



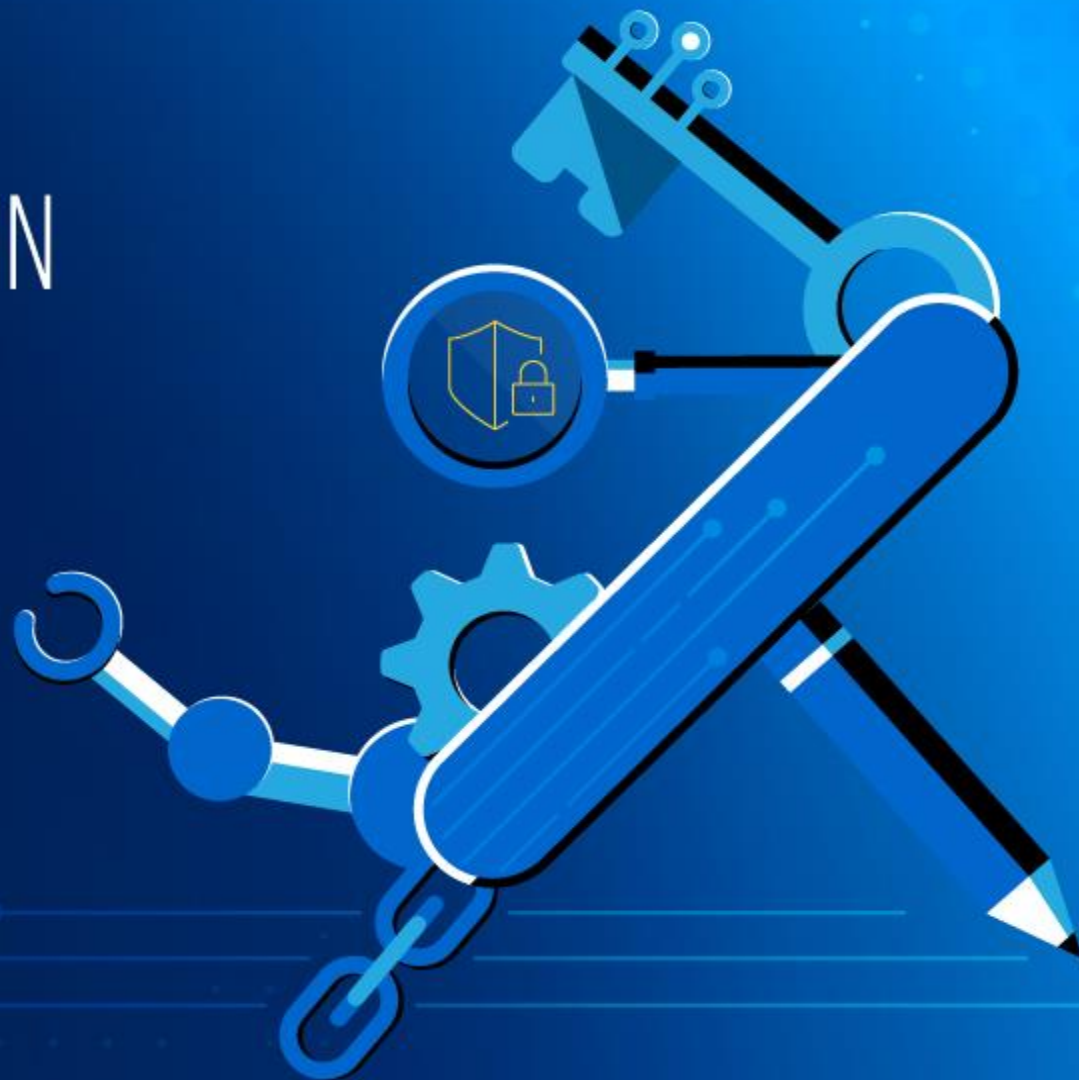
CDM

THE MULTITOOl IN
YOUR CYBER KIT

Underwritten by:



SteelCloud



Introduction

From a Cybersecurity Executive Order to zero trust architectures and agency-specific defense strategies, Federal cyber leaders strive to better protect themselves in a world where attacks seem inevitable. This is where the **Continuous Diagnostics and Mitigation (CDM) Program** can become agencies' greatest ally.

With the right guidance and utilization, CISA's CDM Program can help Feds identify, mitigate, and stop threats before they occur. But are we there yet?

In the latest installment of the CDM research series, MeriTalk surveyed **100 Federal and industry CDM stakeholders** to understand where we are today and how the program will underpin key cyber efforts like endpoint detection and response (EDR) capabilities and threat-hunting environments going forward.



Executive Summary

Cyber Executive Order (EO) amplifies CDM's impact:



Nearly all CDM stakeholders (**93%**) say the Program has **improved Federal cyber** resilience in the past year; **58%** say it's had a major impact



67% believe CDM is more important since President Biden's May 2021 Cybersecurity EO, noting **increases in CDM initiatives** such as EDR; network security and management; and asset management

Still, intake is slow, and dashboards have much more to give:



Fewer than **one in three** Federal cyber leaders give their agency's use of and participation in CDM an "A"



While **55%** have incorporated CDM data feeds into their own risk management process, **89%** feel Feds are just **scratching the surface** of the dashboards' potential

CDM stakeholders say we're not talking enough about the program's potential:



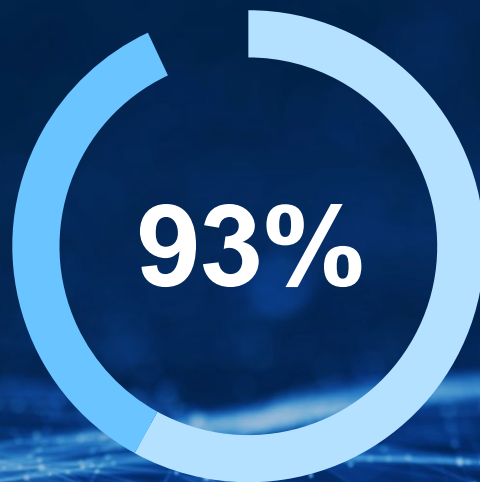
When asked if we're talking about CDM too much or not enough, **68%** say **not enough**



Going forward, CDM stakeholders want to focus improvements on **data quality** and **operationalizing dashboards** across the enterprise

CDM is Weight-Bearing

93% feel the CDM Program has **improved** Federal cyber resilience in the past year



58% say it had a major impact

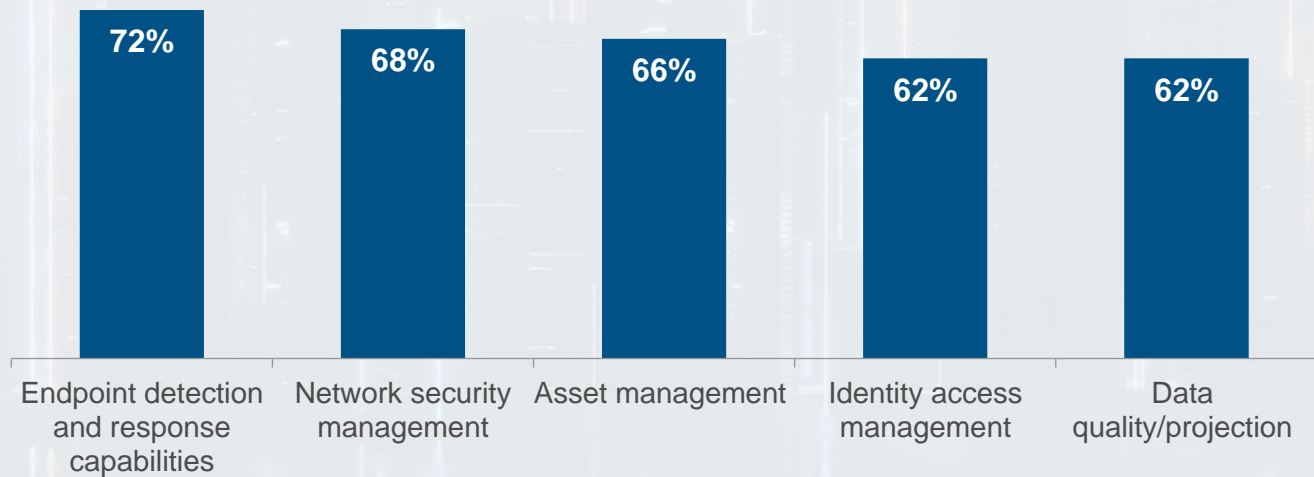


Two out of three (67%) believe CDM has **gained importance** since President Biden's May 2021 Cyber EO

Cyber EO Escalates Adoption



Where has agency prioritization of the following **CDM initiatives** shifted as a result of the Cyber EO? % who have increased prioritization










TAKEAWAY:

CDM and EO Efforts in Lock Step

Tangible Benefits

How have you seen Federal agencies **benefiting** from CDM in the past year?*

-  **49%** Improved visibility and situational awareness
-  **49%** Improved ability to automatically identify assets
-  **41%** Improved reporting accuracy
-  **39%** Streamlined threat monitoring and remediation efforts
-  **31%** Improved risk-management decision-making
-  **31%** Enhanced near real-time risk response capabilities
-  **31%** Streamlined compliance with FISMA

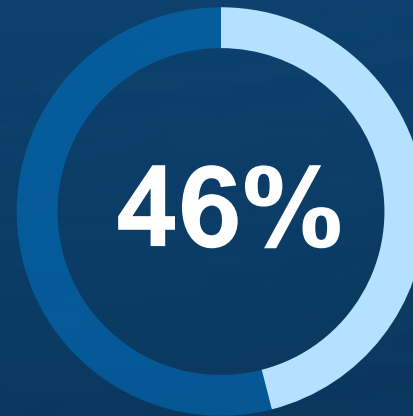
*Respondents asked to select all that apply

Two Steps Forward; Two Steps Back

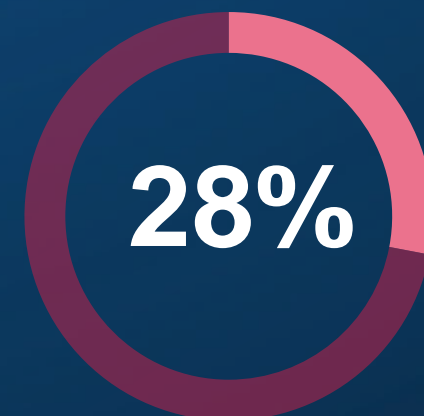
While **53%** say the amount of **data shared** with CISA increased...



...and **46%** say the pace of **CDM adoption** improved



Just **28%** of Feds grade their **use of CDM** an “**A**”



60% still view CDM as more of a compliance-based activity

Dashboard Optimization

55% of Feds have **incorporated CDM data feeds** beyond the dashboard into their own risk management process; another **36%** are working on this



57% have **used CDM to answer a question** previously answered by a human



89%

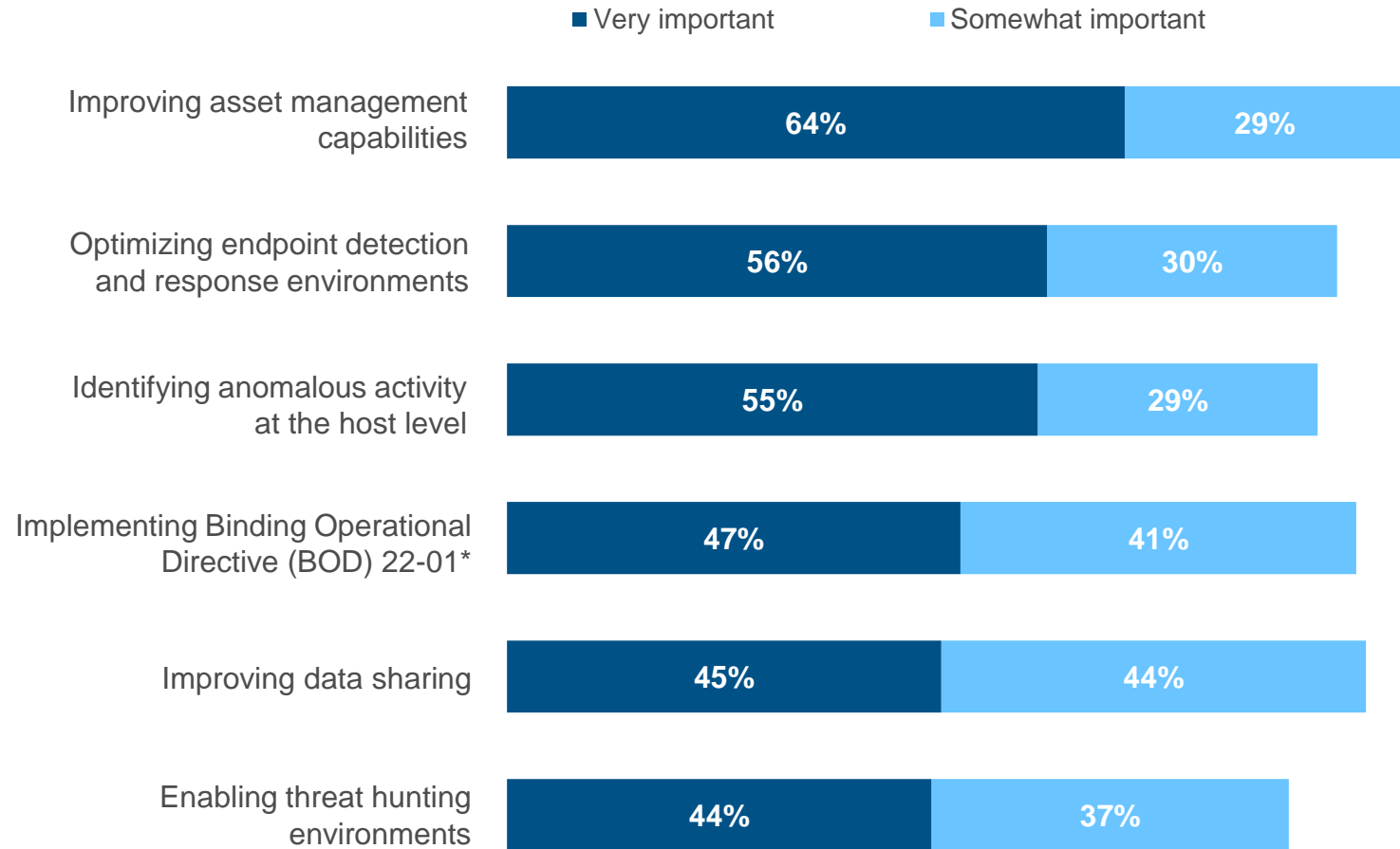
believe Federal agencies are **just scratching the surface** of the CDM dashboards' potential

TAKEAWAY:

Infinite Potential for Further Utilization

Shared Success

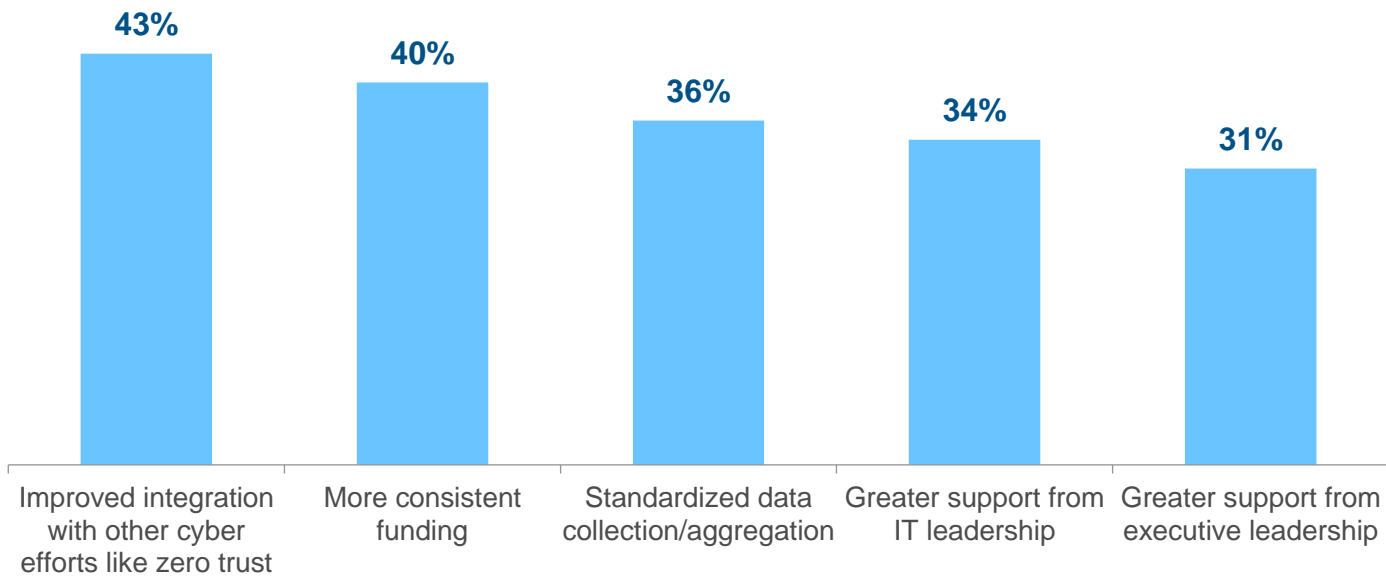
Going forward, how important is the CDM Program to the **success** of the following Federal cybersecurity initiatives?



*BOD 22-01 requires agencies to remediate high-risk vulnerabilities from a CISA-managed catalog

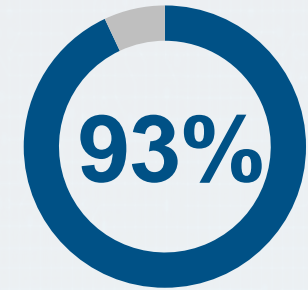
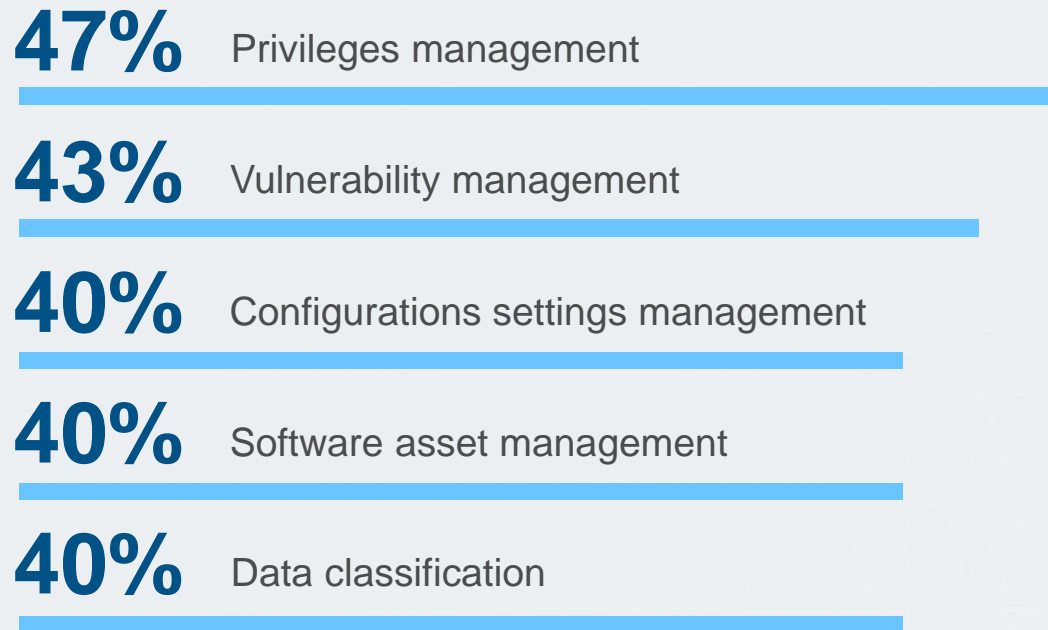
Keys to Integration

What do Federal agencies need to **better integrate and operationalize** CDM dashboard data across their existing security operations?*



Upcoming Investments

Feds: Which **CDM capabilities** will you invest in over the next two years?*



feel Federal agencies should
prioritize threat hunting

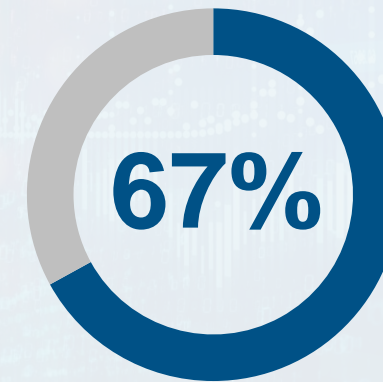
TAKEAWAY:
CDM Sets the Foundation

Fortifying the Future

OMB's latest FISMA guidance says **CISA will review the CDM program** and lessons learned to improve the program for FY2022.

Where should the CDM PMO focus **improvements**?*

- 1 Data quality **(67%)**
- 2 Operationalizing dashboards across the enterprise **(45%)**
- 3 High availability/disaster recovery **(37%)**
- 4 Dashboards-as-a-Service **(35%)**



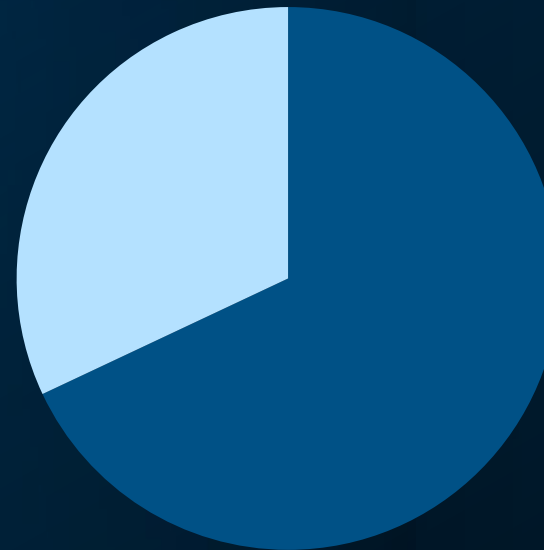
would like to see the CDM Program **reauthorized** in the next three years

*Respondents asked to select all that apply

Critical Conversation

Overall, is the Federal government **talking about CDM** too much or not enough?

32%
Too much



68%
Not enough



Advice from Cyber Defenders

If you could **tell Congress** one thing about the CDM Program, what would it be?

“ **Greater acceleration** of funding, integration, and accountability for agencies. **Utilize AWARE** scores, establish repercussions for agencies not meeting requirements, and reward the agencies gaining momentum”

“ CDM must **address ongoing modernization** and zero trust, and catch up to the agencies who already have adopted secure cloud solutions to accomplishing their missions in a cost effective, realistic manner”

“ Agency needs vary greatly; CISA must embrace an **agile and adaptive approach** that truly embraces the principles of zero trust”

“ More closely align (or merge) the CDM Program with **zero trust**. They are different but complementary, and implementations should be coordinated”

“ Help address the **skilled labor shortage** to help accelerate the CDM mission pace. This is the biggest bottleneck”

“ **Mandate CDM** at the Federal level. Provide funding to support CDM efforts throughout the Federal enterprise, including DoD”

Recommendations

Accelerate Implementation

93% of CDM stakeholders credit the program with improving Federal cyber resilience in the past year. Notable improvements include increased network visibility, streamlined threat monitoring and remediation, and enhanced risk response.

Still, **less than 1/3** would grade their use of and participation in CDM an “A.”

Agencies should work to accelerate adoption while continuing to increase communication and information sharing with CISA, Feds, and industry partners – especially around practical security outcomes. It’s time to move beyond compliance to tactful utilization.

Make the Most of Dashboard Data

Despite slow adoption, agencies are making progress. **More than half** (55%) have applied CDM data feeds into their own risk management process and **57%** have used CDM data to answer a question which previously had to be answered by a human.

Nevertheless, **89%** believe Federal agencies are **just scratching the surface** of the CDM dashboards' potential.

Agencies must work with CISA on improving data quality and standardization to maximize dashboard applications and make the most of growing cyber data.

Integrate with Purpose

CDM stakeholders see the program as change-maker and critical component of achieving the administration’s overall cyber goals.

Eighty-four percent believe the program is critical to their agency’s alignment with the Cybersecurity EO and many credit the EO with increasing their prioritization of **CDM efforts** such as endpoint detection and response; network security and management; and asset management.

Going forward, cyber leaders need to think holistically and work to integrate CDM with other key department initiatives like zero trust strategies and threat-hunting.

Methodology

Industry respondent job titles

CIO/CTO/CFO	21%
Deputy CIO/CTO/CFO	11%
IT Director/Supervisor	23%
Cybersecurity Program Manager/Officer	19%
Cybersecurity Analyst/Engineer	11%
Cybersecurity Consultant/Specialist	2%
Software/Applications Development Manager	6%
Data Center or Network Manager	6%

Federal respondent job titles

Federal Cybersecurity Program Lead	13%
Federal CDM Program Lead	13%
Federal Cybersecurity Functional/Technical Lead	45%
Federal Cybersecurity Consulting Lead	6%
Federal Cybersecurity Sales/Business Development Lead	11%
Federal Cybersecurity Policy or Government Affairs Analyst	2%
Other	9%

Employer

Vendor or Systems Integrator (SI)	53%
Civilian Agency	47%


Expertise

100% of qualifying respondents are familiar with their agency's current CDM adoption efforts or the efforts of Federal agencies they support

MeriTalk conducted an online survey of 100 Federal and industry CDM stakeholders familiar with their agency's CDM adoption efforts or the efforts of Federal agencies they support in March of 2022. The report has a margin of error of $\pm 9.78\%$ at a 95% confidence level.

Thank You



www.meritalk.com 
report@meritalk.com 