Agency Priority Goal | Action Plan | FY 23 – Q3

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- Outdated and legacy technology poses risk of increased vulnerabilities associated with weak authentication exposure and unpatched software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 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 any 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%		77%	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

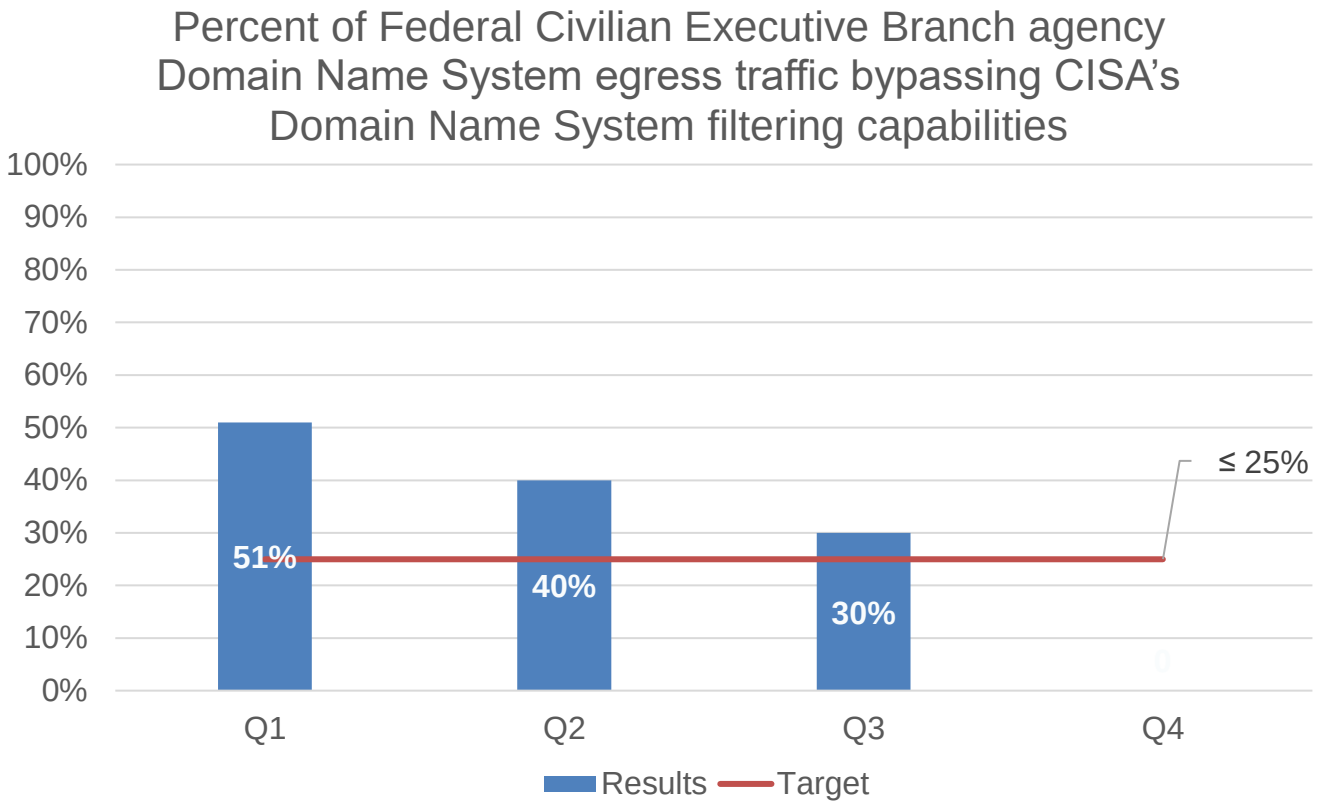
Provide Tools and Services

- 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.

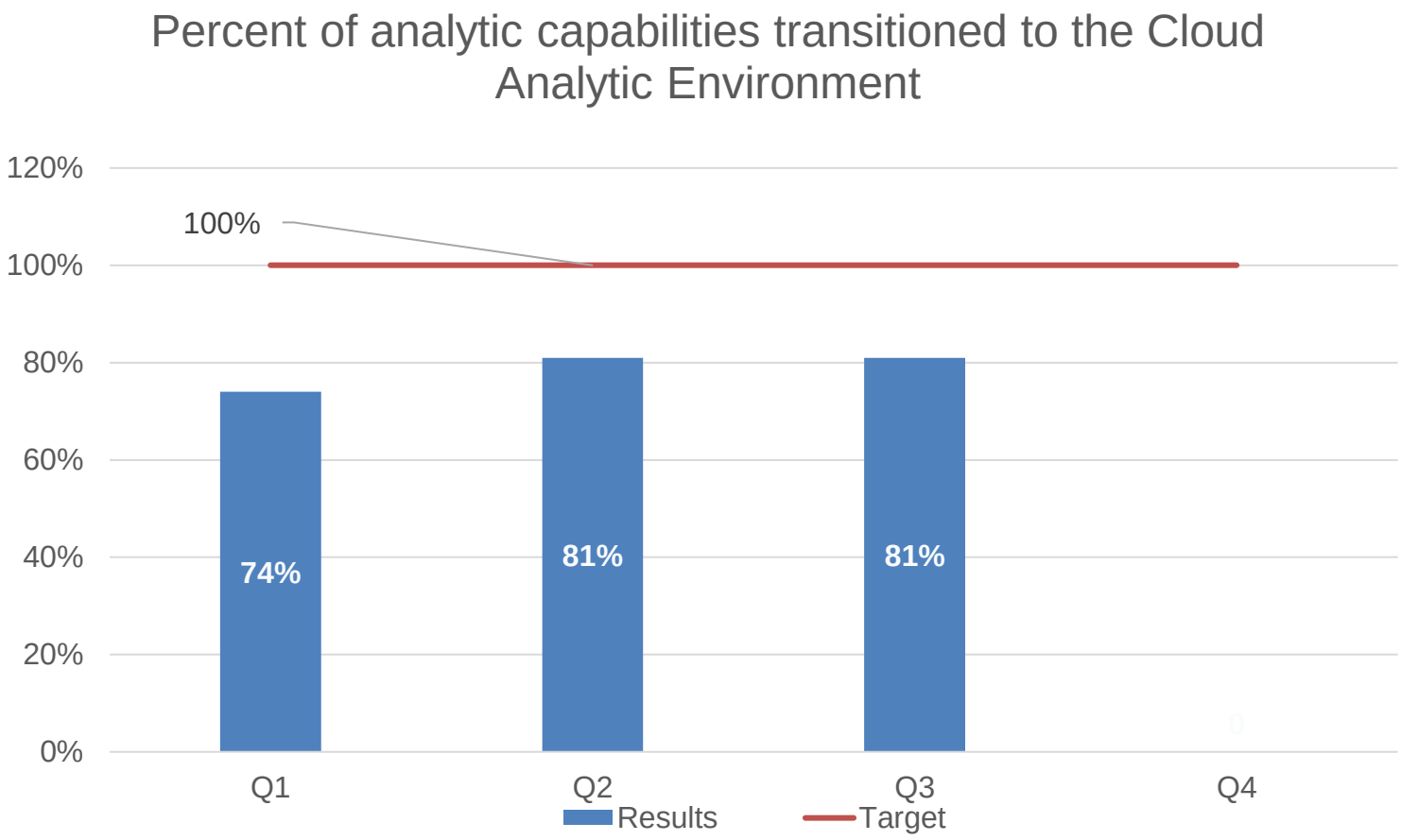
Key indicators



The percent of Federal Civilian Executive Branch Agency Domain Name System egress traffic bypassing CISA's Domain Name System filtering capabilities continues to decrease.

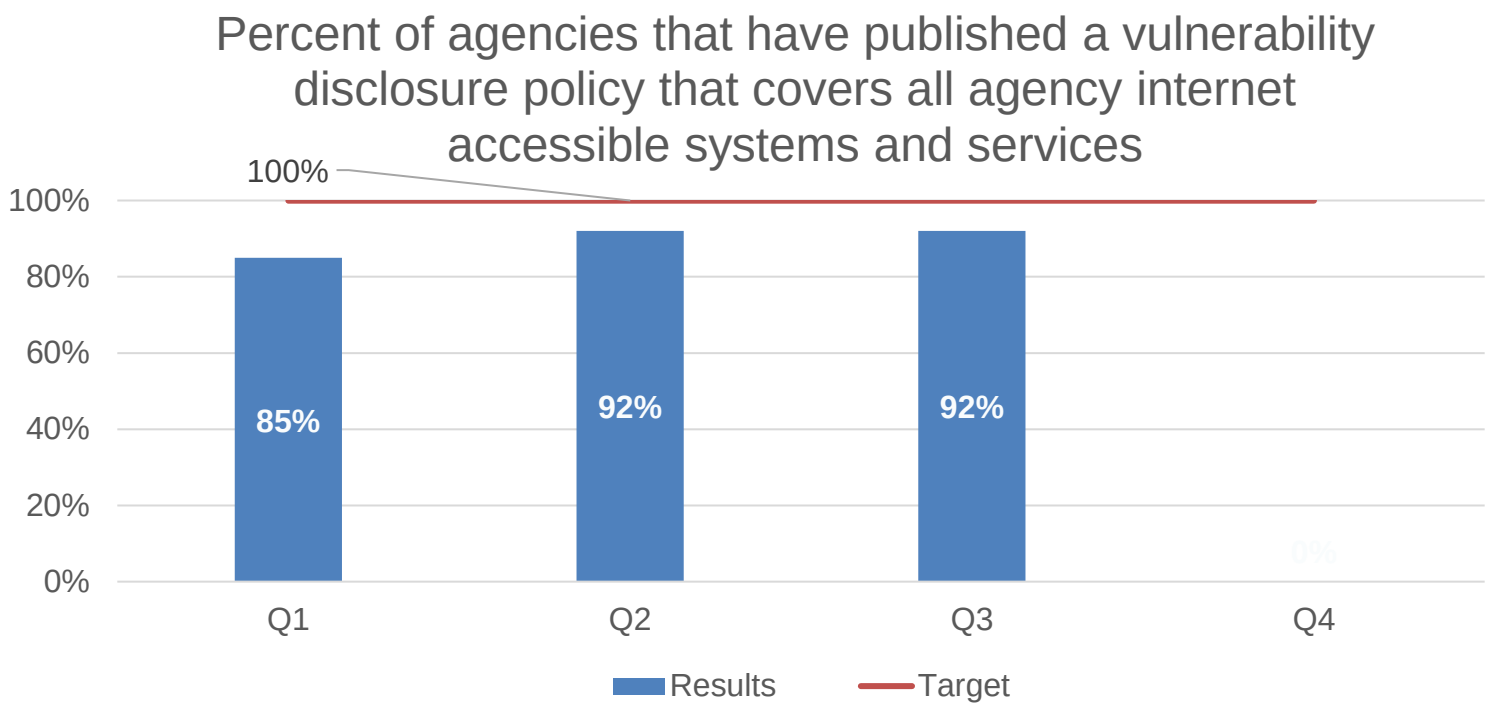
Bypass Packets: 7,655,346,616 / Total DNS packets 2,5167,150,986 = .30 (30%)

Key indicators



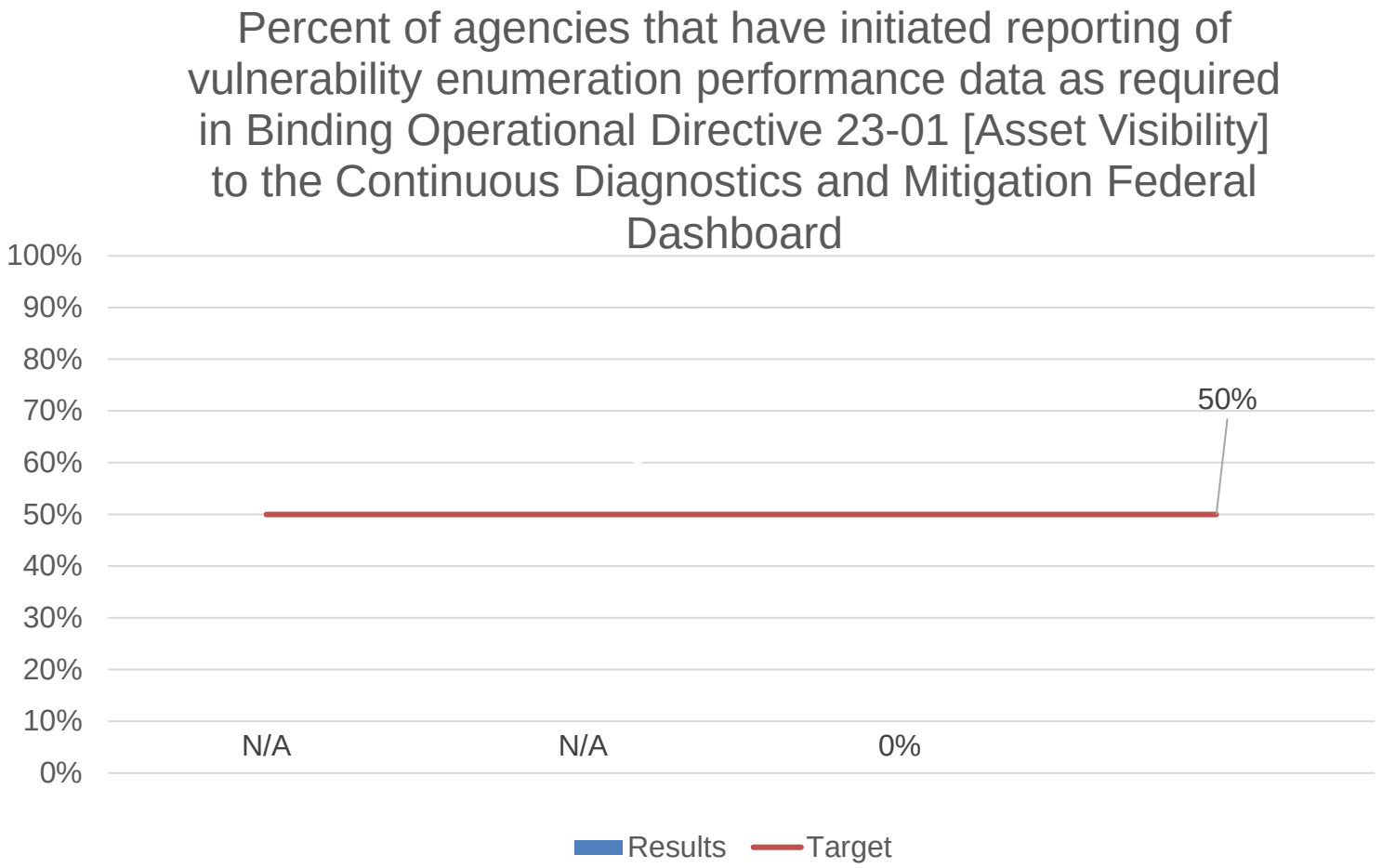
22 of 27 tools have completed migration to the Cloud Analytic Environment (81%). Four tools are on track to complete the migration in this program increment (by 21 July 2023). At that point, 26 of 27 tools will have completed migration (96%). The last tool is scheduled for migration in the next program increment.

Key indicators



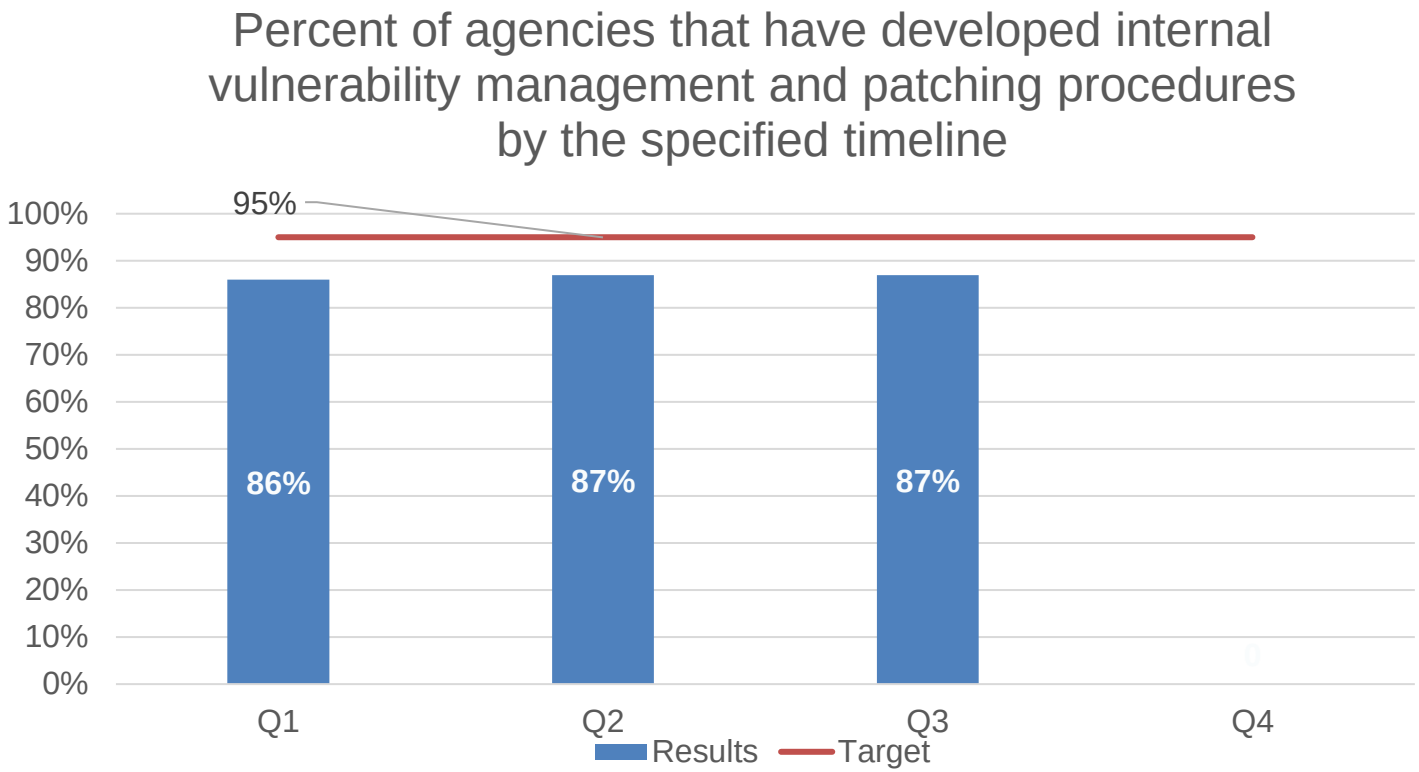
Currently 100% of agencies have published a VDP, and 92% of agencies have a VDP with all internet accessible systems in scope (93 out of 101 FCEB). The goal for overall adoption is 95%, which equates to one additional agency adoption from the 92% reported in Q2/Q3. CISA expects to hit the goal of 95% by Q4.

Key indicators



The window to begin reporting began in Q3. The Federal Dashboard has an ES6 upgrade currently underway explaining the 0% reporting for Q3. CDM team anticipates 60-70% of agencies to report by end of Q4, likely surpassing the target goal of 50%.

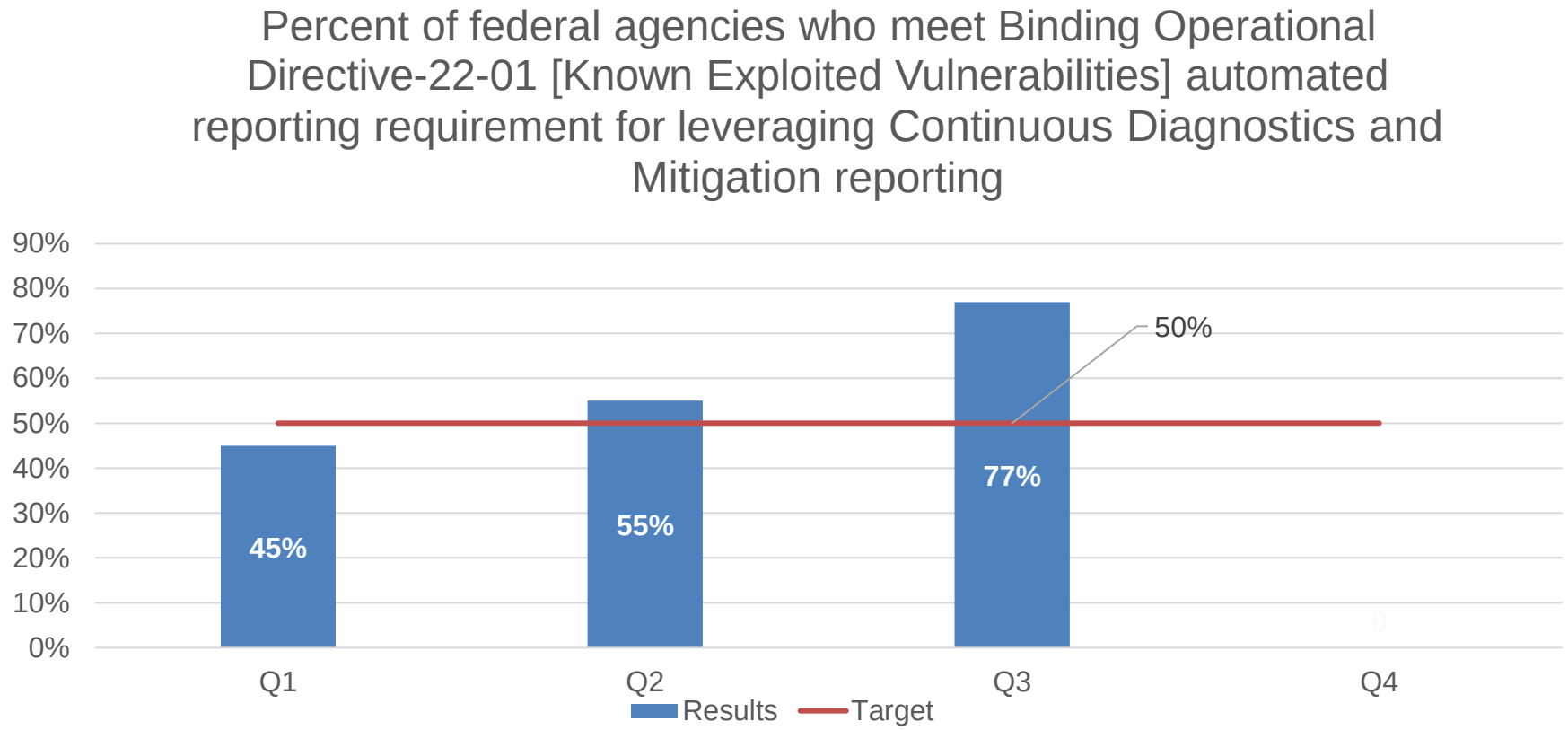
Key indicators



Previous reporting omitted the 5 agencies that had not leveraged our reporting platform. After a comprehensive scrub of cyberscope, this number did drop slightly as we onboarded a few other agencies to cyberscope which had previously not reported. While this number appears to have dropped, the numerator has held steady and we expect to make the target goal of 95% by the end of Q4 by working to prioritize outreach efforts for the remaining agencies.

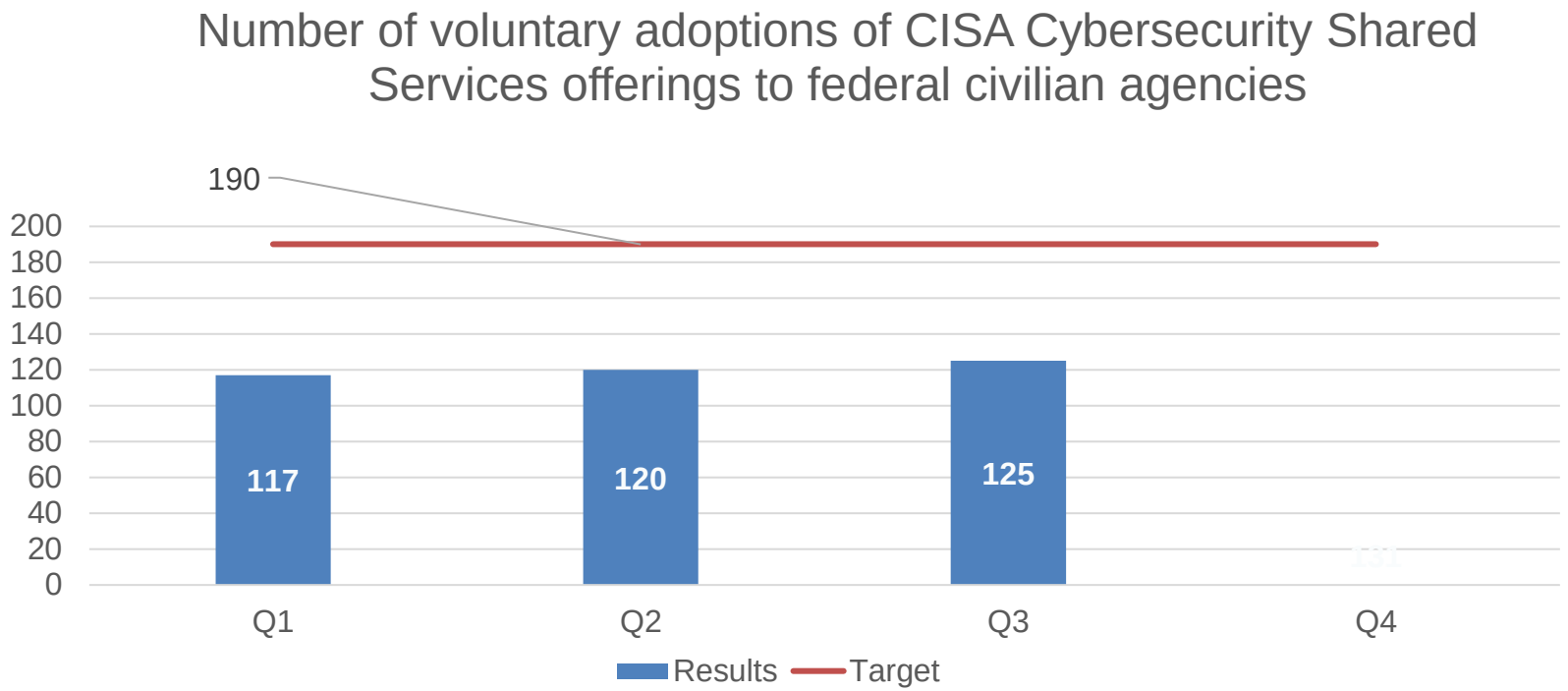
A total of 13 agencies have not reported in CyberScope: Armed Forces Retirement Home (AFRH), Consumer Product Safety Commission (CPSC), Occupational Safety and Health Review Commission (OSHRC), Office of Navajo and Hopi Indian Relocation (ONHIR), Presidio Trust (PT), Commission of Fine Arts (CFA), Chemical Safety Board (CSB), Harry S Truman Scholarship Foundation (HTSF), James Madison Memorial Fellowship Foundation (JMMFF), Office of Special Counsel (OSC), United States Interagency Council on Homelessness (USICH), Federal Communications Commission (FCC), Farm Credit System Insurance Corporation (FCSIC)

Key indicators



72 of the 93 reporting agencies exceeded met the reporting requirement. The denominator changed because only 93 out of the total 101 FCEB agencies are enrolled in CDM.

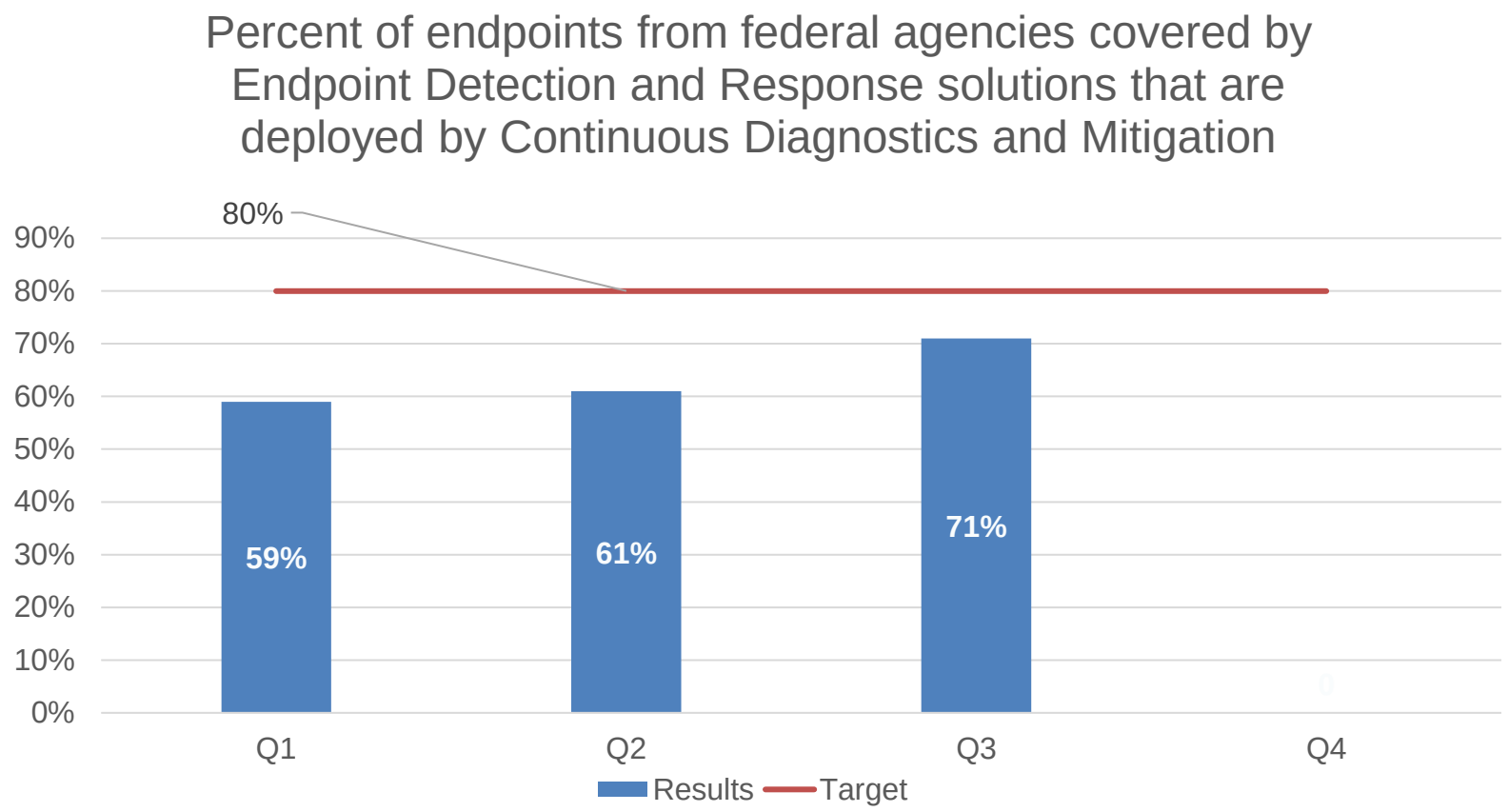
Key indicators



Annual target was projected with the assumption of a new service will be available this fiscal year (e.g. Enterprise Email Security) and the continued momentum of customer interest on operational services. New service will not be available this fiscal year due to requirement changes. Many new customers are different echelons from the same department or agency. Current projected target: 130 for Q4

Number of Adoptions (+5):
Automated Indicator Sharing 22
Mobile Application Vetting 10
Shared Cybersecurity Services 54
Traveler-Verified Information Protection 3
Vulnerability Disclosure Policy Platform 32
Secure Cloud Business Application 4

Key indicators



Based on 747,171 EDR agents deployed of 1,055,384 EDR Requests For Service (RFS) scope received. Although in Q3 we are at 71% of annual target in Q4 we are unlikely to meet the overall goal of 80% at participating agencies, due to the variance created by adding a few new agencies to the Gap-fill scope that have not yet begun to deploy or have just started deploying EDR tools.

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

Overall, CISA has made substantial progress towards its FY23 targets. One measure already met its 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.
- The percent of Federal Civilian Executive Branch Agency Domain Name System egress traffic bypassing CISA's Domain Name System filtering capabilities has continued to decrease, from 40% in Q2 to 30% in Q3 due to the increase in adoption of protective DNS by FCEB agencies.

Measures that are likely to not meet target:

- Percent of endpoints from federal agencies covered by Endpoint Detection and Response (EDR) solution(s) deployed by CDM: This measure is unlikely to meet its target for FY23 due to the variance created by adding a few new agencies to the Gap-fill scope that have not yet begun to deploy or have just started deploying EDR tools.
- Number of voluntary adoptions of CISA Cybersecurity Shared Services offerings by FCEB agencies: The annual target was projected with the assumption that a new service would be available this fiscal year (e.g. Enterprise Email Security). The new service will not be available this fiscal year due to requirement changes.

As the APG sunsets at the end of FY23, CISA is planning to update its GPRAMA measures on cybersecurity for FY24 to include several APG measures (and others) that will continue to provide a comprehensive set of cybersecurity-focused measures to track the agency's progress and outcomes. CISA already conducts a quarterly review of all of its GPRAMA measures and internal measures, including cybersecurity measures, which provides additional assessment and oversight of performance results.