Agency Priority Goal | Action Plan | FY 23 – Q1

Strengthen Federal Cybersecurity

Goal Leader(s):

Matthew Hartman, Deputy Executive Assistant Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency

Goal Overview

Goal statement

- Defend and secure the Federal Enterprise through a collaborative risk management effort with departments and agencies to coordinate risk response and interagency policy actions. By September 30, 2023, 50% percent of federal agencies will meet the end of year Binding Operational Directive-22-01 [Known Exploited Vulnerabilities] requirement for leveraging automated Continuous Diagnostics and Mitigation reporting and CISA will achieve measurable progress toward enhancing operational visibility within the Federal Civilian Executive Branches by improving asset discovery and vulnerability enumeration.

Problem to Be Solved

- Network visibility limitations due to encryption and cloud computing
- Constantly evolving threat landscape and rapid pace of change in the cyber domain compared to the pace of federal government policy generation and implementation
- The Federal Enterprise was not designed to be defended or managed as a single organization, and many federal agency networks are indefensible in part because they are decentralized. This decentralization creates obstacles for effective governance and for standardization of tools and services.
- Outdated and legacy technology poses risk of increased vulnerabilities associated with weak authentication exposure and unpatched software
- Technology investments are often not aligned with operational priorities for cyber defense

What Success Looks Like

- The Executive Order on Improving the Nation’s Cybersecurity empowers DHS with additional authority to gain visibility into the federal enterprise and take action to safeguard systems
- Ramp up use of CISA-approved standardized tools and shared services to make federal networks more defensible and secure
- Agencies can identify threats and vulnerabilities and report on them using the Vulnerability Disclosure Program in advance of network disruptions
- CISA can identify cross-agency threats and vulnerabilities at the Federal Enterprise Level to provide a holistic view of the cyber threat, including access to host-level data and integration of data sources from across CISA’s cyber programs

Tracking the goal

Goal target(s)

In the table below, please repeat the key metrics included in the goal statement (previous slide) that will be used to track progress.

Please update this column each quarter.

Achievement statement		Key indicator(s)	Quantify progress			Frequency
Repeat the achievement statement from the goal statement on the previous slide		A “key performance indicator” measures progress toward a goal target	These values enable us (and you!) to calculate % complete for any type of target*			When is there new data?
By…	We will…	Name of indicator	Target value	Starting value**	Current value	Update cycle
09/30/23	Achieve measurable progress toward enhancing operational visibility within the FCEB by improving asset discovery and vulnerability enumeration.	Percent of federal agencies who meet BOD-22-01 [Known Exploited Vulnerabilities] automated reporting requirement for leveraging CDM reporting	50%		45%	Quarterly

* Even qualitative targets! If the target is to achieve a qualitative outcome, quantify progress this way: 1=“Yes, we achieved it”, 0=“No, not yet”

** As of 10/1/2021

Goal Strategies

Strategy 1: Lead Cyber Defense Operations

Respond to Threat Activity and Incidents

- Conduct and coordinate cyber defense operations to address the top active threats and mitigate critical vulnerabilities in the Federal Enterprise.
- Proactively detect, respond to, and mitigate risks of significant threat activity and critical vulnerabilities for these partners, and stop threats before disruption occurs and minimize the impact of incidents.

Mitigate Critical Vulnerabilities

- Mitigate critical vulnerabilities through reporting of software vulnerabilities, coordinating disclosure and patch development, and Federal Civilian Executive Branch (FCEB)-wide mitigation activities.

Strategy 2: Strengthen Cyber Risk Management

Proactive Risk Management

- Support Departments and Agencies to prioritize and manage strategic risks at an acceptable level, by working with partners to continuously prioritize their most significant risks and address them before network services are disrupted.
- Apply risk management, governance, and compliance principles at the Federal Enterprise level to see and manage strategic risks spanning across multiple agencies.

Take Responsibility for Risk

- As the Nation’s risk advisor, ensure that the most significant risks to Mission Essential Functions are being addressed in a timely manner.

Strategy 3: Provide Cybersecurity Tools & Services

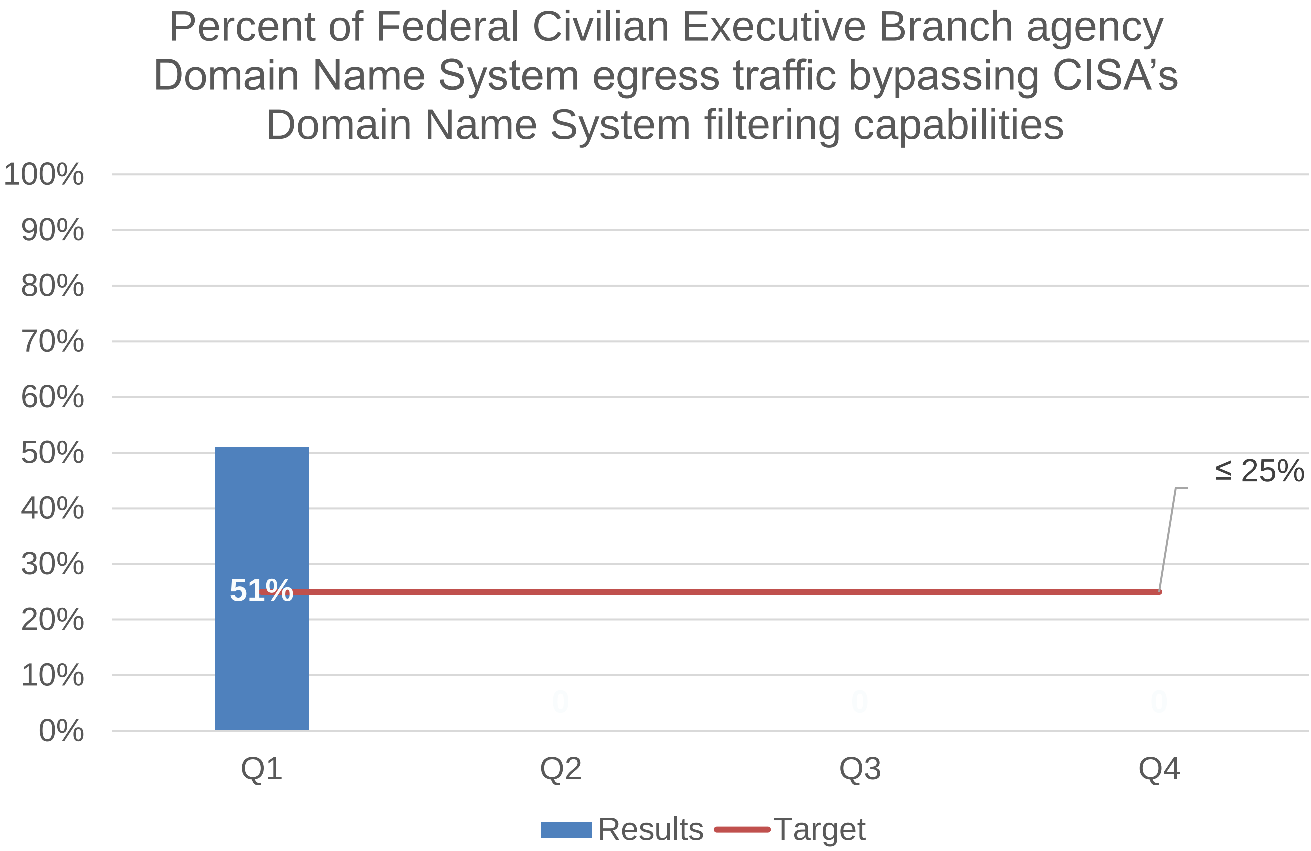
Provide Tools and Services

- Offer cybersecurity tools and services to FCEB agencies to assist them in achieving efficiencies, affordability, and standardization and quickly develop, deploy, and scale new services as needed. These tools and services address priority threats, provide situational awareness of risk postures, and build relationships in advance of an incident.
- Provide an adaptive suite of tools and services that demonstrably fill key gaps in managing priority strategic risks.

Manage Relationships/ Requirements

- Coordinate engagement with FCEB stakeholders to address priorities on cyber defense, risk management, and service needs and incorporate feedback into future service offerings.

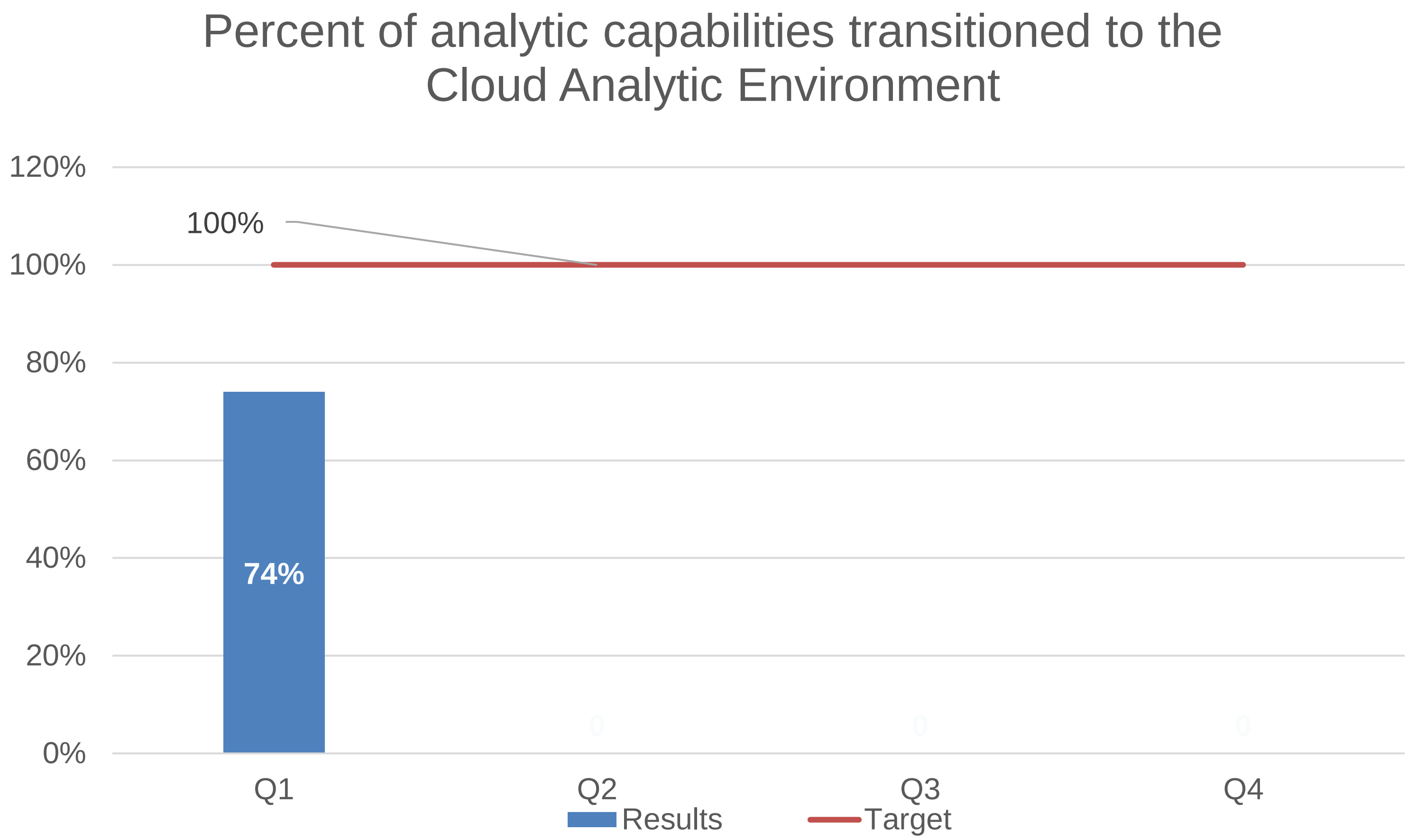
Key indicators


Percent of Federal Civilian Executive Branch agency Domain Name System egress traffic bypassing CISA’s Domain Name System filtering capabilities

The percent of Federal Civilian Executive Branch Agency Domain Name System egress traffic bypassing CISA’s Domain Name System filtering capabilities has decreased significantly since FY22 Q4 (81%) due to the increase in adoption of protective DNS by FCEB agencies.

During the FY23 Q1 collection, the Threat Hunting team identified two issues that are statistically insignificant for Q1 and did not impact the quarter’s result. The team is continuing to investigate the issues and will provide updates when available.

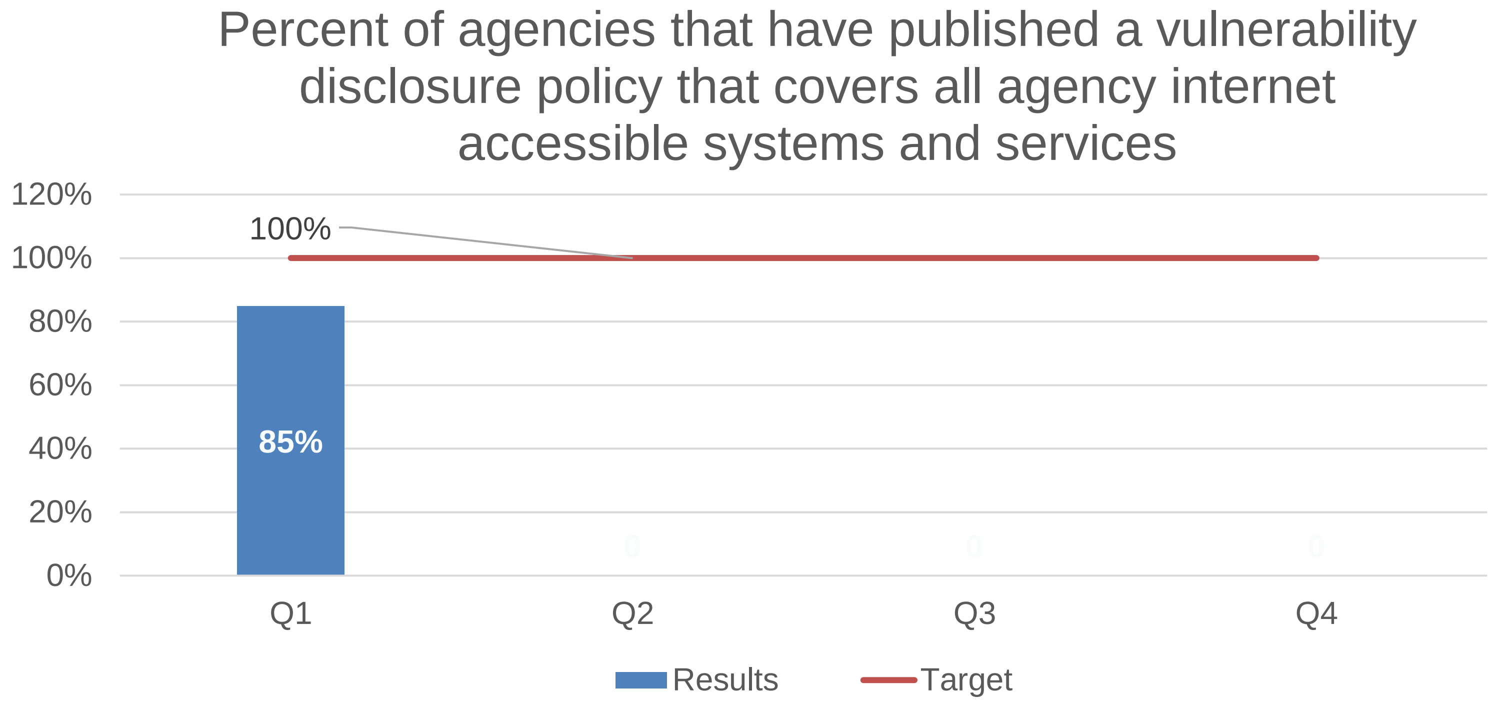
Key indicators



Twenty of 27 tools have completed migration to the Cloud Analytic Environment. Six additional tools are in progress and one tool is in the backlog to be planned for a later program increment.

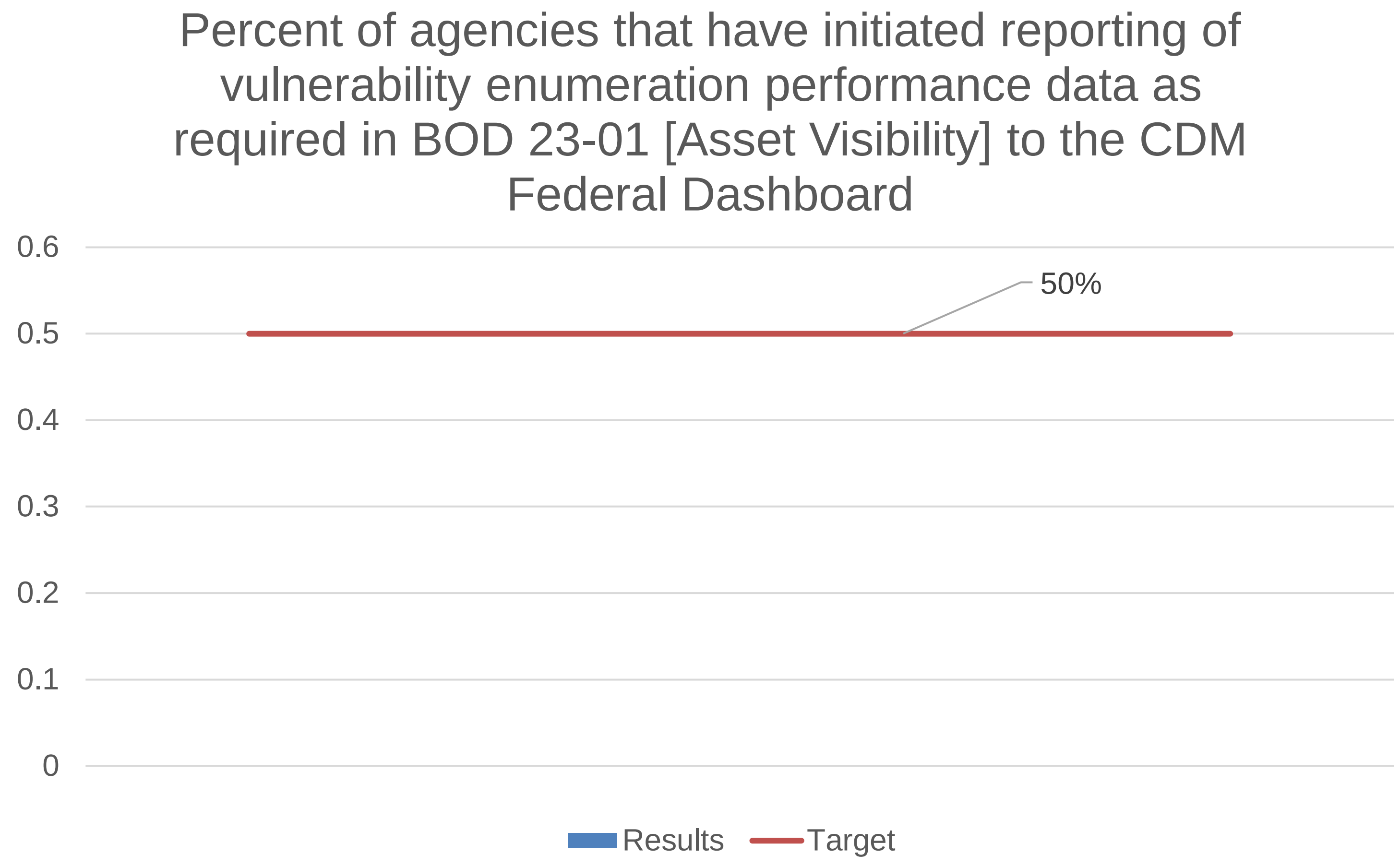
While the percentage is the same as Q4 FY22, progress continues with the six tools that started in Q4. The team anticipates that three tools will be completed in Q2 FY23.

Key indicators



Nearly all 101 Federal Civilian Executive Branch agencies (99%) have published a vulnerable disclosure policy (VDP) and 86 have a VDP with all systems in scope.

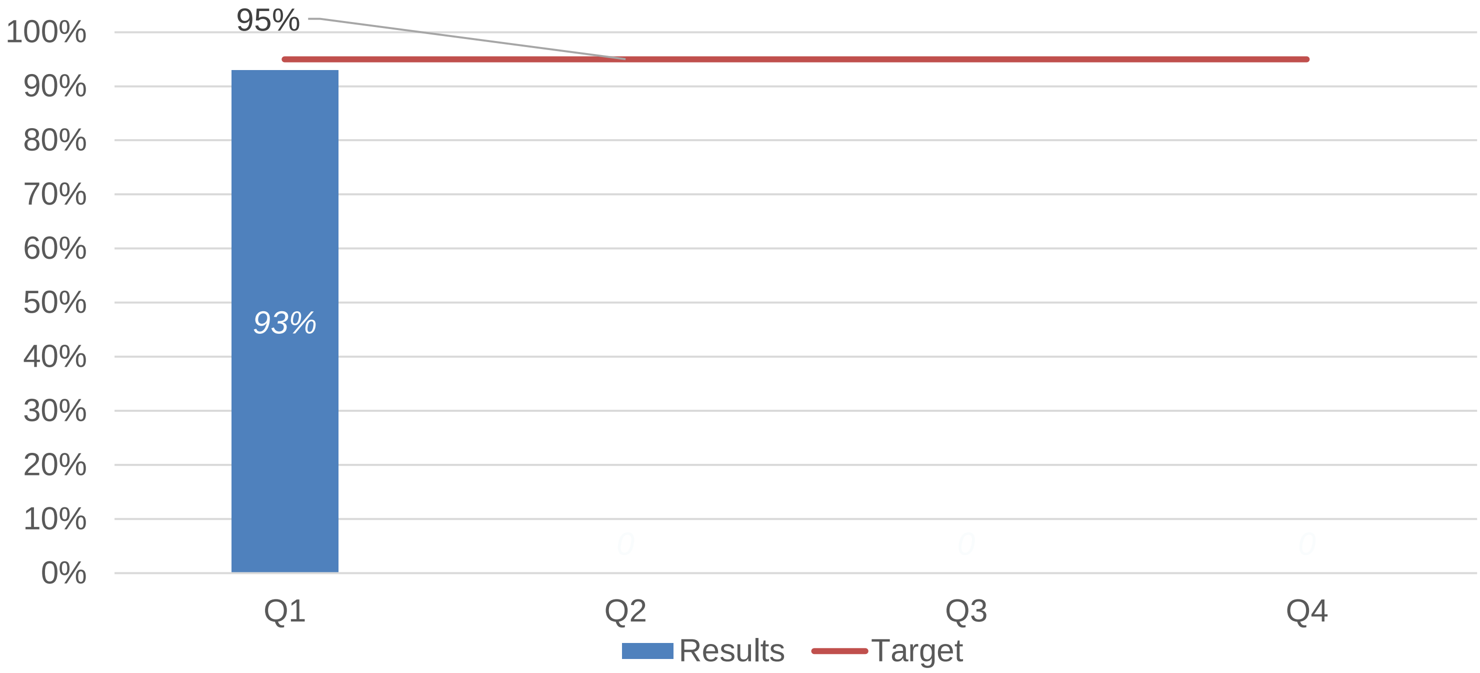
Key indicators



Reporting to begin FY23 Q3. Agencies have until April 3, 2023 - six months after the Binding Operational Directive (BOD 23-1 Asset Visibility) was issued - to initiate the collection and reporting to the CDM Dashboard.

Key indicators

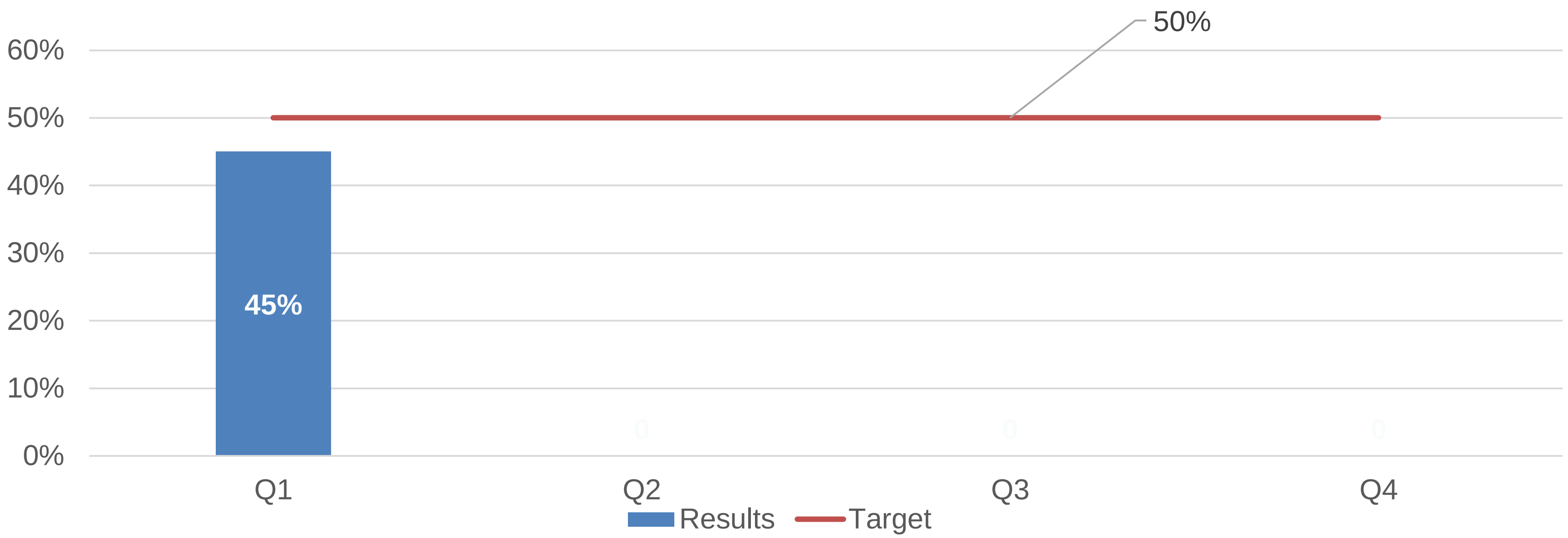
Percent of agencies that have developed internal vulnerability management and patching procedures by the specified timeline



Ninety-four of the 101 Federal Civilian Executive Branch agencies are compliant. Agencies made more progress in Q1 than anticipated - progress in subsequent quarters throughout the year will likely be slower.

Key indicators

Percent of federal agencies who meet BOD-22-01 [Known Exploited Vulnerabilities] automated reporting requirement for leveraging CDM reporting



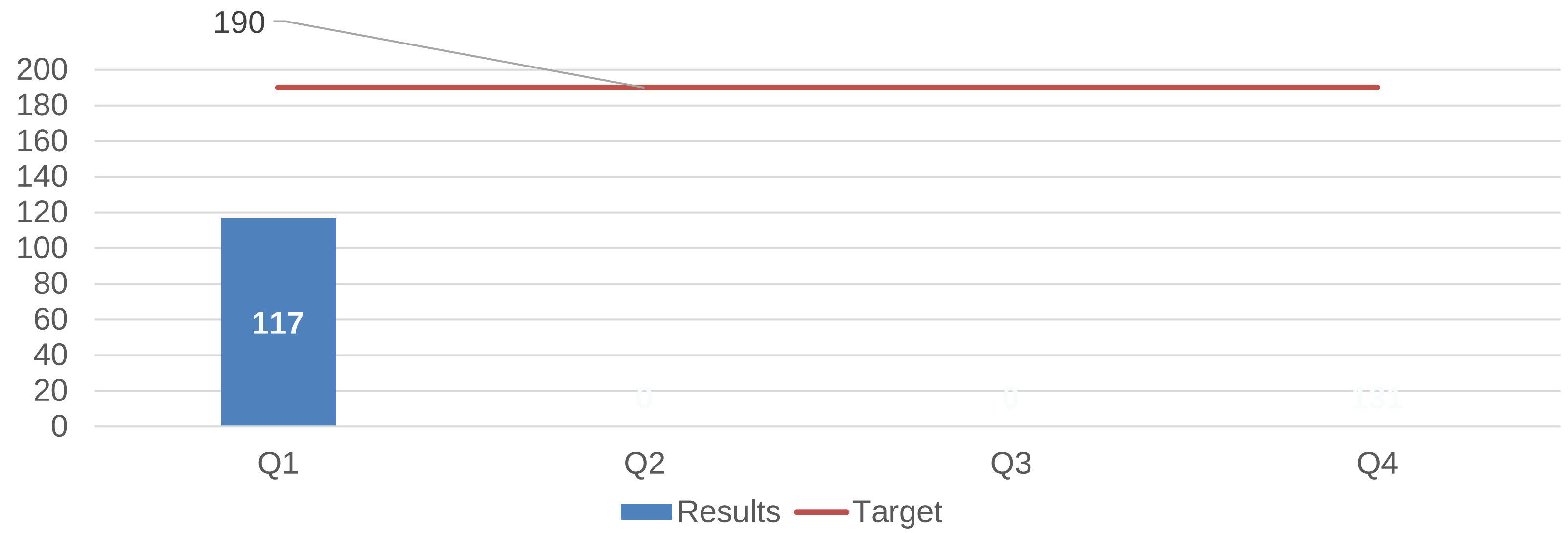
Forty-five of the 101 Federal Civilian Executive Branch agencies met the BOD-22-01 [Known Exploited Vulnerabilities] end of year threshold for automated CDM reporting.

CISA is performing well against this measure, with Q1 results much higher than anticipated. However, we anticipate challenges to both achieving and maintaining comprehensive CDM coverage. Factors outside CDM's control that affect decisions around the maintenance and continuity of scanning tools (e.g., agency resourcing, prioritization, leadership changes, etc.) could impact CDM coverage and visibility in the near and longer term.

Note: This measure takes the place of a retired AWARE score measure. AWARE data quality work is on hold for the immediate future, reprioritized in favor of data quality and automation work (BODS 22-01 & 23-01) as well as asset management baselining efforts.

Key indicators

Number of voluntary adoptions of CISA Cybersecurity Shared Services offerings to federal civilian agencies



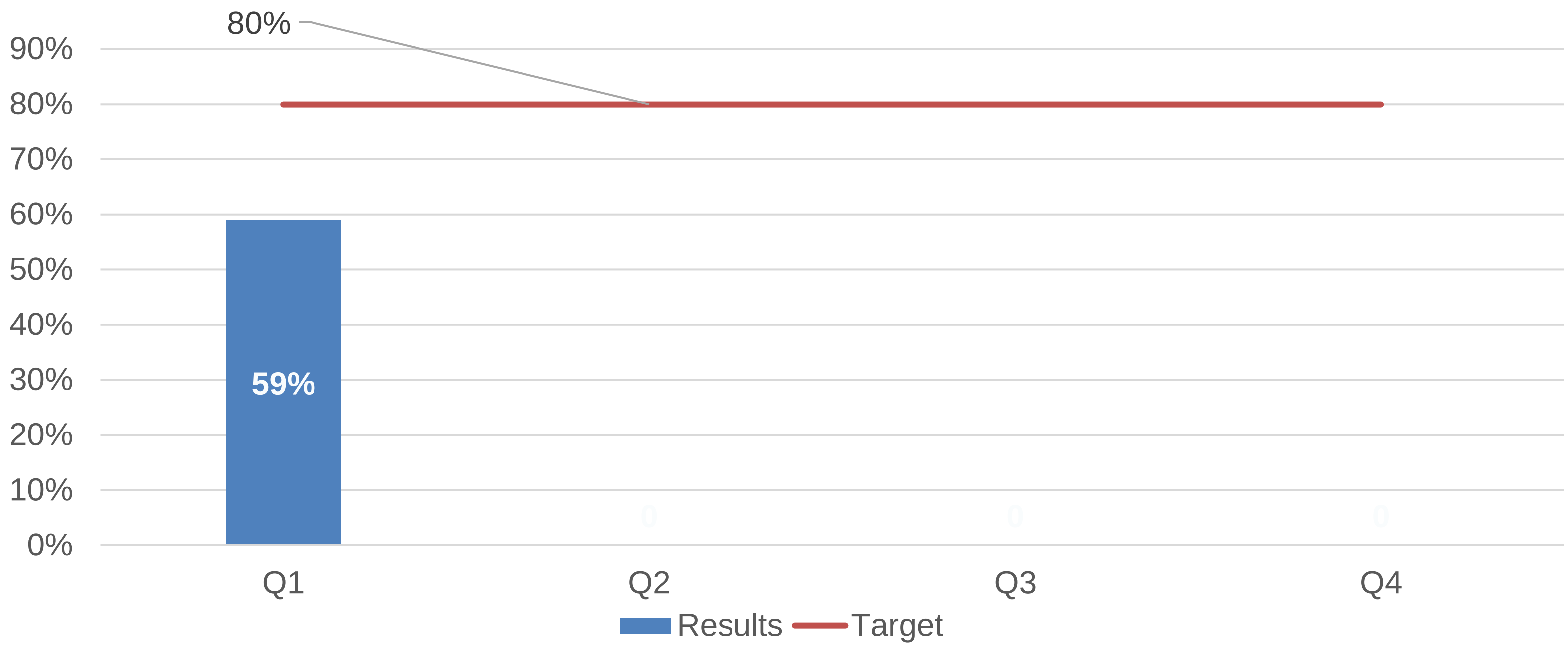
The current service offerings are Automated Indicator Sharing, Mobile Application Vetting, Shared Cybersecurity Services, Traveler-Verified Information Protection, and Vulnerability Disclosure Policy Platform (VDP). The cumulative total of adoptions is 117 with two new adoptions added this quarter from VDP. Twenty-three adoptions were omitted from the baseline with the removal of Protective Domain Name Service Resolver from the voluntary shared services list. As of FY23 Q1, Protective Domain Name Resolver became a mandatory service for the FCEB agencies and no longer meets the definition for inclusion in this measure.

Number of Adoptions:

Automated Indicator Sharing	21
Mobile Application Vetting	10
Shared Cybersecurity Services	54
Traveler-Verified Information Protection	2
Vulnerability Disclosure Policy Platform	30

Key indicators

Percent of endpoints from federal agencies covered by Endpoint Detection and Response solutions that are deployed by Continuous Diagnostics and Mitigation



Of the 908,683 Endpoint Detection and Response (EDR) Requests for Service received, there were 539,865 EDR tools/agents deployed.

This scope of this measure has changed. The measure previously focused on only eight SolarWinds-affected agencies. This measure now covers all agencies with CDM EDR deployments (as of FY23Q1, at ~40).

Key milestones

Milestone Summary				
#	Key Milestone	Milestone Due Date	Milestone Status	Comments
1.1	Conduct program increment planning session to plan the migration of the remaining on-premises analytic capabilities to the Cloud Analytic Environment	Q2	Scheduled	Dates for upcoming program increment planning sessions are scheduled
2.1	100% of agencies with a CDM MOA have deployed the CDM Dashboard and are feeding data to CISA	Q2	On track	This milestone is on track for completion in Q2
2.2	Reach 93% of federal agencies that have developed internal vulnerability management and patching procedures in compliance with CISA-provided scope and timelines	Q3	Complete	Agencies made more progress in Q1 than anticipated, allowing this milestone to be complete ahead of schedule.
2.3	Develop a draft Asset Visibility Capacity Enhancement Guide to signal best practices and assist agencies with implementation of the expected Asset Visibility directive requirements	Q1	Complete	A draft Asset Visibility Enhancement Guide has been completed to signal best practices and assist agencies with implementation of the expected Asset Visibility directive requirements.
3.1	Complete the first wave of EDR deployments (4 CFO Act; 12 non-CFO Act agencies) and initiate the second wave (5 CFO Act; ~25 non-CFO Act agencies)	Q2	On track	This milestone is on track for completion in Q2

Summary of progress

Narrative

Overall, CISA has made progress towards its FY23 targets, and all milestones are scheduled, on track, or complete, with one that was completed ahead of schedule.

Notable accomplishments include:

- *Percent of agencies that have published a vulnerability disclosure policy (VDP) and have all agency internet accessible systems and services covered by their VDP* – the program made a significant jump from 77% in FY22 Q4 to 85% in FY23 Q1.
- *Percent of agencies that have developed internal vulnerability management and patching procedures in compliance with CISA provided scope and timelines* - agencies made more progress than anticipated and are ahead of schedule
- *Percent of Federal Civilian Executive Branch Agency Domain Name System egress traffic bypassing CISA's Domain Name System filtering capabilities* - decreased significantly since FY22 Q4, from 81% to 51% due to the increase in adoption of protective DNS by FCEB agencies.