Cyber Innovations: Technologies, Tools, & Shared Services via The CISA CDM Program

Cyberattacks are more than a breach of security and trust—they're a financial nightmare. According to IBM, the average cost of a cyberattack in the U.S. is over $9 million, many of these attacks result in damages upwards of hundreds of millions of dollars. To combat these growing attacks and the resulting strain on federal government agencies, the Department of Homeland Security (DHS) established the Continuous Diagnostics and Mitigation (CDM) program in 2012 to share cyber technologies, tools, and services to enhance the United States' overall cyber defense.

The Evolution of the CISA CDM Program

Since its creation in 2017, the Cybersecurity Infrastructure Security Agency (CISA), which is a component organization of the DHS, has led the CDM program to provide numerous government agencies with cost-free access to a growing set of cybersecurity technologies, tools, and shared services through contracts with third-party federal IT and cybersecurity system integrators.

For the past 11 years, DHS and CISA have invested more than $2.3 billion in the CDM program, including $650 million via the American Rescue Plan Act. CISA, which now leads the CDM program, is requesting another $4 billion in funding from the U.S. Congress to manage and expand this program through 2033.

CISA CDM Program Objectives

The four CDM program objectives are to:

1. Reduce the cyberattack surface area of each participating agency.
2. Increase visibility into cyber threats to enhance the United States' cyber posture.
3. Improve the United States' federal cyber incident response capabilities.
4. Streamline the Federal Information Security Modernization Act (FISMA)'s reporting requirements.

Current CDM Program Capabilities

The CISA CDM program delivers hardware, software, and related services capabilities in five key areas:

1. Agency and federal dashboards
2. IT asset management
3. Identity and access management
4. Network security management
5. Data protection management

CISA CDM Program Results

To date, the CDM program successfully deployed more than $2 billion in cybersecurity technologies, tools, shared services, and dashboards to 23 CFO Act U.S. federal civilian agencies. The dashboards serve as a vital visualization tool and the related cyber databases produce customized reports and send cyberattack alerts for the most critical cybersecurity risks to IT leaders.

Today, the CDM Program Shared Services Platform 2.0 provides more than 50 non-CFO Act agencies with access to CDM cybersecurity hardware, software, and services capabilities to enhance the cybersecurity of federal government agencies nationwide.

The Future of the CDM Program

After interviewing several CISA executives, the CDM program future appears to be bright as the agency plans to revitalize the program to increase adoption, including:

- Expanding the approved CDM cybersecurity hardware, software, and services to include more AI and automation capabilities.
- Implementing enhanced cybersecurity tools to support zero trust architecture (ZTA).
- Updating cyber incident response (IR) capabilities via increased automated IR playbooks and security orchestration and automated response (SOAR) technologies.

Five Recommended Cybersecurity Actions

Leveraging the CISA CDM program and other available government contracts, here are five key actions that government organizations can take to enhance their cybersecurity:

- Use flexible and scalable cyber ranges to train cybersecurity analysts via emulated networks and simulated cyberattack scenarios.
- Deploy a proven cybersecurity protection, detection, and incident response system for both IT and operational technology (OT).
- Develop customized ZTA, which leverages data segmentation, creates micro-perimeters, and implements data segmentation gateways to improve data access control.
- Reduce cyber-incident response time by implementing an advanced data analytics capability to streamline and simplify response and remediation.
- Ensure cybersecurity supply chain risk management via a proven effective Cyber Risk Radar using open-source data analysis with advanced data analytics.

Conclusion

The CISA CDM program is one element of a comprehensive plan to defend against all cyber threats. Increasing funding for the CISA CDM program will pay off dramatically in the long run, helping to secure U.S. Federal government agencies and enhance cybersecurity for U.S. citizens across our nation.

By Gregory A. Garrett, Vice President Cybersecurity Peraton