MeriTalk
Improving the Outcomes of Government IT

FORTINET

splunk>
turn data into doing™

tenable

CDM Referendum:

How is the Program Performing?

September 25, 2019

Introduction

DHS' **Continuous Diagnostics and Mitigation (CDM)** program is ever-evolving, adapting to meet the cybersecurity needs of Federal agencies. Despite making tremendous strides in providing agencies with a roadmap, CDM still has a ways to go before becoming a true cybersecurity success story.

Is CDM continuing to **drive Federal cyber hygiene**? What do key stakeholders think about the current pace, payoffs, and potential of new measures like AWARE, DEFEND, and the upcoming dashboard revamp? What recommendations do they have for DHS – and do Feds and industry agree?

In the "**CDM Referendum**" study, MeriTalk surveyed more than 160 Federal and industry CDM stakeholders to understand their experiences with the program and suggestions for the future. The study measures progress and challenges, and outlines keys to long-term success.

Executive Summary

- The CDM program is improving Federal cybersecurity:
  - **85%** say CDM has improved Federal cybersecurity – **22%** say CDM has **significantly improved** Federal cybersecurity; **63%** say somewhat improved
  - Most effective area? **Increasing visibility** into the Federal cybersecurity posture
  - Feds and industry agree CDM's doing a **good job** maintaining open lines of communication between DHS, vendors, and other agencies, as well as continually updating guidance

- But CDM still struggles with inertia, culture challenges, and budget uncertainties:
  - **64%** say CDM is rolling out **too slowly** and just **40%** feel CDM is **keeping up with** the changing cyber landscape
  - Just **27%** of Feds say their agency can maintain its CDM progress with current budget allocations
  - And while Feds and industry agree **culture** and **training** are the biggest roadblocks to CDM, they disagree on the **future** of the program – Feds want to focus on high-value environments; industry on broader cyber solutions

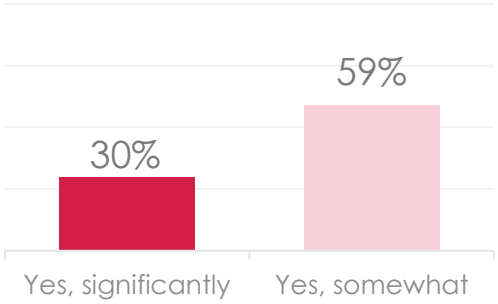
- Stakeholders recommend a path forward:
  - When asked to consider lessons learned, agencies recommend **incremental adoption**, **cloud integration**, and **improved communication**
  - Over the next three years, stakeholders would like to see DHS focus on **early gaps** in CDM capabilities adoption and expanding CDM **applications in cloud**

CDM Impact

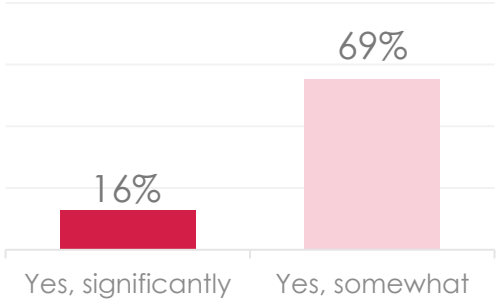
- **85%** of stakeholders say CDM has improved Federal cybersecurity, but **just 22%** say it's made a significant impact

Has CDM improved Federal cybersecurity?

Feds say:



Industry says:

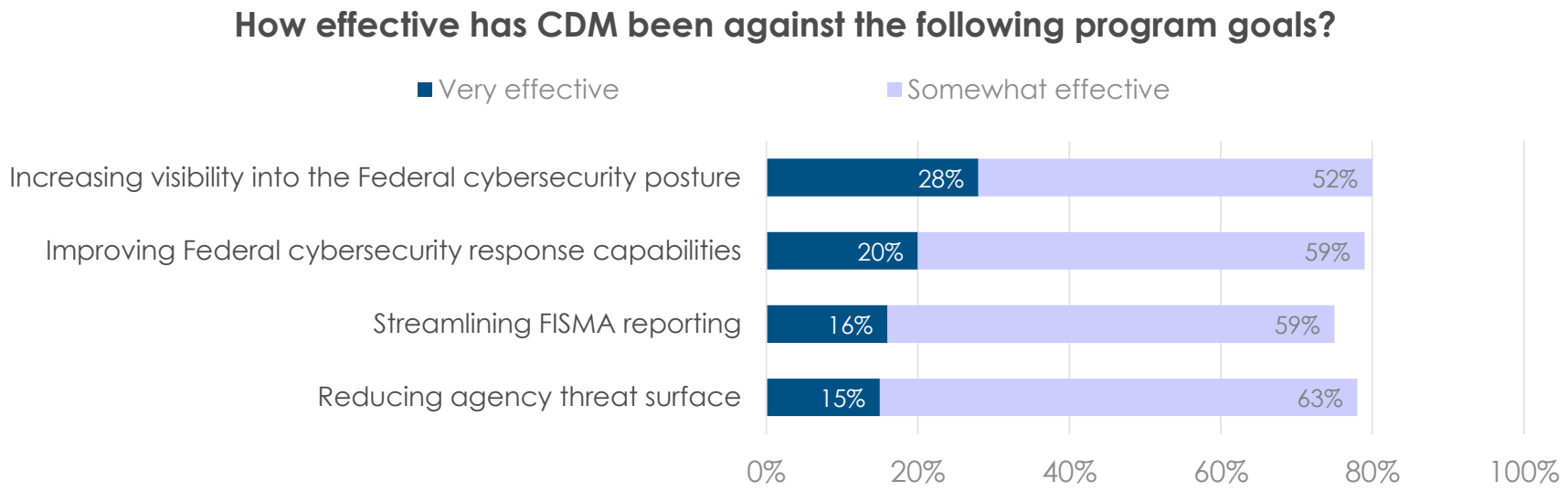


*Feds are nearly **twice as likely** as industry respondents to say CDM's made a significant impact*

Take away: Incremental Progress, but Moving in the Right Direction

Progress Against Goals

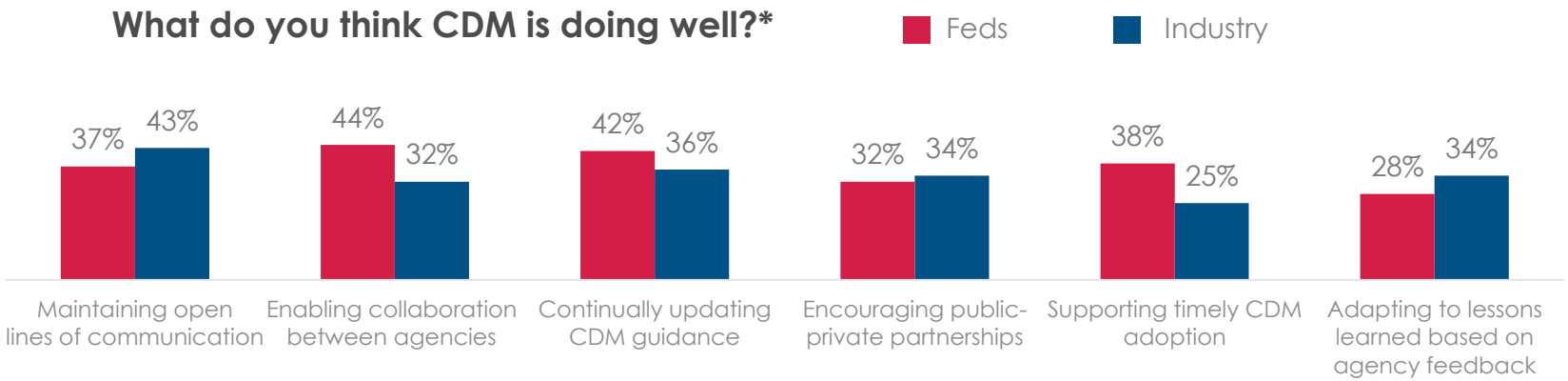
- Stakeholders say CDM has been most effective at increasing visibility into the Federal cybersecurity posture



Take away: Advancement Across the Board

What's Working?

- Feds and industry agree CDM's doing a good job maintaining open lines of communication and continually updating guidance



"CDM is proficient at increasing the signals available to the Federal government but has not addressed the actions resulting from the additional information. Mitigation and automation are still lagging."

Take away: Feds More Likely to Praise Collaboration and Pace

*Respondents asked to select all that apply

What's Not Working?

- Feds and industry agree culture and training are the top roadblocks to CDM success

What are the biggest challenges to CDM?*

59% Culture

54% Training IT and security staff

48% Difficulty integrating legacy systems

44% Challenges with competing priorities

38% Procurement speed

Culture, training, and legacy integration also **topped the list** of agency CDM challenges in 2014**

In 2019, **Feds** were **significantly more likely** than industry respondents to see training and legacy integration as challenges – **62%** to 45% and **55%** to 42%, respectively

Take away: Culture Issues Continue to Hold CDM Back

*Respondents asked to select all that apply **Accordingly to MeriTalk's 2014 "CDM: Under the Hood" study

Adoption Lag

- While Feds are more forgiving than industry, both agree CDM must pick up the pace

64% say CDM is rolling out too slowly & just **40%** say it's keeping up with threats*

Feds are significantly more likely than industry stakeholders to say CDM is rolling out in a timely fashion – **49%** to **24%**,

and

that it's keeping up with the changing cybersecurity landscape – **56%** to **27%**

Just **17%** say DEFEND task orders will have a significant positive impact on CDM adoption speed

"CDM requirements were built in 2011; the protections aren't relevant for the modern threat landscape. Agency owners are compliance-focused vs. cyber-focused."

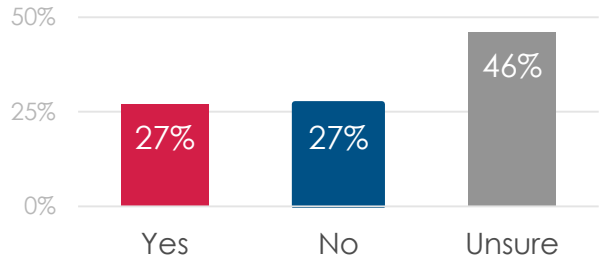
Take away: Five Years Later, We're Still Too Slow*

*In MeriTalk's 2014 "CDM: Under the Hood" study, 58% said CDM was rolling out too slowly

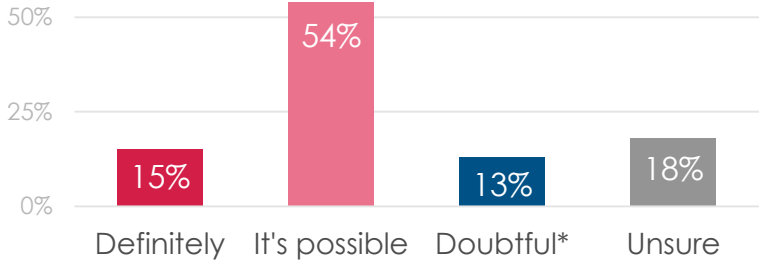
Budget Uncertainty

- Just **27%** of Feds say their agency can maintain its CDM progress with current budget allocations. Even fewer – **15%** – of industry stakeholders feel confident the DEFEND task orders will have enough time to impact the program

Feds: Can your agency maintain its CDM progress with current budget allocations?



Industry: The new DEFEND contract runs six years. Will this be enough time to impact the program?



Take away: Agencies Need Long-term Support

*Percentage who selected "unlikely" or "no way"

Sensor Challenges

- Despite sensor challenges, the new CDM dashboard is expected to help enable better visibility

Just **20%** **of Feds** say they're collecting high-quality data from CDM sensors

64% say the new CDM dashboard contract will help enable better visibility into sensor data

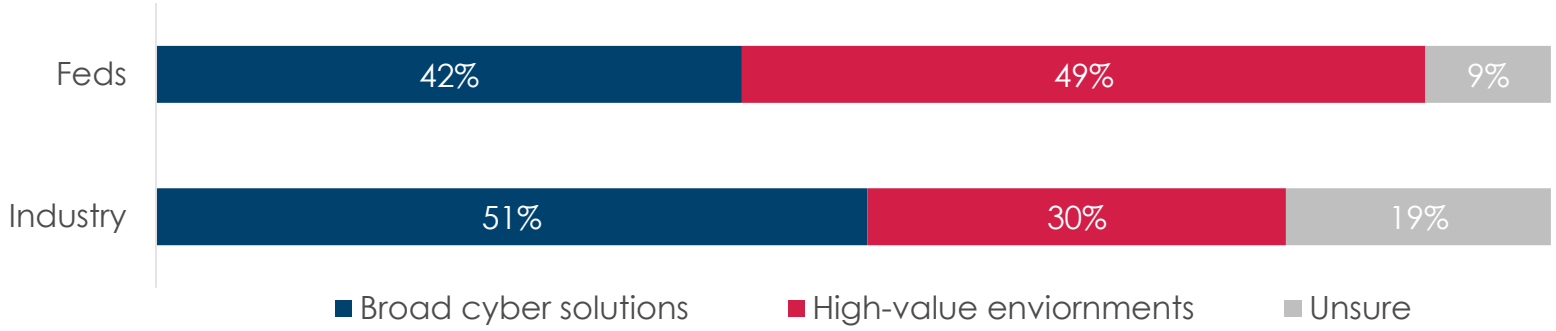
Take away: Help is on the Way

Strategic Confusion

- Feds and industry disagree on the strategic direction of the CDM program

In April, **CDM Program Director Kevin Cox** noted the program was facing a **question about its future** – "Will [CDM] become this wider sense of getting full cybersecurity solutions in place across all these different capability areas, or will we be more targeted on high-value assets, specific environments, etc.?"

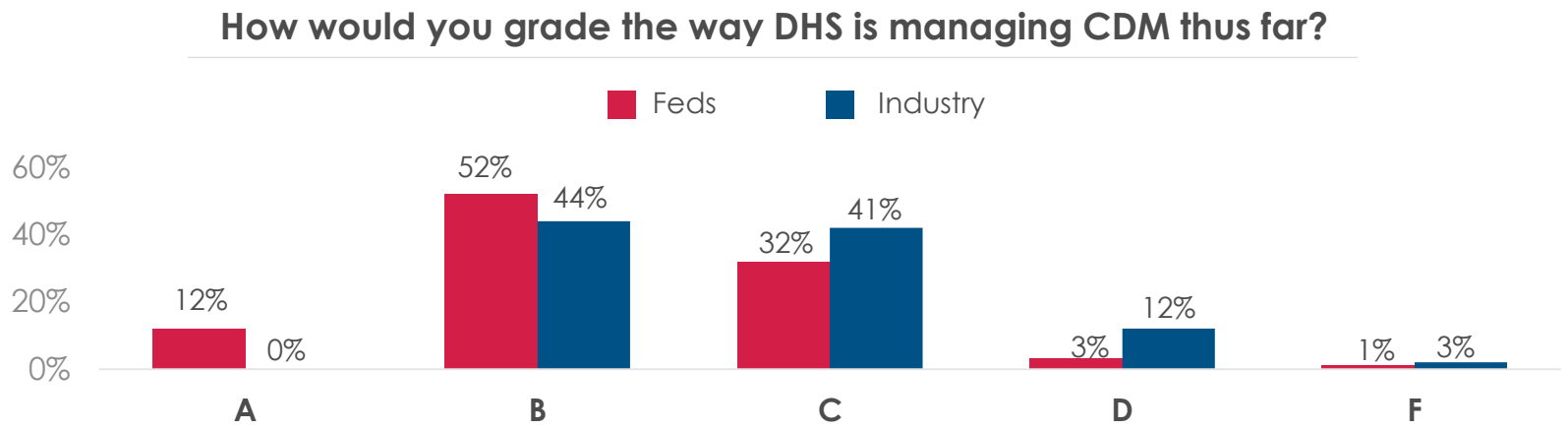
Where do you think CDM should focus?



Take away: Collaboration Needed

DHS Spotlight

- When asked to grade DHS' CDM management, Feds gave as many A's as industry gave D's



"Confusion over continuing costs, staffing needs, and installation assistance has led our agency to suspend interest and participation. CDM must provide clarity, communication, and direct assistance to small agencies."

Take away: Room for Management Improvement

The Road Ahead

- Moving forward, Feds and industry agree DHS should revisit early CDM adoption and cloud environments

Where should DHS focus improvements over the next three years?*

53%	Helping agencies address gaps in early CDM capabilities adoption
49%	Expanding CDM applications in cloud environments
40%	Enhancing collaboration between agencies
36%	Continuing to expand and improve acquisition options
34%	Expanding CDM applications in mobile environments
30%	Enhancing public-private collaboration

Just 26% would like to see DHS focus on successfully evaluating security postures through the **AWARE algorithm**

Take away: Fortify the Foundation Before Moving Forward

*Respondents asked to select all that apply

Advice for DHS

- Stakeholders recommend specialized training, streamlined processes, and budget details to move CDM forward

What changes should CDM make to further improve Federal cybersecurity?

"Offer specialized training across the agencies"

"Streamline the process for vetting and adding solutions; continue to push for adoption across all public sector agencies"

"Centralize databases and automate incident reporting. Eliminate false positives"

"Enhance onsite assistance and future budget planning for long-term support"

"Reduce the documentation burden on applications and focus it more on infrastructure and end-to-end processes"

Take away: More Guidance Needed

Advice for Agencies

- Stakeholders say successful agency adoption hinges on iterative adoption, adaptability, training, and cloud integration

What is the most important lesson you've learned from the CDM process to date?

"Implementation needs to be incremental and iterative"

"Speed and flexibility must be inherent in culture and procurement"

"Find a way to integrate CDM into the cyber incident response team (IRT) to promote collaboration, improve data classification, and enhance efficiency"

"Cloud adoption is imperative to success of the program. Data cannot be trusted unless it is timely. Stakeholders should be cybersecurity professionals"

"Full transparency and collaboration are essential for cyber situational awareness"

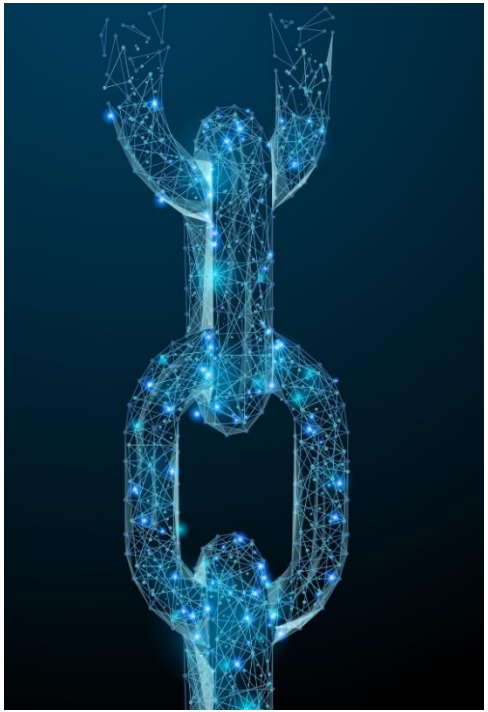
Take away: Opportunity to Share Lessons Learned

Recommendations

Start at the Beginning: While CDM has moved beyond the concept of phases, many agencies still struggle with early adoption issues. It's difficult to hit a moving target. Collaborate with DHS, industry, and other agencies to set a solid foundation with initial CDM steps, like ensuring asset and user visibility, before moving forward.

Focus on the Workforce: Culture and workforce knowledge have remained top CDM challenges for the past five years. Feds and industry agree that agencies – with the help of DHS – must expand conceptual and hands-on training for IT and security staff to ensure CDM success. Prioritizing this effort may bring necessary culture change from the inside out.

Communicate the Big Picture: Feds and industry stakeholders have concerns around CDM's pace, long-term budget feasibility, and strategic program direction. DHS and agency leadership must come together to discuss the path forward and then proactively share their findings with the broader CDM community via opportunities with the revamped dashboard, small group sessions, and larger-scale events.



Methodology & Demographics

MeriTalk, on behalf of our underwriters, conducted an in-person and online survey of 164 Federal and industry CDM leaders in August 2019. The report has a margin of error of ±7.62% at a 95% confidence level.

Respondent job titles*

Executive leadership role (Director+)	16%
Federal cybersecurity lead/manager	28%
Cybersecurity program manager or supervisor	22%
Cybersecurity engineer/specialist	15%
Software/applications development manager	6%
Other IT manager	13%

Organization type

Federal government: Civilian agency	52%
Federal government vendor, contractor, or Systems Integrator (SI)	48%

Expertise

100% of qualifying Federal IT managers and System Integrators are familiar with CDM and have at least some level of involvement with the program

*Based on online respondents

Thank You

www.meritalk.com

egarber@meritalk.com

703-883-9000 ext. 146