ARMIS®

Public Sector

SOLUTION BRIEF

REALIZING THE GOALS OF CDM

How Modernizing Can Close Agency Threat Visibility Gaps

Although the Continuous Diagnostics and Mitigation (CDM) program was established in 2012, its goals are still valid today:

- Reduce agencies' threat surface.
- Increase visibility into the federal cybersecurity posture.
- Improve federal cybersecurity response.
- Streamline Federal Information Security Modernization Act (FISMA) reporting.

The CDM data is intended to be foundational; aligning all parts of the federal IT mission to enable real-time situational awareness and reduce the workload on federal cybersecurity practitioners. CDM does this by automating the collection of systemic vulnerabilities regardless of whether they were procured through hardware and software, or created through misconfigurations.

Where CDM Is Today

Despite the tremendous efforts of the CDM program over the last decade, it continues to fall short and struggles to maintain pace with cyber threats and the increased variety and volume of IT assets connecting to federal networks. Complicated architectures with off-label deployments, custom integrations slowing innovation, and misaligned incentives between a web of stakeholders means even the basics of comprehensive visibility have not been achieved.

These issues are magnified by a rapid increase in cloud services and the expanding number of unmanaged and undermanaged devices across the enterprise – services and devices which are still outside the scope of typical CDM engagements (e.g. workloads, mobile, IoT, medical devices, and facilities technology). Industry studies estimate that traditional IT assets (PCs, laptops, servers) are far less than 50% of the total number of assets in an enterprise environment – and a number which will continue to shrink.

The explosion of endpoints beyond traditional IT is amplifying the "visibility gaps" and "problems of perspective" experienced by federal agencies. Shadow IT and bottom-up budgets mean IT and security leaders do not manage nor are they even aware of all the vulnerable assets within their environment. Challenges exist within the IT family as well. IT operations, cyber operations, and risk management teams all function with disparate opinions about what exactly is being protected and no one perceives the attack surface holistically. This complicates response, leaves attack surfaces unprotected, and leads to time wasted in manual assessments and audits.

What's Needed Now

Solving these issues doesn't require more tooling, but better coordination. Between CDM and agencies' own efforts, there are plenty of capabilities already in place, each with their own opinions on the state of the network. In this environment and in its current iteration, CDM is at odds with ground truth and even with numerous federal directives. While CDM scope remains limited to standard computing environments, BOD 23-01, M-23-03, and M-22-09 all drive federal agencies to expand their risk management practices to IT/OT and other undermanaged devices.

The extent of the current visibility and management gap is a serious threat to federal networks and our country. The major obstacles to achieving the CDM vision revolve around the absence of IT/OT device profiling and the failure to deduplicate/rationalize IP devices identified by various tools.

Agencies need to modernize their approach to CDM by:

- Deploying cloud-based solutions for scaling across federated environments.
- Leveraging the solutions they already have in place.
- Consolidating the sensors in Layer A to what is providing value to the organization.
- Overhauling their Layer B solution with a cloud-first model.

By integrating with the tools you have in place, Armis can provide the Layer B solution for federal agencies, while also enhancing Layer A with information on previously unseen and unknown assets.

Agencies are struggling to account for an unprecedented growth in the number of devices, and device types, connecting to their networks. This explosion of devices is being driven by digital transformation and the need to innovate with new technologies. Agencies need to monitor and protect OT and IoT assets as well as traditional IT assets.

BOD 23-01 put the responsibility for Layer A capabilities squarely on the shoulders of individual agencies. The efficacy of a cloud-first model has been proven in the CDM program, and can be used to provide stronger Layer B capabilities to secure program success.

It’s time to realize the full potential of the CDM program. Agencies must achieve a consolidated view of their risk posture that is accurate and timely. This requires a clear risk status and vulnerability posture for every device and possible attack path, and the ability to rapidly respond to incidents.

Why Armis?

➤ **Comprehensive**
Discover and classify all devices on your networks.

➤ **Agentless**
Nothing to install, no configuration or device disruption.

➤ **Passive**
No device scanning or network impacts.

➤ **Frictionless**
Installs in minutes using existing infrastructure.

Ready to learn more and harden your defenses by closing the visibility gap? Call 1-888-452-4011 or visit armis.com/public-sector.

About Armis

The Armis FedRAMP platform is completely agentless, which simplifies and speeds deployment. It discovers and classifies every device across any environment, including connected devices on and off the environment that most traditional agent-based tools miss. Armis provides a complete, comprehensive, and detailed inventory of an agency's IT, OT, IoT, and cloud assets so agencies can visualize and secure the entire attack surface. The Armis platform allows agencies to detect threats by comparing real-time asset state and behavior and to respond with ease to create automated, policy-based actions such as triggering vulnerability scans or segmenting dangerous devices. Everything works in real-time, so the discovery of assets, identification of issues, and automated enforcement are immediate and continuous.

ARMIS®
Public Sector