Continuous Diagnostics and Mitigation Program Lifecycle Costs

March 30, 2022

Fiscal Year 2021 Report to Congress

Homeland Security

Cybersecurity and Infrastructure Security Agency

Message from the Director

March 30, 2022

I am pleased to present the following report, "Continuous Diagnostics and Mitigation Program Lifecycle Costs," which has been prepared by the Cybersecurity and Infrastructure Security Agency (CISA).

This report has been compiled pursuant to direction in the Joint Explanatory Statement that accompanies the Fiscal Year 2021 Department of Homeland Security Appropriations Act (P.L. 116-260). The report provides an overview of the Continuous Diagnostics and Mitigation (CDM) program's lifecycle cost estimate (LCCE) and a description of the evolution of the program's LCCE over time. The current program LCCE is based on the scope of the current CDM program and the associated cost drivers and assumptions. This report provides an updated 5-year program cost and related schedule of activities based on the approved CDM program LCCE Version 6.0.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Lucille Roybal-Allard
Chairwoman, House Appropriations Subcommittee on Homeland Security

The Honorable Chuck Fleischmann
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Chris Murphy
Chair, Senate Appropriations Subcommittee on Homeland Security

The Honorable Shelley Moore Capito
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to CISA Legislative Affairs at (202) 819-2612.

Sincerely,

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

CISA is leading the civilian governmentwide effort to improve cybersecurity operations, including agencies' visibility into their networks (in both cloud and on-premises environments) to detect and respond to cybersecurity incidents effectively.

To provide agencies with greater flexibility for implementing the CDM requirements, the CDM program expanded its core cybersecurity capability offerings through the Dynamic and Evolving Federal Enterprise Network Defense acquisition program. The CDM capabilities enable CISA to enhance the security of federal agencies against advanced cyber threats. The report is congruent with the identified capability gaps across the Federal Civilian Executive Branch systems and networks.

Continuous Diagnostics and Mitigation Program Lifecycle Costs

Table of Contents

I. Legislative Language

The Joint Explanatory Statement that accompanies the Fiscal Year (FY) 2021 Department of Homeland Security (DHS) Appropriations Act (P.L. 116-260), includes the following direction:

> *Updated Lifecycle Cost Estimates.* — … CISA is directed to provide a report not later than 120 days after the date of enactment of this Act with updated five-year program costs and schedules which is congruent with projected capability gaps across federal civilian systems and networks.

II. Background

The Cybersecurity and Infrastructure Security Agency (CISA)'s Continuous Diagnostics and Mitigation (CDM) program bolsters the Federal Civilian Executive Branch agencies' cyber defenses (Defend Today) and enhances the security posture of the Federal Government (Secure Tomorrow) by providing federal agencies with capabilities to monitor risks to their networks in near real-time. This increased situational awareness allows agencies to prioritize actions to mitigate or accept cybersecurity risks on the basis of an understanding of the potential impacts to their missions. The CDM program accomplishes this by deploying commercial off-the-shelf tools on agency networks that provide enterprisewide visibility of the assets, users, and activities that are on the agencies' networks. This actionable information allows agencies to monitor, defend, and respond rapidly to cyber incidents. CDM capabilities are organized into five key program areas: Deployment of Agency and Federal Dashboards, Asset Management (AM), Identity and Access Management (IdAM), Network Security Management (NSM), and Data Protection Management (DPM).

The CDM program directly supports the following federal goals and mandates:

- *Report to the President on Federal IT Modernization* as provided under Executive Order 13800 (May 11, 2017);
- President's Management Agenda, which includes an information technology (IT) priority of reducing cybersecurity risks to the federal mission by leveraging current commercial capabilities and by implementing cutting-edge cybersecurity capabilities;
- Federal Information Security Modernization Act of 2014, which authorizes DHS to deploy technology to assist agencies with diagnosing and mitigating cyber threats and vulnerabilities continuously;
- Office of Management and Budget (OMB) Circular No. A-130 (2016 revision), *Managing Information as a Strategic Resource*, which directs federal civilian agencies to develop and implement information security continuous-monitoring strategies;
- OMB Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, which provides guidance to agencies on strengthening CDM capabilities;
- OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy,* which provides reporting guidance and deadlines to agencies in accordance with the Federal Information Security Modernization Act of 2014 and which requires agencies to exchange accurate data with the CDM Federal Dashboard; and
- Executive Order 14028, *Improving the Nation's Cybersecurity*, May 12, 2021, which charts a new course to improve the Nation's cybersecurity and to protect federal government networks by modernizing cybersecurity defenses. This will help agencies to protect federal networks, to improve information-sharing between the U.S. Government and the private sector on cyber issues, and to strengthen the United States' ability to respond to incidents when they occur.

CDM is designated as a Level I major acquisition program, per DHS Acquisition Management Directive 102-01. The CDM program structure supports varying deployment requirements tailored to agency needs. The population of agencies includes the 23 civilian Chief Financial Officer (CFO) Act agencies as well as non-CFO Act agencies that have opted to participate through signed CDM memoranda of agreement, which is a prerequisite to program participation. Currently, 54 non-CFO Act agencies are participating, but that number is expected to grow to 81 with specific OMB guidance.

The first CDM lifecycle cost estimate (LCCE) was developed in 2011 and was approved by DHS it in 2012. The base year of the LCCE is FY 2013. The methodologies used to develop the program LCCE have evolved over time depending on the stage of the acquisition cycle that the program was in when the estimate was updated. Additionally, the program updates the LCCE annually, incorporating actual costs from program execution and revising assumptions to reflect adjustments to program or contract schedules.[1] The program also tracks variances between estimates and actual costs as they become available, to understand the accuracy of the estimating techniques and technical information. The CDM program follows guidance in the U.S. Government Accountability Office (GAO)'s "Cost Estimating and Assessment Guide: Best Practices for Development and Management Program Costs," dated March 12, 2020 (GAO-20-195G), and in DHS Management Directive 102-01 when developing and updating the program LCCEs.

Major updates to the program LCCE were made to support program acquisition decision events. Per Acquisition Decision Memorandum dated March 12, 2018, the DHS Acquisition Decision Authority directed CDM to prepare for an acquisition decision event that incorporates DPM into the program's requirements baseline. Version 6.0 (V6.0) of the CDM LCCE was updated to support this decision, and covers the following:

- Completion of gap-fill efforts for agencies and networks not included in the prior scope;
- The new scalable Dashboard Ecosystem to provide enhanced performance, scalability, and analytics; Dashboard-as-a-Service; Data Visualization; Machine Learning; and Threat Intelligence;
- IdAM services required for Zero Trust Networks;
- Expansion of targeted NSM deployments;
- DPM – 50 total Tier 1 high-value assets (HVA);
- Extension of the anticipated program lifecycle from FY 2031 to FY 2033;
- Sustained development and engineering (D&E), and program planning and operations (PP&O) through FY 2033; and
- Authorized personnel increase from 84 to 106.

LCCE V6.0 covers FY 2012 through FY 2033. The end date is calculated on the basis of CDM's projected full operational capability (FOC) date of FY 2026 plus 7 years of sustainment. FOC is defined as the date when the CDM program has made the following available to all participating Federal Civilian Executive Branch agencies:

[1] The next annual LCCE update, scheduled for January 2022, will include details on the supplemental funding that CDM received from the 2021 American Rescue Plan Act (P.L. 117-2).

- The ability to manage what is on their networks (AM), who is on their networks (IdAM), what is happening on their networks (NSM), and how data are protected (DPM);
- An agency dashboard to receive and display all capability data feeds; and
- A federal dashboard to receive, aggregate, and display summary data received from agency dashboards and to transmit policy and other requests to agencies, as appropriate.

The CDM program receives two types of appropriated funds: Procurement, Construction, and Improvements (PC&I); and Operations and Support (O&S). These funds are allocated to support the CDM Program Management Office (PMO) and Support, and the five major CDM capability areas: Deployment of Agency and Federal Dashboards, AM, IdAM, NSM, and DPM. Within each capability area, CDM applied the DHS Cost Analysis Division's standard work breakdown structure for IT systems within both PC&I and O&S cost elements.

III. Data

The following table contains the planned obligations (dollars in millions) at the program level by appropriation versus the amounts in the Future Years Homeland Security Program report (FYHSP) to display the surplus and shortfalls from the previous baseline to CDM LCCE V6.0.

CDM Life Cycle Cost Estimate (LCCE) vs Funding Profile (in TY$K)									
Appropriation	**Prior Years (2012-2020)**	**FY21**	**FY22**	**FY23**	**FY24**	**FY25**	**FY26**	**To Complete (FY27 - FY33)**	**Total**
CDM Funded Only V6.0 Adjusted LCCE TY$K (50% Confidence Level)									
Research & Development (R&D)	-	-	-	-	-	-	-	-	-
Procurement, Construction, & Improvements (PC&I)	$1,425,767	$211,346	$155,135	$286,707	$362,407	$419,931	$422,774	$1,547,569	**$4,831,637**
Operations and Support (O&S)	$407,170	$111,008	$55,971	$77,734	$95,905	$98,094	$99,942	$645,853	**$1,591,676**
Total	**$1,832,937**	**$322,354**	**$211,106**	**$364,441**	**$458,312**	**$518,025**	**$522,716**	**$2,193,422**	**$6,423,313**
Funding Profile (FYHSP)									
Research & Development (R&D)	-	-	-	-	-	-	-	-	-
Procurement, Construction, & Improvements (PC&I)	$1,430,365	$214,350	$127,965	$81,183	$58,282	$18,098	$18,098	$ -	**$1,948,341**
Operations and Support (O&S)	$407,973	$110,684	$83,142	$55,329	$56,372	$57,332	$58,243	$ -	**$829,075**
All Other Funding	-	-	-	-	-	-	-	$ -	-
Total	**$1,838,338**	**$325,034**	**$211,107**	**$136,512**	**$114,654**	**$75,430**	**$76,341**	**$0**	**$2,777,416**
Surplus / Shortfall									
Research & Development (R&D)	-	-	-	-	-	-	-	-	**$ -**
Procurement, Construction, & Improvements (PC&I)	$ 4,598	$ 3,004	$ (27,170)	$ (205,524)	$ (304,125)	$ (401,833)	$ (404,676)	$ (1,547,569)	**$ (2,883,296)**
Operations and Support (O&S)	$ -	$ (324)	$ 27,171	$ (22,405)	$ (39,533)	$ (40,762)	$ (41,699)	$ (645,853)	**$ (763,404)**
All Other Funding	-	-	-	-	-	-	-		**$ -**
Total	**$ 4,598**	**$ 2,680**	**$ 1**	**$ (227,929)**	**$ (343,658)**	**$ (442,595)**	**$ (446,375)**	**$ (2,193,422)**	**$ (3,646,700)**

Numbers may not add to total due to rounding.

As outlined in the preceding Background section, the CDM program consists of multiple capabilities that function together to meet the program's mission. This section provides the cost assumptions, cost drivers, and projected evolution for each CDM capability area.

Program Management Office

The PMO cost category includes all federal salaries and benefits, as well as contract civilian labor required to support both D&E and PP&O activities for the CDM program. These costs include support actions necessary to enable the successful requirements for development, planning, and technical engineering efforts ongoing within the PMO.

Cost Assumptions:

- Sustained level of effort will be required for D&E efforts through achievement of FOC by the end of FY 2026.
- PP&O support costs are required at current levels through FOC.
- Reduced level of effort will be required post-FOC on the basis of assessment of expected PMO support activities.

Cost Drivers:

- Number of government and contractor personnel required to support requirements, architecture, test and evaluation (security, functional, and operational), security accreditation support, and configuration/change management support.

- The use of Federally Funded Research and Development Center (FFRDC) support for architecture, long-term planning, and unique knowledge and experience. More FFRDC support was used earlier in the program lifecycle and has decreased slowly over time.

Projected Evolution:

- No significant changes are anticipated in this area.

Program Management Office Estimate (Then-Year $ in millions at 50% Confidence Level)									
	Prior	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027 - FY 2033	Total
PC&I	$147.188	$19.842	$24.131	$24.131	$24.432	$22.424	$20.919	$43.156	$326.223
O&S	$229.566	$56.802	$50.827	$55.202	$57.926	$58.495	$59.024	$332.715	$900.557
Total	$376.754	$76.644	$74.958	$79.333	$82.358	$80.919	$79.943	$375.871	$1,226.780

Dashboard

Cost Assumptions:

- Procurement and deployment of the Dashboard Ecosystem will occur from FY 2020 to FY 2022.
- Sustainment of the Dashboard will begin in FY 2023 and will be required through the program's end of life.
- Dashboard data storage will increase 3 percent annually from FY 2022 to FY 2025 to enable additional NSM and DPM data collection and dashboard reporting needs.
- Procurement of threat intelligence capability will occur in FY 2023 on the basis of dashboard capability deployment plan.
- Threat intelligence solution will be procured as a commercial, off-the-shelf solution and will be sustained through a software-as-a-service model.
- Sustainment labor will begin in FY 2021 for the Dashboard deployment and sustainment plan and will be required throughout the program's lifecycle to incorporate ongoing releases and additional capability reporting into the CDM Dashboard.
- The Dashboard PMO will prioritize the incorporation of capability enhancements into its planned 6-month release cycle.

Cost Drivers:

- Threat intelligence sustainment.
- U.S. General Services Administration Advantage product costs and Alliant 2 labor rates.

- Dashboard enhancements.

Challenges:

- The contractor sizing guidance is based on recommended product specifications and takes into consideration aspects of the CDM Dashboard that may affect license and infrastructure needs over time, like data size, infrastructure resources, and licenses.
- Product price and product quantities of threat intelligence sustainment efforts.

Projected Evolution:

- Continued annual growth factors have been incorporated, and the project will be in sustainment through the end-of-the-program lifecycle with continued enhancements.
- Current planned enhancements to the CDM Dashboard identified above include data visualization, threat intelligence, and machine-learning.

Dashboard Estimate (Then-Year $ in millions at 50% Confidence Level)									
	Prior	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027 - FY 2033	Total
PC&I	$91.671	$11.474	$23.865	$23.689	$6.010	$6.130	$6.253	$47.413	$216.505
O&S	$20.560	$11.916	$2.835	$22.392	$37.979	$39.599	$40.620	$311.573	$487.474
Total	$112.231	$23.390	$26.700	$46.081	$43.989	$45.729	$46.873	$358.986	$703.979

AM is focused on helping agencies to know "What is on the Network?" to ensure strong cyber hygiene, which is foundational for cybersecurity. If an agency does not have situational awareness of its IT assets, those assets cannot be managed.

- The Hardware Asset Management (HWAM) capability discovers and manages internet protocol-addressable hardware on the network and identifies unauthorized or unmanaged hardware on agency networks. HWAM is used to establish and maintain an authorized hardware inventory baseline, capturing unique hardware identifiers and other properties.
- The Software Asset Management capability discovers the full agency software inventory and identifies unauthorized or unmanaged software in IT assets on a network. Because unauthorized software may be vulnerable and exploited as a pivot to other network assets, there is a need for unauthorized software to be removed or managed.
- The Configuration Settings Management function reduces the risk of misconfiguration of IT assets, including misconfigurations of hardware devices (to include physical, virtual, and operating system) and software.
- The Vulnerability Management capability detects known software vulnerabilities that an adversary could use to gain access to a system or network and to obtain unauthorized access to sensitive data.

Cost Assumptions:

- CDM will fund 1 year of capability sustainment following its deployment; subsequent maintenance and sustainment efforts will be funded by the receiving departments and agencies.

- CDM will fund 1 year of sustainment activity and licensing following the initial deployment of CDM capabilities; subsequent maintenance and sustainment activities, to include product licensing, will be funded by receiving departments and agencies.
- Sustainment and maintenance of the shared service environment will continue to be funded by CDM.

Cost Drivers:

- CDM sustainment efforts and maintenance of product licenses and services associated with the deployment of AM capabilities through gap-fill efforts completed under Dynamic and Evolving Federal Enterprise Network Defense task orders. These task orders cover Agencies/Components not originally covered by prior AM deployments, at present consisting primarily of the U.S. Secret Service and the Department of Energy's National Laboratories.
- Inclusion of 17 additional non-CFO Act agencies that have opted in for CDM, as well as four non-CFO Act agencies that are switching from the shared-services platform to an on-premises solution. The plan assumes eight agencies in each of FYs 2020 and 2021, plus five in FY 2022, bringing the total of participating non-CFO Act agencies to 81.
- All labor and items necessary to manage and maintain the previously procured hardware and software deployed to enable AM capabilities.
- Sustainment cost associated with the AM base deployment is driven by continued operations, services, and licensing to maintain the shared service environment for previously included non-CFO act agencies (Group F - Shared Services).

Challenges:

- Continued update to specific areas covered within the capability.
- Identification of agency networks not previously included in the CDM scope.

Projected Evolution:

- Backlogged or planned future capabilities that were not included in the original AM task orders, providing AM capabilities for CDM for cloud and CDM for mobile device management.
- Cloud implementation consists of the deployment of AM capabilities to cloud IT assets at participating agencies that request it. This includes coverage of IT assets associated with the cloud service provider's solution. Deployment began in FY 2020 and will continue through FY 2024.
- Mobile AM consists of the deployment of AM capabilities to mobile IT assets for participating agencies, and includes assets associated with mobile solutions. Deployment is expected to begin in FY 2021 and to continue through FY 2024.

Asset Management Estimate (Then-Year $ in millions at 50% Confidence Level)									
	Prior	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027 - FY 2033	Total
PC&I	$728.493	$124.941	$63.121	$64.600	$35.248	$19.009	$6.919	$52.466	$1,094.797
O&S	$94.411	$20.598	$ -	$ -	$ -	$ -	$ -	$ -	$115.009
Total	$822.904	$145.539	$63.121	$64.600	$35.248	$19.009	$6.919	$52.466	$1,209.806

IdAM, commonly described as “Who is on the Network?” focuses on management of access to agency networks and systems and accounts with elevated privileges, and covers credentials management, strong authentication, and security-related behaviors. The IdAM capability area includes the following:

- TRUST helps agencies to ensure that users are vetted to the appropriate degree when granted access to systems and networks.
- BEHAVE ensures that authorized users possess appropriate security-related training.
- Credentials Management (CRED) ensures that only proper credentials are used to access all systems, services, facilities, and information.
- Privilege Management (PRIV) manages the privileges associated with granted credentials.

Cost Assumptions:

- Targeted deployments of Identity Lifecycle Management (ILM) tools will begin in FY 2022; labor efforts and product procurements will be spread evenly between FY 2022 and FY 2028.
- An additional 57 Privilege Account Manager (PAM) installations are required to support agencies and components or data centers.
- Advanced Cloud Access Management (ACAM) Federation Services will rely on agencies to provide an agency identity provider capability. No federation on-premises assets are included. User-entity Behavior Analysis (UEBA) capabilities implementation to support ACAM will focus only on agencies that possess HVAs, have mature ILM infrastructure, and can utilize advanced capabilities (currently estimated to be six agencies). Targeted deployments will take place FY 2025 – FY 2031.
- Cloud Access Management (CAM) and Role-based Access Control (RBAC) will require an additional connector from CDM tools to Identity-as-a-Service; additional ILM user licenses will be required, as well as virtual directory services and a CAM gateway. Targeted deployments are planned from FY 2022 to FY 2029.
- Identity, Credential, and Access Management (ICAM) services for data security require that data loss prevention (DLP) and data rights management tools have been acquired and implemented for selected agencies’ HVAs.
- Product cost is based on vendor-proposed cost for CDM tools as identified in the Department of State (DOS) Independent Government Cost Estimate (IGCE).
- Targeted deployment will begin in FY 2025, and the labor and products required to accomplish the acquisition will be procured and deployed from FY 2025 to FY 2031.

Cost Drivers:

- ACAM product costs are based on vendor-proposed costs for CDM tools as identified in the DOS IGCE.
- CAM- and RBAC-required tasks and level of effort to implement the CAM and RBAC solution are roughly 1.5 times the effort associated with CRED management.
- ICAM services for data security may require additional software licenses for tools required to identify sensitive data and to protect unstructured data access rights and entitlements.

Challenges:

The extent to which agencies will continue the current telework posture is still unknown at this time, which presents a challenge for long-term planning for enterprisewide IdAM requirements.

Projected Evolution:

The CDM program also is planning to strengthen agencies' fundamental IdAM capabilities further through the implementation of tools designed to manage identities and access across the agency enterprise throughout a user's lifecycle. These tools include:

- ILM supports lifecycle management of the identity as highlighted in OMB Memorandum 19-17. The CRED, TRUST, BEHAVE, and PRIV capabilities are updated by providing licenses for the Master User Record Lifecycle Manager module. This module allows agencies to go beyond measuring the outcomes of their processes related to identities and credentials and to take control of those processes in a consistent, efficient, auditable manner.
- Mobile ILM and PAM Integration extends ILM capabilities to the mobile environment to manage mobile users on the network in support of the CRED, TRUST, and BEHAVE capabilities, and extends PRIV PAM capabilities for privileged accounts that manage Enterprise Mobility Managers.
- CAM and RBAC extend ILM capabilities to integrate CRED, TRUST, BEHAVE, and PRIV capabilities with agency-provided CAM capabilities for single-agency federation.
- ACAM Federation Services provides licenses and integration services for CAM capabilities for interagency federation to enable the credentials issued by one agency to be recognized and utilized at another agency, and provides integration services for UEBA capabilities to detect anomalous patterns of activities for users and devices.
- Identity and Privilege Management-as-a-Service provides an "as-a-service" delivery of ILM capabilities for CRED, TRUST, and BEHAVE to augment the identity governance capability installed previously in the shared services platform for non-CFO Act agencies, and provides PRIV capabilities through PAM services to agencies that are unable to host an on-premises solution.
- ICAM Services to Support Data Security provides licenses and implementation services for data security services, including data discovery and classification to find sensitive data across agency networks and privileged roles and role context to support data rights management and DLP capabilities. Where needed, ICAM provides Attribute-Based Access Control capabilities to enable support for data access security in HVAs.

Identity and Access Management Estimate (Then-Year $ in millions at 50% Confidence Level)									
								FY 2027 -	
	Prior	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2033	Total
PC&I	$229.519	$48.089	$23.137	$22.684	$26.571	$44.778	$54.044	$360.485	$809.307
O&S	$12.360	$18.342	$ -	$ -	$ -	$ -	$ -	$ -	$30.702
Total	$241.879	$66.431	$23.137	$22.684	$26.571	$44.778	$54.044	$360.485	$840.009

Network Security Management

The NSM capability set, often described as "What's Happening on the Network?" enables agencies to prepare for and respond to incidents and contingencies, to establish and manage cybersecurity policies across the enterprise, and to monitor quality and operational security. NSM is subdivided further into the following capabilities:

- Network Filters and Boundary Controls (BOUND-F) provides network filter devices such as firewalls and gateways that sit at the boundary between enclaves (such as a trusted internal network or subnet and an external or internal less-trusted network).
- Network Cryptographic Mechanism Controls (BOUND-E) provides visibility into risks associated with the use of cryptographic mechanisms employed on an organization's network. Agencies use cryptography to protect credentials, data at rest, and data in motion.
- Network Access Control (NAC) provides the capability to manage network segments and enclaves, along with associated network resources.
- Incident Response Reporting and Incident Response Optimization focus on the implementation of controls and processes to perform and automate incident response.
- Ongoing Assessment enables agencies to ensure alignment with federal policies regarding information security continuous monitoring, thus maintaining ongoing awareness of information security, vulnerabilities, and threats to support timely organizational risk management decisions.
- Ongoing Authorization dynamically monitors the security risk level using the results of Ongoing Assessment to detect when changing threats, vulnerabilities, technologies, and mission/business processes may result in an unacceptable security risk level to enable agencies to implement timely remediation measures.
- Contingency Planning is focused on the implementation of controls and processes to execute contingency plans in support of incident response.
- Manage Events (Audit Data Control) implements methods to perform audit data collection functions, such as operating system syslog, application log messages, system utilities monitoring logs, security activities logs, abnormal application behavior, and network security activity logs. These data then can be made available to support security assessments and forensic analysis.
- Design and Build in Security provides tools and methodologies to address software acquired or newly developed to ensure that security and privacy requirements are identified and included during all stages of the system development lifecycle.

Cost Assumptions:
The implementation of NSM is structured to leverage existing tools and products to the maximum extent possible, whether deployed by CDM or other in-house agency efforts, thus minimizing additional product procurement costs. Deployments will take the form of a targeted approach based on agency needs and readiness, diverging somewhat from the enterprisewide approach to AM, and to a lesser extent, IdAM. Deployments will continue to follow the typical CDM approach, consisting of a discover activity to gather specific agency requirements and architecture prior to procurement, installation, and configuration of tools and products on agency networks. Deployment information for NSM capabilities are as follows:

- Generally, CDM assumes that approximately half of participating CFO Act agencies already have implemented NSM tools and capabilities on their networks.
- BOUND-E will be targeted to approximately half of CFO Act agencies. Initial work began in FY 2017 in several agency groups and is planned to be completed for all interested agency groups in FY 2027.
- The complexity of BOUND-F is driven by the number of hardware assets procured under AM and the agencies' network architecture. Initial discovery efforts indicated that approximately 60 percent of CFO Act agencies already possess a BOUND-F capability; the program intends to use a targeted approach to reach approximately half of participating agencies from FY 2022 to FY 2027.
- All participating agencies may require implementation of NAC; deployment may require increased labor because of rigorous testing and baselining needs. NAC will augment existing CDM solutions and builds on tools deployed in AM as part of HWAM. The number of work enclaves are based primarily on agency complexity (federated vs. nonfederated agencies).
- Incident Response Reporting implementation began at DHS in FY 2017; work for remaining agencies will begin in FY 2022 on the basis of lessons learned from DHS deployment and will continue through FY 2027.

Cost Drivers:
- Enterprise complexity is the most relevant factor affecting network protection costs within agencies.
- Agency BOUND-E also contribute significantly to NSM costs.
- For NAC, management of network segments is influenced moderately by the number of servers. Complexity of NAC implementation is influenced by the complexity of agency network architectures and agency federation. The number of edge filters is based primarily on the enterprise complexity of the agency.

Challenges:
- High uncertainty regarding relative cost drivers between the various efforts.
- Cost estimate based on Dashboard endpoint device counts.

Projected Evolution:
The evolution of NSM capability deployments will include the expansion of currently planned deployments on agency networks to include cloud-based and mobile assets.

Network Security Management Estimate (Then-Year $ in millions at 50% Confidence Level)									
	Prior	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027 - FY 2033	Total
PC&I	$211.030	$7.000	$16.702	$87.150	$153.195	$195.241	$201.657	$718.098	$1,590.073
O&S	$40.028	$3.050	$ -	$ -	$ -	$ -	$ -	$ -	$43.078
Total	$251.058	$10.050	$16.702	$87.150	$153.195	$195.241	$201.657	$718.098	$1,633.151

Data Protection Management

DPM is focused on protecting sensitive data, including the protection of individuals' privacy and civil rights and civil liberties associated with that data, at rest, in use, and in motion, particularly data residing in systems designated as HVAs.

- Data Discovery and Classification provides identification of "data assets" across the organization for processing, storing, and transmitting information at all sensitivity levels.
- Data Protection addresses primarily two methods to protect data. The first capability is the application of cryptographic methods, while the second capability "hides" sensitive data field values using data masking or obfuscation methods.
- Information Rights Management (IRM) implements access controls (e.g., role-based access) to enterprise information (e.g., documents, files, etc.). IRM solutions provide fine-grained and identity-aware protections that are persistent for an agency's enterprise resources.
- DLP provides data protection measures to block exfiltration of sensitive data (e.g., personally identifiable information) outside the organization inappropriately (i.e., outside a documented routine use).

Cost Assumptions:

The CDM LCCE assumes that DPM will be applied using a targeted approach for 50 top-tier HVAs. This estimate is highly scalable and can be adjusted as necessary if additional funding is made available.

- CDM will deploy the DPM solution to Tier 1 HVAs on the basis of a targeted approach.
- The CDM LCCE approach for DPM assumes that each HVA will require all DPM capabilities.

Cost Drivers:

- The cost is being driven by the complexity of the participating agencies' network environments, specifically the complexity of HVA architectures. The complexity of DPM revolves around the dynamics stemming from the fluid nature of data in missions systems (e.g., data movement, replication, classification, etc.), which touches multiple CDM capabilities and tools simultaneously, including data discovery and classification, data loss prevention, data protection other than encryption, data protection through encryption, micro-segmentation, IRM, and data spillage within each covered environment.

Challenges:

- Deployment is also dependent on an agency's participation, ability, and readiness to identify, deploy, and sustain DPM solutions.
- High uncertainty regarding relative cost drivers between the various DPM capability implementations.

Projected Evolution:

The CDM program is still in the early stages of DPM planning and is still in progress with several pilot implementations at the U.S. Agency for International Development. Note that the estimates in the following table are preliminary and will be revised on the basis of subsequent planning and analysis.

Data Protection Management Estimate (Then-Year $ in millions at 50% Confidence Level)									
	Prior	FY 2021	FY 2022	FY 2023	FY 2024	FY 2025	FY 2026	FY 2027 - FY 2033	Total
PC&I	$12.601	$ -	$4.178	$64.452	$116.951	$132.349	$132.982	$325.950	$789.463
O&S	$0.399	$0.300	$ -	$ -	$ -	$ -	$ -	$ -	$0.699
Total	$13.000	$0.300	$4.178	$64.452	$116.951	$132.349	$132.982	$325.950	$790.162

IV. Discussion

The DHS Under Secretary for Management directed the CDM program to plan for the incorporation of DPM. LCCE V6.0 supports the program's acquisition decision made on April 15, 2021, to incorporate DPM into the program baseline. This acquisition decision also recognized the need to rebaseline the program costs to meet current program objectives, including:

- Providing coverage for agencies or networks not included in the prior scope of work;
- New dashboard that addresses performance challenges from the legacy CDM Dashboard, providing enhanced performance, scalability, analytics, Dashboard-as-a-Service, Visualization, Machine Learning, Threat Intelligence, and redundancy;
- ICAM services required as a basis for Zero Trust Networks;
- Targeted NSM deployments;
- DPM – Tier 1 (50 total HVAs);
- Extension of CDM FOC from FY 2022 to FY 2026, and the program end-of-life from FY 2031 to FY 2033;
- Sustained D&E and PP&O through the program end-of-life; and
- Authorized personnel increase from 84 to 106.

V. DHS Action Plan

On March 26, 2021, the CDM program received a DHS Acting CFO-signed memo approving the LCCE for the CDM LCCE V6.0. The program is awaiting formal baseline approval from the DHS Acquisition Review Board held April 15, 2021, and is expected to have FYHSP numbers mirroring the CDM LCCE V6.0 in FY 2023.

The CDM program will track potential future challenges in fulfilling the mission of the program through annual departmental budget tradeoffs. The CDM program will need to adjust if it is not funded to the LCCE and/or it receives additional funding. The CDM program will continue to keep Congress and OMB updated on these adjustments made to the LCCE tasks.

Appendix: Abbreviations

Abbreviation	**Definition**
ACAM	Advanced Cloud Access Management
AM	Asset Management
BEHAVE	Element tracked within IdAM capability
BOUND-E	Network Cryptographic Mechanism Controls
BOUND-F	Network Filters and Boundary Controls
CAM	Cloud Access Management
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CISA	Cybersecurity and Infrastructure Agency
CRED	Credentials Management
D&E	Development and Engineering
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DOS	Department of State
DPM	Data Protection Management
FFRDC	Federally Funded Research and Development Center
FOC	Full Operational Capability
FY	Fiscal Year
FYHSP	Future Years Homeland Security Program
GAO	U.S. Government Accountability Office
HVA	High-Value Asset
HWAM	Hardware Asset Management
ICAM	Identity, Credential, and Access Management
IdAM	Identity and Access Management
IGCE	Independent Government Cost Estimate
ILM	Identity Lifecycle Management
IRM	Information Rights Management
IT	Information Technology
LCCE	Lifecycle Cost Estimate
NAC	Network Access Control
NSM	Network Security Management
O&S	Operations and Support
OMB	Office of Management and Budget
PAM	Privilege Account Manager
PC&I	Procurement, Construction, and Improvements
PMO	Program Management Office
PP&O	Program Planning and Operations
PRIV	Privilege Management
R&D	Research and Development

Abbreviation	Definition
RBAC	Role-Based Access Control
TRUST	Element within IdAM capability
UEBA	User-Entity Behavior Analysis
V6.0	Version 6.0