ICIT

CENTER FOR CYBERSECURITY POLICY AND LAW

WHITEPAPER

CDM 2.0: ADVANCING FEDERAL CYBERSECURITY

JUNE, 2026

The U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is at a strategic inflection point. Workforce reductions, funding pressures, organizational realignment, leadership transitions, and contracting constraints are reshaping how the agency operates at the same time as the federal cyber threat environment is becoming more complex and operationally demanding. Nation-state adversaries, ransomware syndicates, software supply chain compromises, malicious cyber operations, and expanding risks across cloud and hybrid environments continue to challenge federal network security. At the same time, advances in artificial intelligence (AI), automation, and adversary tooling are accelerating the speed at which vulnerabilities can be identified and exploited, exposing gaps in visibility, coordination, and operational response across government systems. CISA must therefore deliver greater operational impact with fewer resources while sustaining government-wide cybersecurity modernization efforts and improving its ability to defend federal networks against increasingly adaptive threats.

At the center of this challenge sits the Continuous Diagnostics and Mitigation (CDM) Program, CISA's flagship program for building cybersecurity capabilities across Federal Civilian Executive Branch (FCEB) Departments and Agencies. Launched in 2012 by DHS, CDM was designed to provide federal agencies with tools, sensors, dashboards, and shared services to continuously monitor cybersecurity risk across federal networks. Through a phased acquisition approach and government-wide contracting vehicle, CDM has deployed capabilities supporting asset management, identity and access management, network security management, and data protection. Its federal dashboard architecture aggregates agency-level data to provide government-wide visibility into cyber risk, enabling prioritization, accountability, and oversight.

However, CDM's structure, governance model, and reporting orientation have often prioritized compliance tracking and scorecard metrics over operational integration and threat-driven defense. As federal agencies transition to cloud-first architecture, expand deployment of AI-enabled systems, and adopt Zero Trust security principles, CDM must evolve beyond a tool deployment and reporting program into a dynamic operational platform capable of supporting real-time cyber defense across modern federal environments. To remain effective, the program must provide continuous visibility across cloud, hybrid, and on-premises systems while enabling faster detection, threat hunting, identity protection, vulnerability management, and coordinated incident response.

The recommendations in this paper are grounded in a core principle: CDM should serve as the federal government's central platform for enabling Zero Trust implementation, continuous cybersecurity visibility, enterprise risk management, and coordinated defense across the Federal Civilian Executive Branch, and its resources, acquisition vehicles, shared services, and technical standards should be aligned accordingly. Modernizing CDM around this principle would align the program with the Administration's cybersecurity priorities and strengthen CISA's ability to identify, prioritize, and respond to threats affecting federal networks at enterprise scale.

This approach is consistent with Pillar 3 of President Trump's *Cyber Strategy for America*, which calls for the federal government to "Modernize and Secure Federal Government Networks" through

accelerated adoption of advanced cybersecurity capabilities, cloud modernization, AI-powered defenses, post-quantum cryptography, and improved procurement processes. The strategy also emphasizes the need for the federal government to improve operational coordination, agility, and resilience across federal cybersecurity efforts.

The following recommendations outline structural, technical, acquisition, and governance reforms necessary to modernize CDM for the next decade and align it with the Administration's cybersecurity modernization objectives, including supporting Zero Trust implementation, extending visibility into cloud and emerging technology environments, strengthening defenses against increasingly automated cyber threats, and enabling CISA to defend federal networks with greater speed, coordination, and operational effectiveness in an era of persistent cyber conflict.

REFORM THE ACQUISITION AND FUNDING MODEL

Modernizing CDM must begin with restructuring how cybersecurity tools and services are acquired, funded, and sustained. The current model fragments purchasing authority, increases administrative overhead, and incentivizes siloed implementations that work against enterprise Zero Trust adoption. A reformed acquisition and funding structure should aggregate buying power, reduce duplication, and create predictable, durable support for core cybersecurity capabilities.

Centralize and Clarify Funding for Core Capabilities

A sustainable CDM 2.0 model requires a clearer distinction between "core" and ancillary capabilities. The program should restructure its contracting and funding approach to eliminate procurement-driven silos and ensure enduring support for essential cybersecurity functions.

Key actions include:

- Centralizing funding for core operational capabilities to ensure they are sustained in perpetuity.
- Clearly defining "core" capabilities while enabling ancillary capabilities to be funded through agency-specific contracts or decentralized procurement.
- Providing limited optionality in technology selection (like endpoint detection response/persistent access capabilities (EDR/PAC) models) by constraining choices to best-in-class solutions, balancing enterprise efficiencies with the concentration risk associated with overreliance on few providers. Maintaining sufficient diversity in CDM-deployed tools can mitigate concentration risk, supported through a revamped Approved Products List (APL) focused on leading providers within each capability area.

Establish a DEFEND Successor Enterprise Vehicle for Core Cybersecurity Tools and Implementation Support by issuing a Blanket Purchase Agreement (BPA) or Multiple Award Schedule with two buckets: Solution Providers and Services Providers.

To streamline procurement and centralize buying power, CDM should establish a BPA or Multiple Award Schedule organized into two distinct categories outlined below. This vehicle should replace the legacy DEFEND-era approach for covered categories and be structured to separate product procurement from limited implementation support, rather than routing software purchases through broad systems-integration contracts.

- Technology/Solution Providers: Original Equipment Manufacturer (OEMs), Value Added Resellers (VARs), Distributors
- Services Providers: Operational systems integration and technology support

By centralizing tool procurement with a pre-vetted, qualified pool of solution providers, CDM can increase enterprise visibility, standardize terms and conditions, co-term contracts, and reduce administrative burden across agencies. Consolidated purchasing would create stronger negotiating leverage, reduce duplicative contracting actions, and drive cost efficiencies regardless of agency size.

Improve Cybersecurity Tools, Systems, and Platforms Management and Procurement Coordination

Agencies currently operate with limited insight into duplicative purchases, shelfware, and redundant cybersecurity tools and platforms. The White House Office of Management and Budget (OMB) should implement mechanisms and reporting tools that:

- Identify duplicative cybersecurity purchases, shelfware, and redundant capabilities across and within agencies.
- Support tool, system, and platforms licensing pathways for cybersecurity capabilities based on aggregated demand and standardized contract terms.
- Improve visibility into cybersecurity capability coverage, progress, and remaining gaps for oversight bodies and agency leadership.
- Improve visibility into barriers preventing rapid technology evaluation, procurement, and deployment.

The Federal Chief Information Officer and CISA should leverage these data sets to reinforce agencies' broader software inventory, tool-rationalization, and enterprise-consolidation efforts. These reforms align with the bipartisan SAMOSA Act (Strengthening Agency Management and Oversight of Software Assets).

Modernize Tool Vetting

The CDM acquisition framework must be streamlined to accelerate deployment timelines, reduce integration friction, and better support department-level or government-wide tool consolidation. Lengthy APL processes and complex integration requirements slow implementation, increase cost, and work against enterprise approaches. Agencies must be empowered to utilize the best available tools to combat evolving, dynamic cybersecurity threats that cannot wait on non-value-added procurement processes.

Key improvements include:

- Separating tool acquisition from bespoke system integration and prioritizing consolidated or enterprise procurements.
- Modernizing technical requirements to emphasize open standards and interoperable solutions, reusable architectures, cloud-native technologies, and pre-integrated enterprise-ready solutions.

This shift will reduce customization, shorten deployment cycles, improve interoperability across agencies, and better align CDM with agencies' ongoing tool-rationalization and enterprise consolidation efforts under M-22-01 and M-22-09.

APL Lifecycle Management

The APL must remain current to be credible and useful. Products that have reached end-of-life, end-of-support, or that no longer receive active security updates from their manufacturers should not remain on the APL, as they may introduce known vulnerabilities into the federal enterprise and undermine the program's objective of reducing agency threat surfaces.

Key actions include:

- Establishing a maximum product currency period (e.g., three years from listing or most recent re-evaluation), after which products must be re-validated against current technical requirements or be removed from the APL. The existing three-year re-evaluation cycle should be enforced and, where necessary, accelerated for capability categories experiencing rapid technological change, such as AI-enabled security tools and cloud-native platforms.
- Requiring that all APL-listed products maintain active vendor support, current security patching, and compatibility with modern federal IT environments, including cloud and hybrid architectures. Products that cannot demonstrate interoperability with Zero Trust reference architectures should be flagged for review.

- Resuming APL submissions on a regular cadence, with modernized evaluation criteria aligned to current federal cybersecurity priorities including Zero Trust Architecture, cloud-native design, and AI-readiness. An indefinitely frozen APL creates a static product ecosystem that cannot keep pace with a threat environment increasingly accelerated by adversarial AI.
- Publishing APL product metadata, including listing date, most recent re-evaluation date, and vendor-attested support lifecycle, so agencies can make informed procurement decisions and avoid deploying tools that are approaching end-of-support.

MODERNIZE CDM'S TECHNICAL CORE

Beyond acquisition reform, CDM must evolve technically. The program's architecture and dashboard capabilities should transition from compliance reporting tools into real-time operational cybersecurity infrastructure.

Operationalize the CDM Dashboard

The CDM dashboard should no longer function primarily as a FISMA reporting mechanism. Instead, it should evolve into a federated operational platform that aggregates key telemetry, analytics, and workflow data from agency tools to support proactive cybersecurity management across the federal civilian enterprise. It should complement - not replace - agency Security Information and Event Management (SIEM), Security Operation Center (SOC), and case-management capabilities by providing a common operating picture, shared analytics, and enterprise-level coordination.

Key enhancements should include:

- Integration of external attack surface management capabilities.
- Visibility into non-traditional asset classes (Operational Technology (OT)/IoT, cloud, mobile, cryptographic assets).
- Zero Trust maturity visibility, including agency-level progress against M-22-09 goals, CISA Zero Trust Maturity Model benchmarks, and coverage metrics for key Zero Trust capabilities across the five pillars (Identity, Devices, Networks, Applications and Workloads, Data).
- Support for continuous monitoring and operational decision-making by CISA and agencies, with a common operating picture and situational awareness for senior federal leadership.

This dashboard (or federated dashboards) must leverage commercially available solutions over the current custom-built system that has been slow to evolve and adapt. This evolution would reposition CDM as a shared decision-support and coordination layer rather than a compliance artifact.

Expand Shared Services

Expanding shared services under CISA's Continuous Diagnostics and Mitigation (CDM) program strengthens federal cybersecurity by improving real-time visibility, reducing duplicative costs, and enabling more consistent, government-wide threat detection and response.

CDM should increase adoption of shared services models, including:

- Group F / managed security services approaches focused on delivering cybersecurity outcomes rather than tools.
- Shared operational capabilities such as security operations, monitoring, and incident response. See Attachment 1 for Shared Operational Services Model Pilot.
- Extending the PAC delivery model (limited, vetted providers delivering capabilities as a centrally managed service with persistent CISA visibility) beyond EDR to additional capability areas where enterprise consistency delivers measurable security and efficiency gains, including Zero Trust access and network security capabilities that enable agencies to move away from implicit-trust network architectures. CISA leadership has identified the PAC model as a success, and agencies should be incentivized to adopt similar as-a-service approaches for other core Zero Trust functions, enabling CISA to achieve the "common operating picture" envisioned by the Administration's Cyber Strategy.

EXPAND VISIBILITY TO NON-TRADITIONAL AND EMERGING ASSETS

As federal networks increasingly rely on cloud services, mobile devices, operational technology, and software-as-a-service platforms, the threat surface has expanded far beyond on-premises infrastructure. Adversaries are exploiting identity systems, misconfigurations, and supply chain vulnerabilities that legacy asset management tools were not designed to detect. CDM must evolve beyond traditional IT asset visibility to address modern technology and increasingly complex threat environments and provide the comprehensive asset inventory that M-22-09 and Zero Trust Architecture require as a foundational capability.

Expand Asset Coverage

Visibility should be extended - in a phased, risk-prioritized manner tied to available funding - to include:

- Cloud infrastructure and workloads
- AI systems and models
- OT and IoT devices
- Mobile platforms
- SaaS applications and service identities
- Cryptographic assets
- Shadow IT and unsanctioned cloud services, including unauthorized AI applications.

Deploy Cloud-Native Application Protection Platforms (CNAPP)

Expanding CDM coverage to cloud environments is no longer optional. Federal systems are hybrid-by-default and increasingly multi-cloud. Without comprehensive cloud visibility (IaaS, PaaS, SaaS, and cloud-native services), agencies face heightened risk of undetected misconfigurations, identity abuse, data exposure, and systemic compromise. As agencies adopt SaaS and multi-cloud environments, CNAPP capabilities should integrate with Zero Trust access controls to provide unified visibility across user-to-application connections and infrastructure-level telemetry.

CNAPP capabilities should focus on securing:

- Cloud infrastructure and services
- Containers, Kubernetes, and serverless platforms
- Service identities and API activity

Key CNAPP capabilities include:

- Monitoring cloud control plane telemetry (IAM changes, role misuse, anomalous API activity).
- Detecting over-permissioned identities, token theft, lateral movement, and misconfiguration.
- Enabling automated containment actions such as token revocation, workload quarantine, and configuration rollback.
- Continuous configuration monitoring and drift detection.
- Cross-cloud correlation and attack-path modeling.

CDM should shift toward identity-centric security models, reflecting the central role of Identity and Access Management (IAM) and API activity in modern cloud threats. Technical standards for covered categories should include analysis of identities and permissions to effectively detect lateral movement and token theft in cloud environments.

Adapt CDM to Support Secure AI Adoption

Federal agencies are rapidly adopting artificial intelligence for mission delivery, business automation, and cybersecurity operations. This adoption introduces new categories of risk, including model and data supply chain vulnerabilities, shadow AI usage, sensitive data exposure through AI workflows, and reliance on third-party AI services that may not meet federal security requirements. The Administration's Cyber Strategy identifies AI-powered defenses as a modernization priority, and EO 14306 directs interagency coordination on AI software vulnerability management.

CDM should evolve to provide agencies with standardized visibility, shared guardrails, and acquisition-aligned implementation patterns for secure and resilient AI adoption.

Key actions include:

- Establishing AI security as a recognized CDM capability area, encompassing AI asset discovery and inventory, AI usage monitoring, data protection and recovery controls for AI workflows, and third-party AI risk visibility. This capability area should be mapped to the Zero Trust Maturity Model and treated as part of CDM's enterprise visibility mission.

- Expanding CDM asset coverage definitions to explicitly include AI systems and dependencies, such as deployed models, AI-enabled SaaS features, AI gateways, and service identities used by AI workflows.
- Defining minimum AI telemetry standards for CDM dashboard integration, so agencies can measure and report AI-related risk consistently across the FCEB.
- Leveraging CDM shared services to deliver AI security guardrails at scale, so agencies can adopt AI while preserving government-wide visibility and consistent safeguards, rather than each agency building standalone AI governance programs.
- Leveraging existing CDM security capabilities that cover defined baselines, where feasible, to improve efficiency.
- Modernizing APL evaluation criteria to assess AI-readiness, prioritizing solutions that integrate AI security controls with existing Zero Trust capabilities (identity, data protection, access governance, and logging) rather than treating AI security as a separate program.

AUTHORITY

Structural reform for CDM will require enhanced governance authority, but that authority should be narrowly tailored and transparent. OMB should designate a limited set of core enterprise cybersecurity categories for CDM management and direct agencies to use approved CDM vehicles for those categories unless they receive a documented exception. Under FISMA, CISA already has authorities to monitor implementation, issue binding operational directives, provide operational and technical assistance, and deploy technology to agencies, while OMB promulgates guidance and government-wide procurement policy to steer agency behavior.

Recommended actions include:

- OMB should be responsible for identifying and periodically refreshing the covered categories; for example, endpoint detection and response, vulnerability management, asset discovery, Zero Trust access and network security, cloud security, data protection, and other common cybersecurity functions that are mission-agnostic and suitable for standardization across the FCEB. Categories requiring high customization or mission-specific implementation should remain outside mandatory CDM scope unless agencies opt in.
- OMB should direct agencies to use CDM vehicles for those covered categories, subject to a formal waiver process for mission, cost, timing, or technical reasons. Current OMB guidance already requires justification when agencies acquire tools outside CDM-aligned vehicles.

- CDM funding and acquisition incentives should reward agencies that adopt Zero Trust-native architectures, including modern identity-centric access models that reduce dependence on legacy perimeter-based network designs. Agencies that demonstrate measurable progress toward transport-independent security (e.g., increased percentage of user-to-application traffic governed by Zero Trust access policies, reduction in implicit trust zones, improved enterprise logging coverage) should receive priority consideration for CDM support and advanced capability onboarding.

- CISA should be authorized to define technical standards, integration requirements, data-sharing rules, and performance measures for the covered categories in consultation with OMB, and to review agency waiver requests for technical sufficiency before OMB makes a final decision. That would give CISA a concrete governance role without giving it unlimited procurement control.

- CISA should also have clear reimbursable authority to execute or support enterprise procurements on agencies' behalf, in coordination with DHS contracting components and/or GSA, with agencies participating in requirements development, governance, and implementation planning.

Strengthened but bounded authority, implemented through collaborative governance with agencies, would allow CDM to evolve from an advisory and reporting function into a true enterprise cybersecurity capability across the FCEB, while preserving mission-specific exceptions and clear limits on what CISA is authorized to manage.

ATTACHMENT 1: SHARED SERVICES MODEL PILOT REPORT LANGUAGE

Centralized Chief Information Officer (CIO) Services Pilot Program

Centralizing Chief Information Officer (CIO) services for small agencies could produce a more secure, efficient, and cost-effective Federal information technology (IT) management model which reduces duplication of effort, strengthens cybersecurity oversight, improves acquisition outcomes, and enables small agencies to focus limited personnel resources on mission delivery rather than administrative IT overhead.

To assess the feasibility and effectiveness of this approach, the Committee provides funding for fiscal year 2027 for the Cybersecurity and Infrastructure Security Agency (CISA) to establish and carry out a pilot program under which CISA would assume the duties and responsibilities of the Chief Information Officer, as defined in section 3502 of title 44, United States Code, for not fewer than five small agencies. For the purposes of this pilot, "small agency" should be defined consistent with the Small Agency Council definition of Executive agencies with 500 or fewer full-time equivalent employees.

Under this pilot, CISA would provide centralized IT management, cybersecurity oversight, capital planning, enterprise architecture, policy implementation, and related CIO functions on behalf of participating agencies. The Committee expects CISA to structure this pilot in a manner that strengthens cybersecurity governance, improves acquisition efficiency, and reduces fragmentation in IT investments across participating agencies.

The pilot should:

- Consolidate core CIO operational authorities and oversight functions within CISA for participating agencies while preserving mission-specific program control at the agency level.
- Standardize cybersecurity policies, architecture, and security tooling across participating agencies to reduce duplicative investments and improve enterprise visibility, using Zero Trust architecture as the baseline security model for all participating agencies.
- Leverage existing governmentwide acquisition vehicles, shared services, and best-in-class contracts where appropriate to reduce procurement overhead and ensure secure-by-design technology adoption.
- Improve software supply chain transparency and ensure alignment with secure-by-design and secure software development practices.
- Establish clear service-level expectations, governance mechanisms, and accountability structures between CISA and participating agencies.

The Committee expects that centralizing CIO services for small agencies could allow participating agencies to reduce duplicative IT management structures, rationalize tool spending, and reallocate full-time equivalents toward mission priorities. Over time, savings generated through reduced contract duplication, consolidated licensing, and streamlined cybersecurity operations may offset the cost of the centralized service model.

CISA should ensure that the operational management of the pilot remains within the agency to preserve unity of command and cybersecurity accountability. As CISA assumes CIO responsibilities, it would also assume associated enterprise risk management responsibilities for the IT and cybersecurity posture of participating agencies.

Funding provided for this pilot is available only for fiscal year 2027. Not later than 60 days after the end of fiscal year 2027, CISA is directed to submit a report to the Committees on Appropriations of the House of Representatives and the Senate that includes:

- An assessment of operational effectiveness and service quality;
- Lessons learned and implementation challenges;
- A detailed accounting of costs incurred by CISA and participating agencies; and

- An estimate of projected cost savings or cost avoidance in future fiscal years if the pilot were continued or expanded governmentwide.

The Committee expects this evaluation to inform future decisions regarding broader adoption of centralized CIO services for small agencies across the Federal Government. ATTACHMENT 2: DRAFT OMB PASSBACK LANGUAGE

For FY[XX] budget submissions, agencies are directed to utilize CISA's CDM enterprise acquisition and shared services for the procurement of core cybersecurity capabilities where CDM vehicles are available. Core capabilities include Endpoint Detection and Response / Extended Detection and Response, Cloud-Native Detection and Response, Identity and Access Management / Privileged Access Management, enterprise vulnerability/asset management, centralized logging/ Security Information and Event Management, and Zero Trust access and network security solutions and AI security and assurance (as CDM-supported tools become available). These categories reflect the capability areas necessary to implement Zero Trust Architecture across the FCEB, consistent with the Administration's Cyber Strategy, M-22-09, and the CISA Zero Trust Maturity Model. Agencies should coordinate planned procurements with CISA and OMB prior to obligating funds. Where agencies choose alternate procurement approaches, they must justify why CDM vehicles are not suitable, and document expected impacts on interoperability and cost.

Implementation & Funding:

Agencies are expected to prioritize CDM vehicles for appropriate requirements and to negotiate reimbursement or transfer arrangements with CISA. OMB will favorably consider funding requests that route core cybersecurity investments through CDM in final apportionments.

Reporting & Timeline:

Agencies will:

1. Provide CISA and OMB with a procurement coordination plan within 45 days.
2. Report semi-annually on progress toward CDM adoption and any deviations.

Exceptions & Appeals:

Agencies may seek exemptions with documented justification; OMB will review and respond within 45 days. OMB may apply budgetary incentives (e.g., priority apportionment or expedited approval) for agencies that comply.