2019; and *Change 13.1.1 to Department of Homeland Security Sensitive Systems Policy Directive 4300A*, Oct. 2, 2019.

**Recommendation 2:** We recommend the Chief Information Security Officer mitigate the vulnerabilities identified on the Continuous Diagnostics and Mitigation information technology assets.

**Recommendation 3:** We recommend the Chief Information Security Officer define patch management responsibilities for the Continuous Diagnostics and Mitigation information technology assets.

## Management Comments and OIG Analysis

DHS concurred with our recommendations and provided comments to the draft report. A summary of DHS' responses and our analysis follows. We included a copy of DHS' management comments in their entirety in Appendix B. DHS also provided technical comments to our draft report. We made changes to incorporate these comments as appropriate.

All recommendations will remain open and resolved until DHS provides additional documentation to show that actions taken fully meet the intent of the recommendation(s).

**Response to Recommendation 1: Concur.** In its response, the DHS Director of the GAO-OIG Liaison Office stated that DHS OCISO staff transitioned the Department's dashboard to a scalable platform on January 6, 2021. According to the Department, this move helped to ensure components use tools that meet requirements, set appropriate deadlines, and integrate component data. DHS requested that the OIG consider this recommendation resolved and closed, as implemented.

**OIG Analysis:** We consider these actions responsive to the recommendation, which is now resolved and open. This recommendation will remain open until we receive the Department's updated CDM program plan, as documentary evidence that the DHS' dashboard platform is appropriately scalable, components are required to use tools that meet program requirements and are subject to appropriate deadlines for implementation, and the dashboard contains fully integrated component data.

**Response to Recommendation 2: Concur.** According to the DHS Director of the GAO-OIG Liaison Office, DHS OCISO staff corrected these vulnerabilities on November 22, 2019. DHS requested that the OIG consider this recommendation resolved and closed, as implemented.

**OIG Analysis:** We consider these actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until we receive vulnerability assessment re-scans of the CDM servers and databases to verify that DHS completed mitigation of the previously identified vulnerabilities.

**Response to Recommendation 3: Concur.** According to the DHS Director of the GAO-OIG Liaison Office, DHS OCISO defined patch management responsibilities for CDM IT assets as part of its *DHS Continuous Monitoring as a Service System Security Plan* (SSP), dated July 6, 2016. DHS requested that the OIG consider this recommendation resolved and closed, as implemented.

**OIG Analysis:** We consider these actions responsive to the recommendation, which is resolved and open. We reviewed the 2016 SSP that DHS provided. We also reviewed the more recent 2019 SSP that we extracted from the system of record, which was in effect at the time of our testing. Both documents outline roles and responsibilities for "operations personnel" to remediate vulnerabilities. However, when asked about our findings, DHS headquarters personnel said there was confusion about who was responsible for addressing database vulnerabilities. Specifically, personnel did not know whether the contractor supporting DHS' Continuous Monitoring as a Service (CMaaS) or the data center hosting the infrastructure was responsible for addressing database vulnerabilities. Although the SSPs defined responsibilities in a generalized manner, they were not specific enough to alleviate confusion. This recommendation will remain open until we receive evidence DHS has sufficiently communicated specific responsibilities to eliminate confusion between the contractor and data center.

## Appendix A
## Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine whether the CDM program strengthened the cybersecurity posture of the Department. We conducted site visits within the Washington, DC area at DHS headquarters, a CISA field office, and a DEFEND contractor located in Chantilly, VA. We compared DHS' efforts to plan and implement its CDM program with Federal and departmental plans and requirements. Our audit scope was limited to the implementation of the CDM program within DHS and its components.

To conduct this audit, we established a focused data collection approach consisting of information-gathering meetings and interviews. We conducted interviews and teleconferences with DHS officials; staff from the DHS OCIO, OCISO, and CISA program offices; program and project managers; IT specialists; and contractors involved in DHS' implementation of CDM. We researched and used Federal and departmental criteria related to information security requirements. We obtained and reviewed published reports, memorandums, news articles, and other relevant documents related to DHS' implementation, management, and use of CDM. We also requested and analyzed supporting documentation, as necessary, following each interview. We used this information to accomplish our audit objectives.

We relied on the work of internal specialists from the OIG's Information Assurance and Testing Branch who performed vulnerability scans on DHS CDM assets. Specifically, they assessed 47 servers, 4 databases, and 19 network appliances. At the time of our assessment, our software vulnerability scanner did not support performing in-depth, credentialed scans of the 19 network appliances. Therefore, they could not determine whether the applications may have contained critical- or high-risk security vulnerabilities. We incorporated the results of their work as appropriate in our findings.

We conducted this performance audit between August 2019 and August 2020 pursuant to the *Inspector General Act of 1978, as amended*, and according to 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

# Appendix B
# DHS Comments to the Draft Report

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

Homeland Security

April 15, 2021

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

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

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2021.04.15 15:27:04 -04'00'

SUBJECT: Management Response to Draft Report: "DHS Has Made Limited Progress Implementing the Continuous Diagnostics and Mitigation Program: (Project No. 19-056-AUD-CISA)

Thank you for the opportunity to comment on this draft report. The Department of Homeland Security (DHS or the Department) appreciates the work of the Office of the Inspector General (OIG) in planning and conducting its review and issuing this report.

While DHS acknowledges the initial challenges in fully implementing its Continuous Diagnostics and Mitigation (CDM) program, the statement that the Department "has not yet strengthened its cybersecurity posture" is inaccurate. In addition, DHS disagrees with the assertion that $38 million was "wasted" during the initial effort to design and deploy a department-wide CDM solution.

The OIG conclusions did not provide adequate context regarding the first phases of CDM deployment and the subsequent adjustments to the implementation approach. Specifically, DHS has a multifaceted information technology enterprise where Components had already invested in cyber tools to meet their specific requirements. In many cases, transitioning to CDM mandated tools proved to be expensive and difficult, hence the decision to shift to meeting capability vice employing a specific, named tool. Additionally, the federal CDM project management office maintenance model was designed to only support license costs for two years or less resulting in challenges with sustainment. The draft also reflects an incomplete understanding of the value DHS derived from the experience and the important lessons learned from deploying across a large, complex infrastructure.

Regardless, DHS remains committed to building on its CDM program successes, while also exercising sound business judgment, obtaining the best value for the government, and incorporating lessons learned where appropriate.

DHS concurs with the three recommendations contained in the draft report. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under separate cover addressing several accuracy, contextual, and other issues for OIG'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.

Attachment

**Attachment: Management Response to Recommendations Contained in 19-056-AUD-CISA**

OIG recommended that the DHS CISO:

**Recommendation 1**: Update the Department's Continuous Diagnostics and Mitigation program plan to determine how OCISO [Office of the Chief Information Security Officer] will transition the agency dashboard to a scalable platform, ensure components use tools that meet requirements, set appropriate deadlines and integrate component data.

**Response:** Concur. DHS OCISO staff completed transitioning the agency's dashboard to a scalable platform on January 6, 2021, which ensures components use tools that meet requirements, set appropriate deadlines, and integrate component data. We request that the OIG consider this recommendation resolved and closed, as implemented.

**Recommendation 2**: Mitigate the vulnerabilities identified on the Continuous Diagnostics and Mitigation information technology assets.

**Response:** Concur. DHS OCISO staff completed mitigation of these vulnerabilities on November 22, 2019. We request that the OIG consider this recommendation resolved and closed, as implemented.

**Recommendation 3:** Define patch management responsibilities for the Continuous Diagnostics and Mitigation information technology assets.

**Response:** Concur. The DHS CISO defined patch management responsibilities for CDM information technology assets as part of the DHS Continuous Monitoring Service System Security Plan, dated July 6, 2016. We request that the OIG consider this recommendation resolved and closed, as implemented.

# Appendix C
# Continuous Diagnostic and Mitigation Technical Assessment Results

| Vulnerability Patch Management Assessment Results | | | | |
|---|---|---|---|---|
| **Category** | **Vulnerability** | **Number Tested** | **Number Failed** | **Risk Level** |
| Databases | Latest service pack and hot fix not applied | 4 | 2 | High |
| | Permission to execute the registry extended stored procedures granted to a user or group | 4 | 4 | High |
| | Update not installed | 4 | 2 | High |
| | Database not encrypted | 4 | 4 | High |
| | Password easily guessed | 4 | 1 | High |
| Network Appliances | None identified | 19 | 0 | N/A |
| Server OS 1 | Non-root configuration local privilege escalation | 20 | 20 | High |
| Server OS 2 | Non-root configuration local privilege escalation | 6 | 6 | High |
| Server OS 3 | Server unsupported version detection | 21 | 2 | Critical |
| | Core services unsupported | 21 | 3 | Critical |
| | Internet browser | 21 | 4 | Critical |
| | Security update for Microsoft Visual Studio Code (February 2019) | 21 | 5 | High |

| Configuration Management Assessment Results | | | |
|---|---|---|---|
| **Servers** | **Vulnerability – Test Fails** | **Number Tested** | **Number Failed** |
| Server OS 1 | All system command files must be owned by root. | 20 | 20 |
| | The system must require passwords to contain a minimum of 15 characters. | 20 | 20 |
| | The system must disable accounts after three consecutive unsuccessful logon attempts. | 20 | 20 |
| | Network Service must not be running, unless using Network or Satellite. | 20 | 20 |
| | The system package management tool must cryptographically verify the authenticity of all software packages during installation. | 20 | 20 |
| | The system must require passwords to contain at least one numeric character. | 20 | 20 |
| Server OS 2 | Must configure OS so the file permissions, ownership, and group membership of system files and commands match the vendor values. | 6 | 6 |
| | Must configure OS so the cryptographic hash of system files and commands matches vendor values. | 6 | 1 |

| Configuration Management Assessment Results | | | |
|---|---|---|---|
| **Servers** | **Vulnerability – Test Fails** | **Number Tested** | **Number Failed** |
| | OSs must require authentication upon booting into single-user and maintenance modes. | 6 | 6 |
| | Must configure OS to encrypt remote X connections for interactive users. | 6 | 6 |
| | Must configure OS so passwords are restricted to a 24-hours/1-day minimum lifetime. | 6 | 6 |
| | OS must have a host-based intrusion detection tool installed. | 6 | 6 |
| | OS must not interpret characters and should block special devices from untrusted file systems. | 6 | 6 |
| | OS must display the date and time of the last successful account logon upon logon. | 6 | 6 |
| | OS must not execute unapproved, untrusted binary files. | 6 | 6 |
| Server OS 3 | Must not allow Solicited Remote Assistance. | 21 | 1 |
| | Must turn off Autoplay for non-volume devices. | 21 | 1 |
| | Must configure the default Autorun behavior to prevent Autorun commands. | 21 | 1 |
| | Must disable autoplay for all drives. | 21 | 1 |
| | Must disable install with elevated privileges option. | 21 | 1 |
| | The Windows Remote Management client must not use Basic authentication. | 21 | 1 |
| | The Windows Remote Management service must not use Basic authentication. | 21 | 1 |
| | Must configure named pipes that can be accessed anonymously to contain no values on member servers. | 21 | 4 |
| | Must not configure unauthorized remotely accessible registry paths. | 21 | 1 |
| | Passwords must be at least 14 characters. | 21 | 21 |
| | Downloading print driver packages over HTTP must be prevented. | 21 | 21 |
| | Local administrator accounts must have their privileged token filtered to prevent use of elevated privileges over the network on domain systems. | 21 | 21 |
| | Domain users must be required to elevate when setting a networks location. | 21 | 18 |
| | Must route all Direct Access traffic through the internal network. | 21 | 18 |
| | Must enable IP stateless auto configuration limits state. | 21 | 18 |

| Unsupported Operating Systems Assessment Results | | |
|---|---|---|
| **IT Asset Category** | **Unsupported Operating Systems** | **Number of Vulnerabilities Identified** |
| OS 1 | N/A | 0 |
| OS 2 | N/A | 0 |
| OS 3 | N/A | 0 |
| Databases | Microsoft Type 1 | 2 |
| | Microsoft Type 2 | 2 |

## Appendix D
## Office of Audit Major Contributors to This Report

Richard Harsche, Director
Priscilla Cast, Audit Manager
Brian Smythe, Auditor in Charge
Nathaniel Nicholson, Auditor
Garrick Greer, Auditor
Tom Hamlin, Communications Analyst
Jeff Mun, Independent Referencer

# Appendix E
# Report Distribution

**Department of Homeland Security**
Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

**Office of Management and Budget**
Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**
Congressional Oversight and Appropriations Committees

## Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

## OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305