



Agency Priority Goal | Action Plan | FY 23 – Q4

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- Outdated and legacy technology poses risk of increased vulnerabilities associated with weak authentication exposure and unpatched software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

Goal Strategies

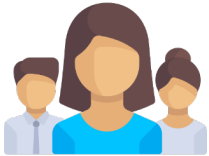
Strategy 1: Lead Cyber Defense Operations

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.



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.

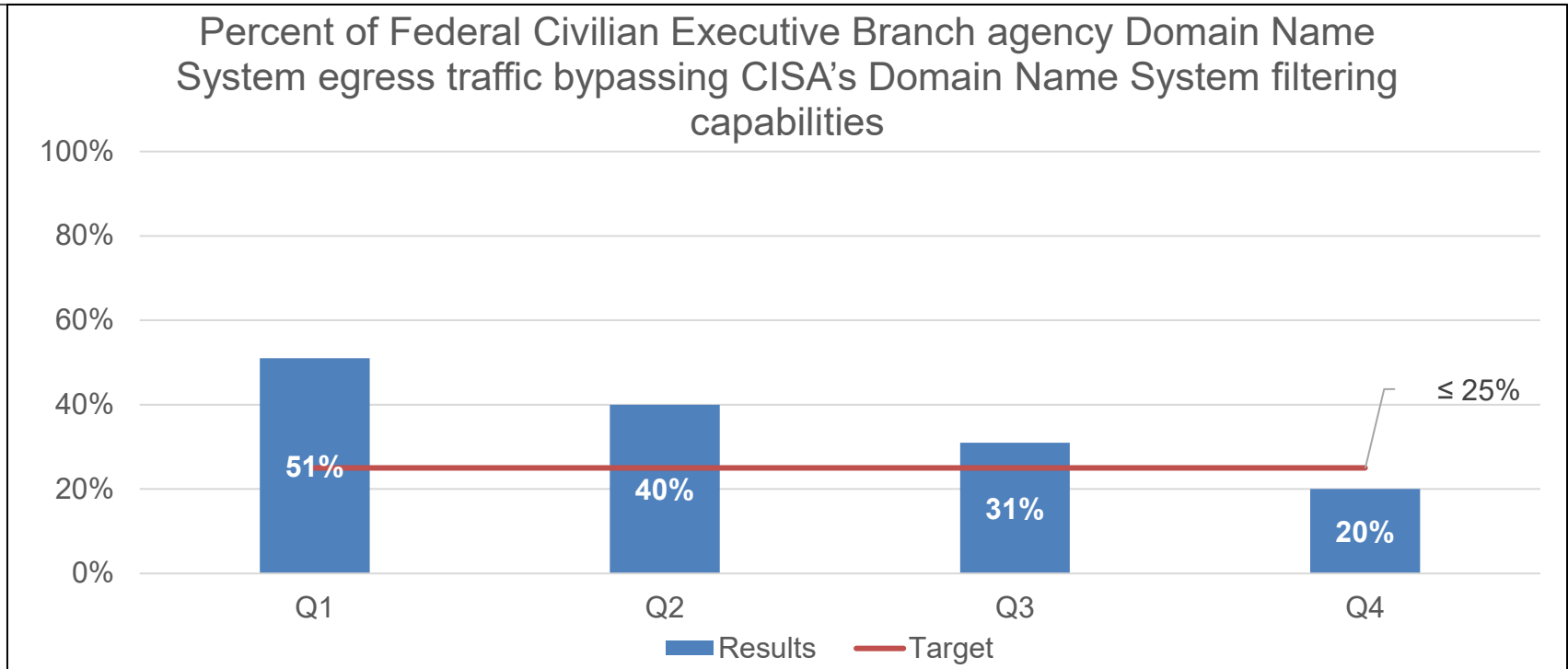
Please update this column each quarter.

Achievement statement Repeat the achievement statement from the goal statement on the previous slide		Key indicator(s) A “key performance indicator” measures progress toward a goal target	Quantify progress These values enable us (and you!) to calculate % complete for <u>any</u> type of target*			Frequency 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 Federal Civilian Executive Branches by improving asset discovery and vulnerability enumeration.	Percent of federal agencies who meet Binding Operational Directive-22-01 [Known Exploited Vulnerabilities] automated reporting requirement for leveraging CDM reporting	50%		84%	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”

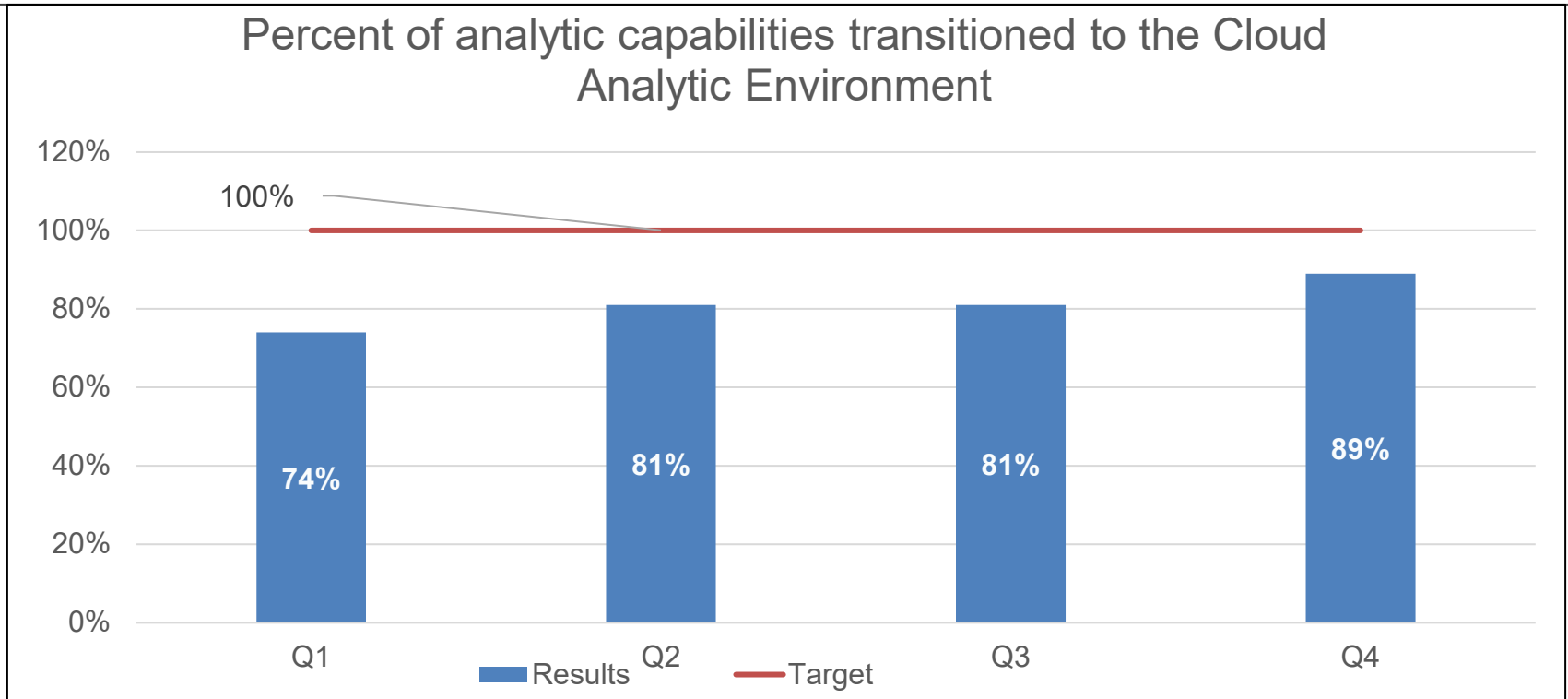
** As of 10/1/2021

Key Indicators



The Q4 result is 20%. CISA analysts identified an increase to our DNS bypass traffic as an unintended consequence from a one-time outlier from an agency's Q4 data. Given the specific circumstances, the Q4 calculation was adjusted to exclude that one-time outlier data.

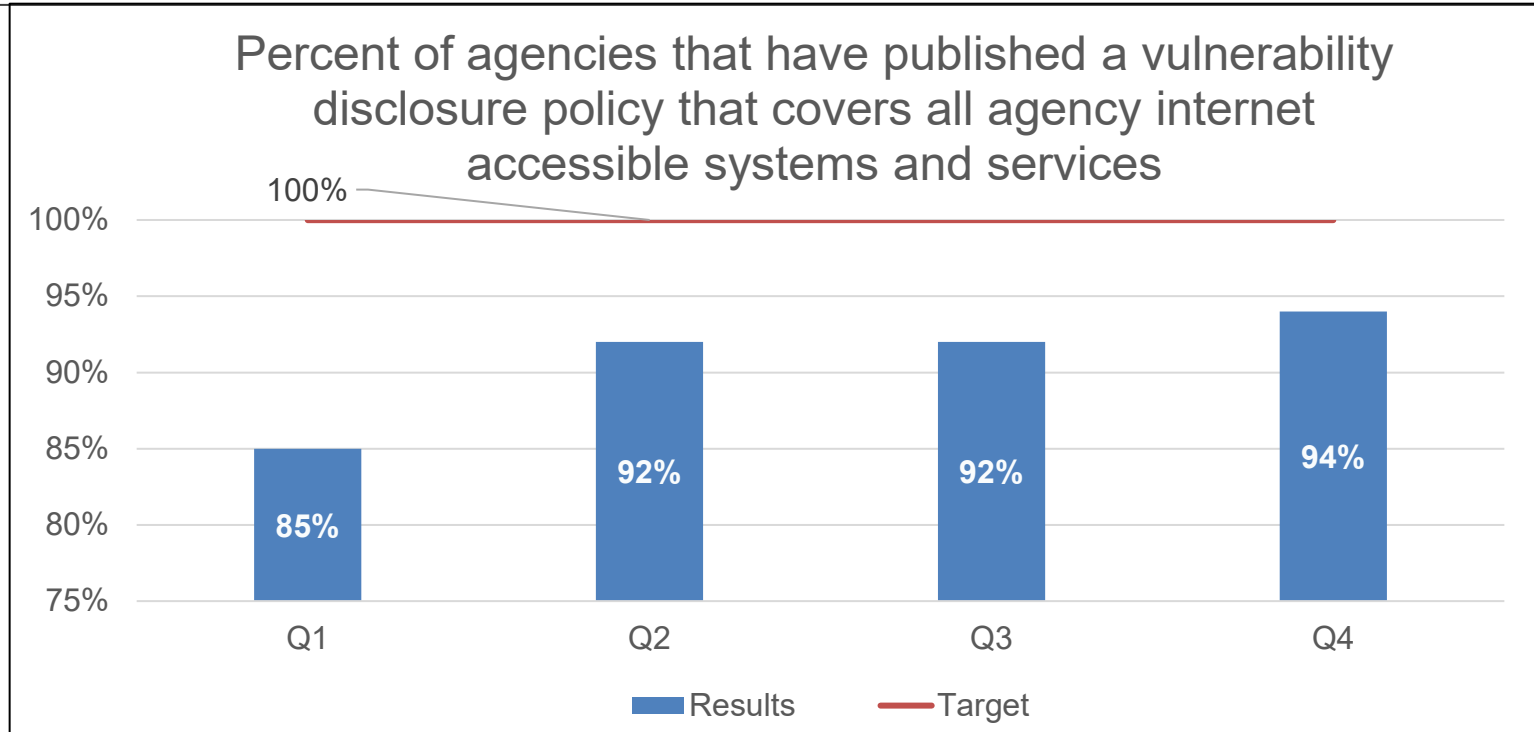
Key Indicators



24 of 27 tools have completed migration to the Cloud Analytic Environment (88.8%). Three tools are pending. One tool is at 99% completion with only one small data store that is currently in progress. Threat Intelligence Platform and Indicator data are also in progress and near completion; however, resources were diverted to other tasks for the remainder of this program increment.

Corrective Action: Work is expected to be completed in Q1 FY24, as a new program increment is in progress.

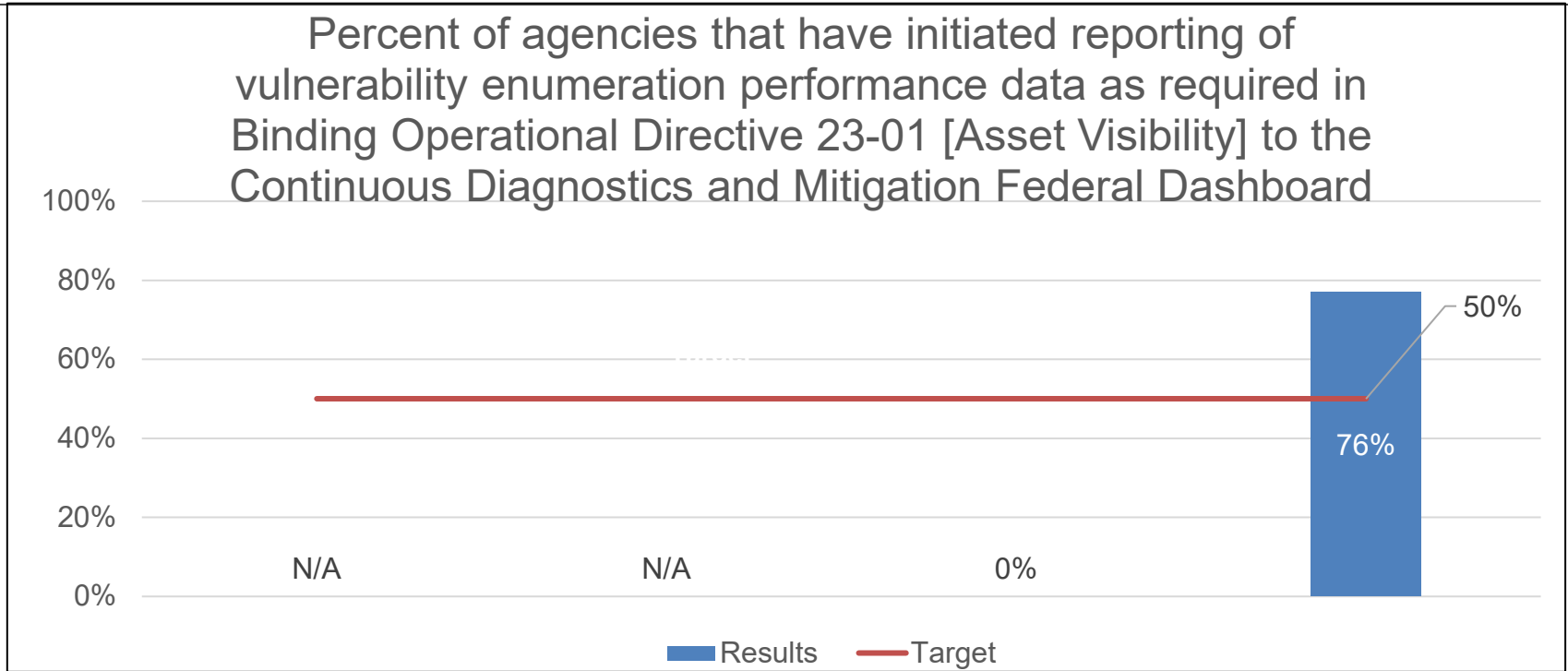
Key Indicators



Overall, for FY23, the result of 94% represents a high level of compliance and strong performance. The 100% target was submitted at the beginning of FY23. Based on lessons learned from this year's reporting cycle, CISA has identified an internal target of 95% as a more realistic benchmark for high compliance and will track against that target internally moving forward.

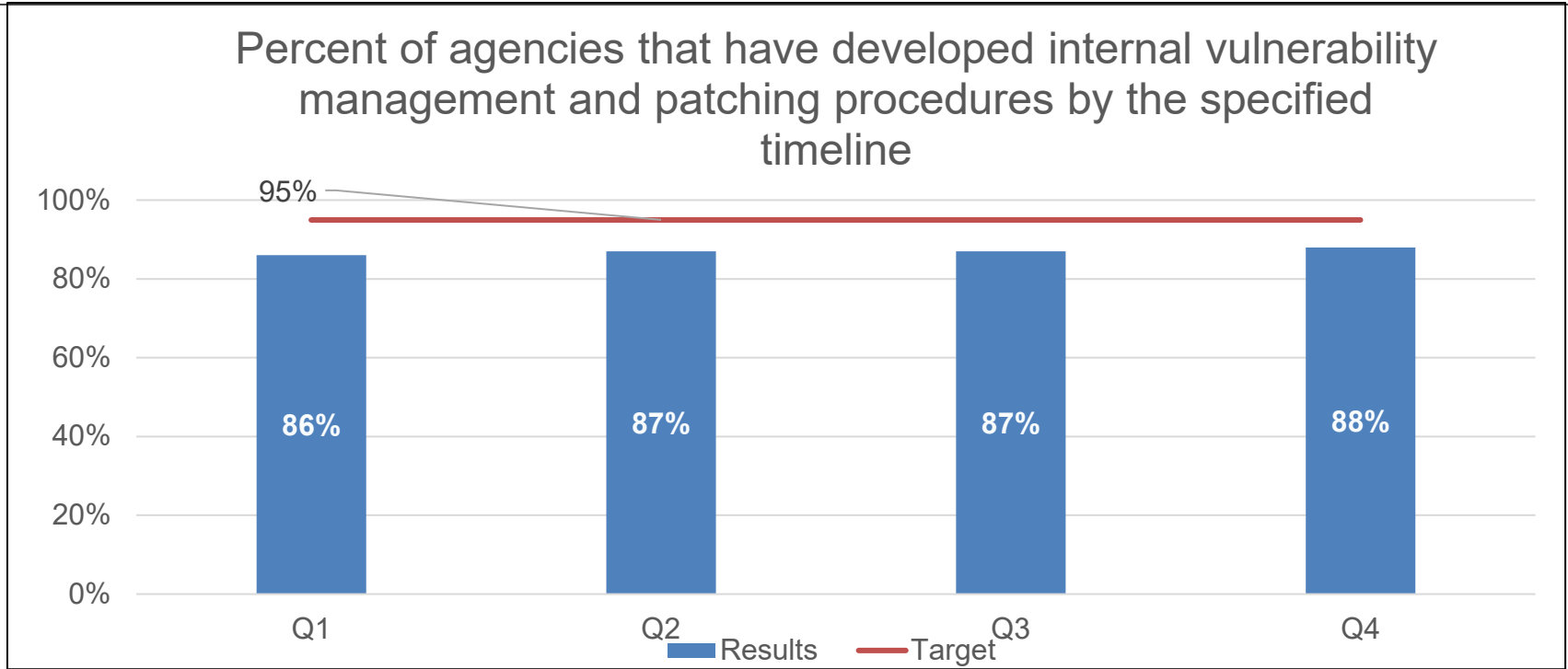
Corrective Action: There is a recurring challenge bringing the last ~10% of FCEB Agencies into compliance, consistently with the same very small set of non-CFO Act agencies. The program identified limited actions to close the gap and acknowledged the need to prioritize resources in line with the risk posture and operational priorities.

Key Indicators



71 out of 93 agencies are compliant, or 76% of the participating agencies. CISA is outperforming expectations for this measure, with Q4 results much higher than anticipated. However, we anticipate that factors like agency resourcing, prioritization and leadership changes will create challenges for achieving comprehensive CDM coverage. We foresee stabilized performance in FY24.

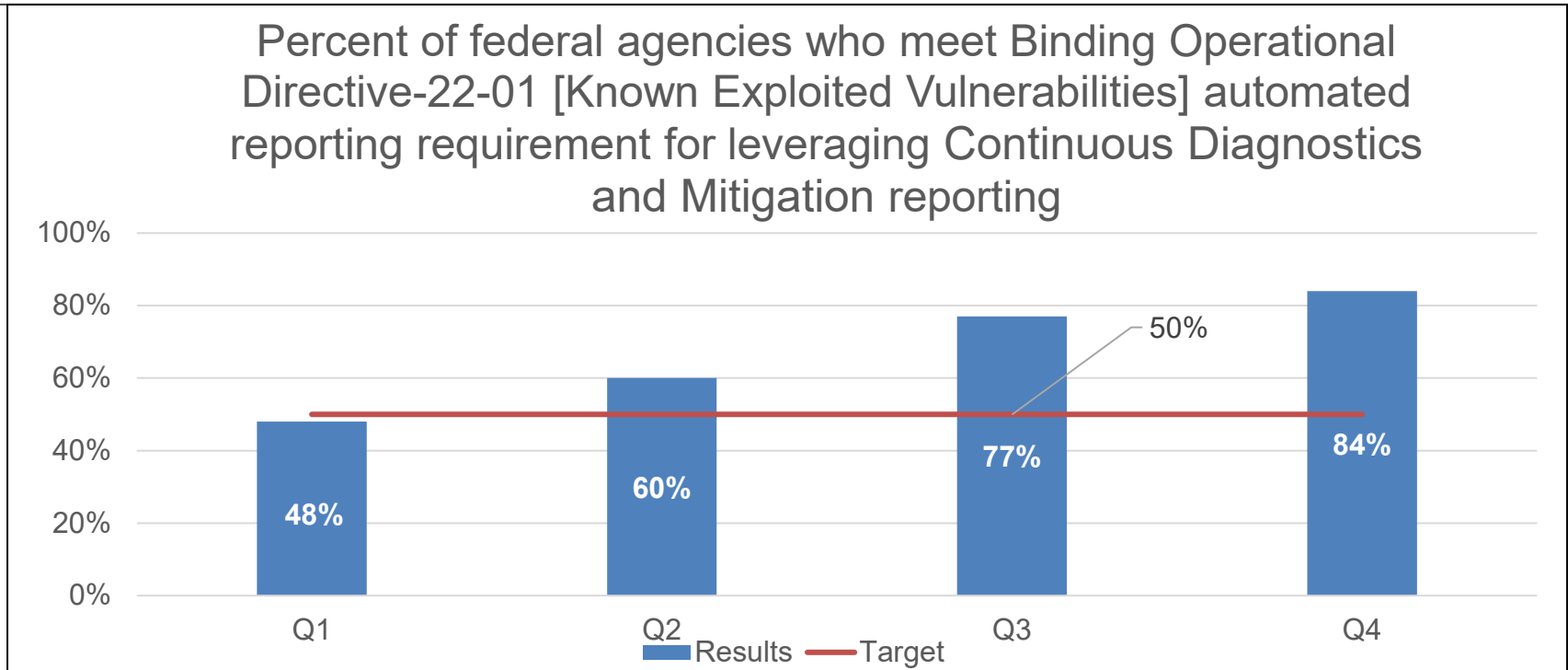
Key Indicators



As of FY23 Q4 reporting, 88% of FCEB agencies are in compliance (89/101). Although we expected to hit the target of 95% by the end of Q4, lack of responsiveness by agencies prevented us from achieving this goal. The Non-CFO Act agencies in question consistently struggle with responsiveness and/or implementation of Cyber Directives requirements; however, they continue to show overall improvement in their cybersecurity risk posture.

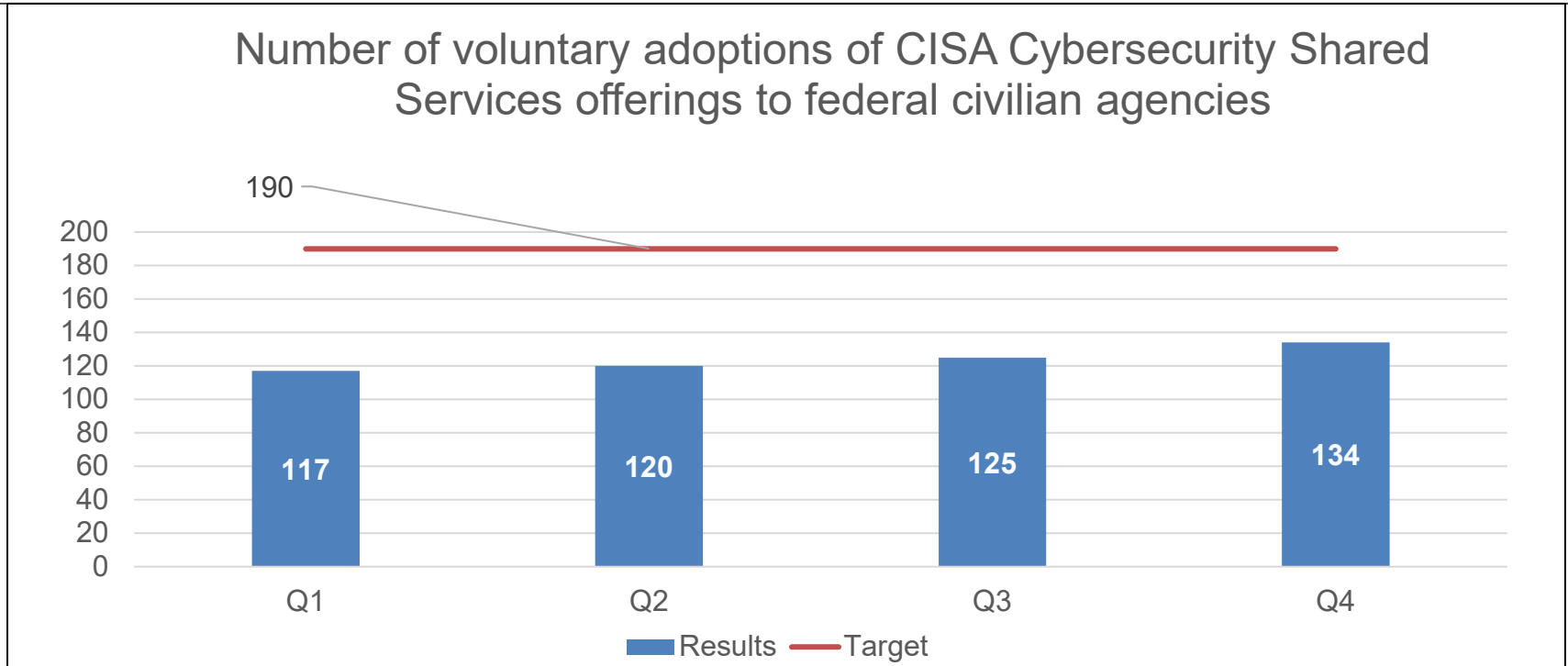
Corrective Action: CISA continues to work with each of these agencies individually to drive compliance with this requirement and to hit the desired goals. This target is expected to be reached by FY24 Q4.

Key Indicators



As of Q4, 78 of 93 reporting agencies met the BOD's automated reporting requirement, well exceeding the annual target. Note that the denominator was changed to include the 93 out of the total 101 FCEB agencies enrolled in CDM; reporting for all quarters were adjusted accordingly.

Key Indicators

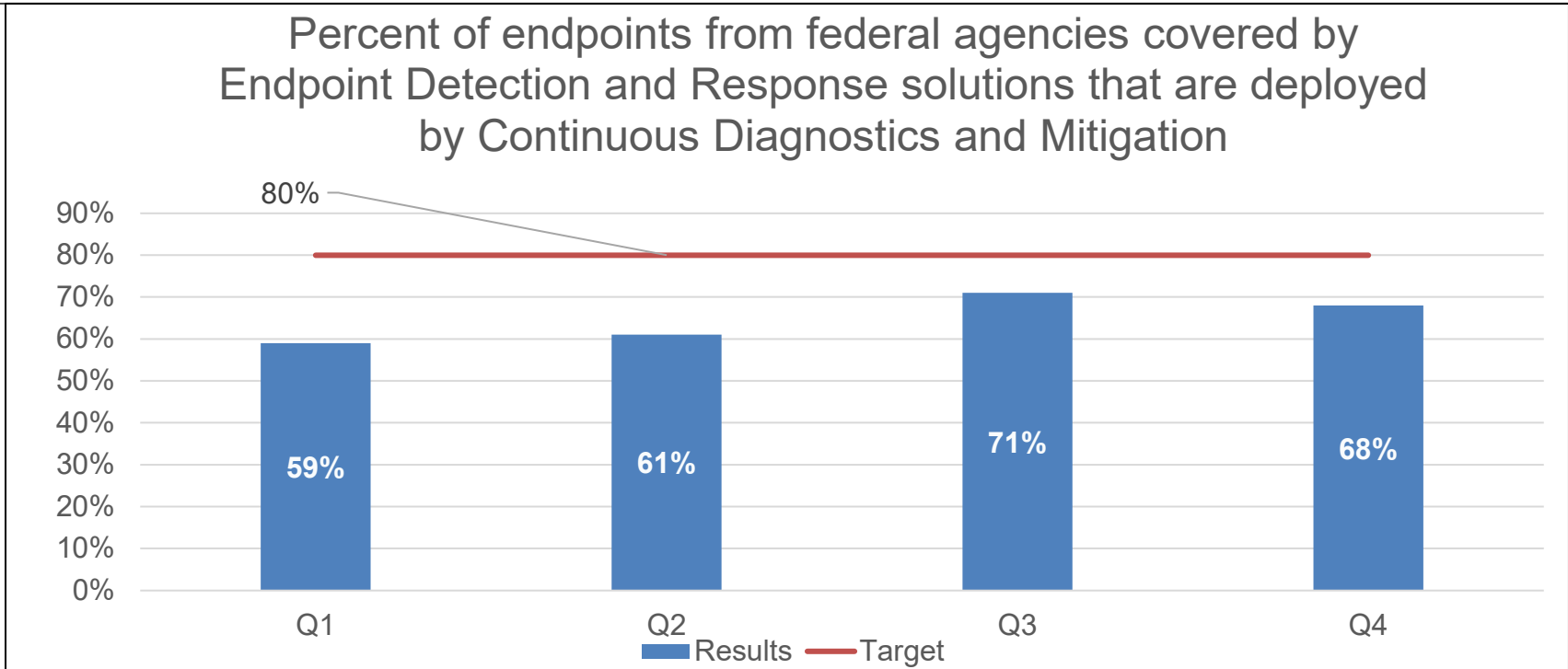


The annual target was projected with the expectation that a new service would become available this fiscal year. As this did not occur, we fell short of our annual goal for this measure.

Automated Indicator Sharing 22
Mobile Application Vetting 18 (+8)
Shared Cybersecurity Services 54
Traveler-Verified Information Protection 4 (+1)
Vulnerability Disclosure Policy Platform 32
Secure Cloud Business Application 4

Corrective Action: The program will change the approach to setting this annual target so that the projection is more stable, only including current services and excluding services that are still under development. Otherwise, achievement of the target is very dependent on external factors.

Key Indicators



Of the 1,211,866 EDR Requests For Service (RFS) received by the end of FY23, 826,815 EDR agents were deployed. It should be noted that the number of endpoints in scope (the denominator) increased throughout FY23 as CDM worked with agencies to identify gaps, which explains the drop in percentage between Q3 and Q4. Had we used a fixed value for our denominator, we would have reported an FY23 result of 89.1% (826,815 EDR agents deployed as of 9/30/23 / 927,600 endpoints in scope as of 10/1/2022).

Corrective Action: Going forward, the program will track progress against a fixed value of the known EDR gap as of a certain date (e.g., 1,211,866 as of 10/1/2023). The program will still track and address any new gaps identified using its standard intake process.

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	Complete	Mission Engineering conducted Program Increment Planning for Quarter 2 (PI 23.2) January 23-January 27, 2023. The PI 23.2 Release Planning Review was successfully conducted on Wednesday, 1 February 2023. The next program increment planning session is scheduled for April 24 - April 28, 2023 for Quarter 3.
2.1	100% of agencies with a CDM Memorandum of Agreement (MOA) have deployed the CDM Dashboard and are feeding data to CISA	Q2	Complete	93/93 MOA agencies have deployed the CDM Dashboard and are feeding data to CISA. These include the 64 (of 74 total) DEFEND-F agencies that have MOAs with CDM. CDM plans to continue its efforts (currently approximately 18 months long) to make contact with the remaining ten DEFEND-F agencies.
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.

Key Milestones

Milestone Summary				
#	Key Milestone	Milestone Due Date	Milestone Status	Comments
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	Complete	This milestone was completed on schedule. As of Q2, CISA has completed the first wave of deployments with four CFO Act Agencies (SBA, SSA, HUD, and DHS) and 23 non-CFO Act agencies. There are nine CFO Act Agencies currently in deployment with CISA. They include (DOC, DOE, DOJ, DOL, Education, HHS, NASA, Treasury, and USAID). CISA is also in the process of deploying to six additional non-CFO Act agencies.

Narrative

CISA met its overall goal and target for the year. Three measures met their target and all milestones have been completed. Notable accomplishments include:

- Key measure, Percent of federal agencies who meet BOD-22-01 [Known Exploited Vulnerabilities (KEVS)] automated reporting requirement for leveraging CDM reporting, met its target ahead of schedule, with results much higher than anticipated, exceeding the target by 34% (84%, with target of 50%)
- Percent of agencies that have initiated reporting of vulnerability enumeration performance data as required in BOD 23-01 [Asset Visibility] to the CDM Federal Dashboard hadn't reported in previous quarters but exceeded its target by 27% (77%, with target of 50%)
- Percent of Federal Civilian Executive Branch Agency Domain Name System egress traffic bypassing CISA's Domain Name System filtering capabilities. The result continued to decrease from 30% in Q3 to 20% in Q4, meeting its annual target.

The remaining five measures did not meet their targets for various reasons:

- Unexpected shifts in resources and/or schedule delays affected anticipated progress towards targets
- External agencies non-compliance and reporting, which CISA has no control over
- Unanticipated increases in demand for CISA services resulting in scope expansion

Corrective Actions:

For those measures that did not meet the annual target, some have schedule slippages and the FY23 targets are expected to be met in early FY24; others will require limiting external factors and prioritizing resources in line with the risk posture to set a more realistic target in the future. In addition, CISA will continue to work with each of these agencies individually to drive compliance and more effective communication of the requirements to hit the desired goals in FY24.