Agency Priority Goal | Action Plan | FY 22 – 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, 90% of the agencies that have reached data preparation quality readiness, will achieve an acceptable data quality level to support reliable risk scoring reported on the Federal Dashboard to gauge the strength of the federal enterprise cybersecurity posture.

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- Outdated and legacy technology poses risk of increased vulnerabilities associated with weak authentication exposure and unpatched software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 an acceptable data quality level to support reliable risk scoring reported on the Federal Dashboard to gauge the strength of the federal enterprise cybersecurity posture	Percent of agencies for which a CDM dataset, measured to be at the established acceptable quality target and supporting the Agency-Wide Adaptive Risk Enumeration (AWARE) score, can be provided for assets reporting to the federal dashboard	90%	50%	50%	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

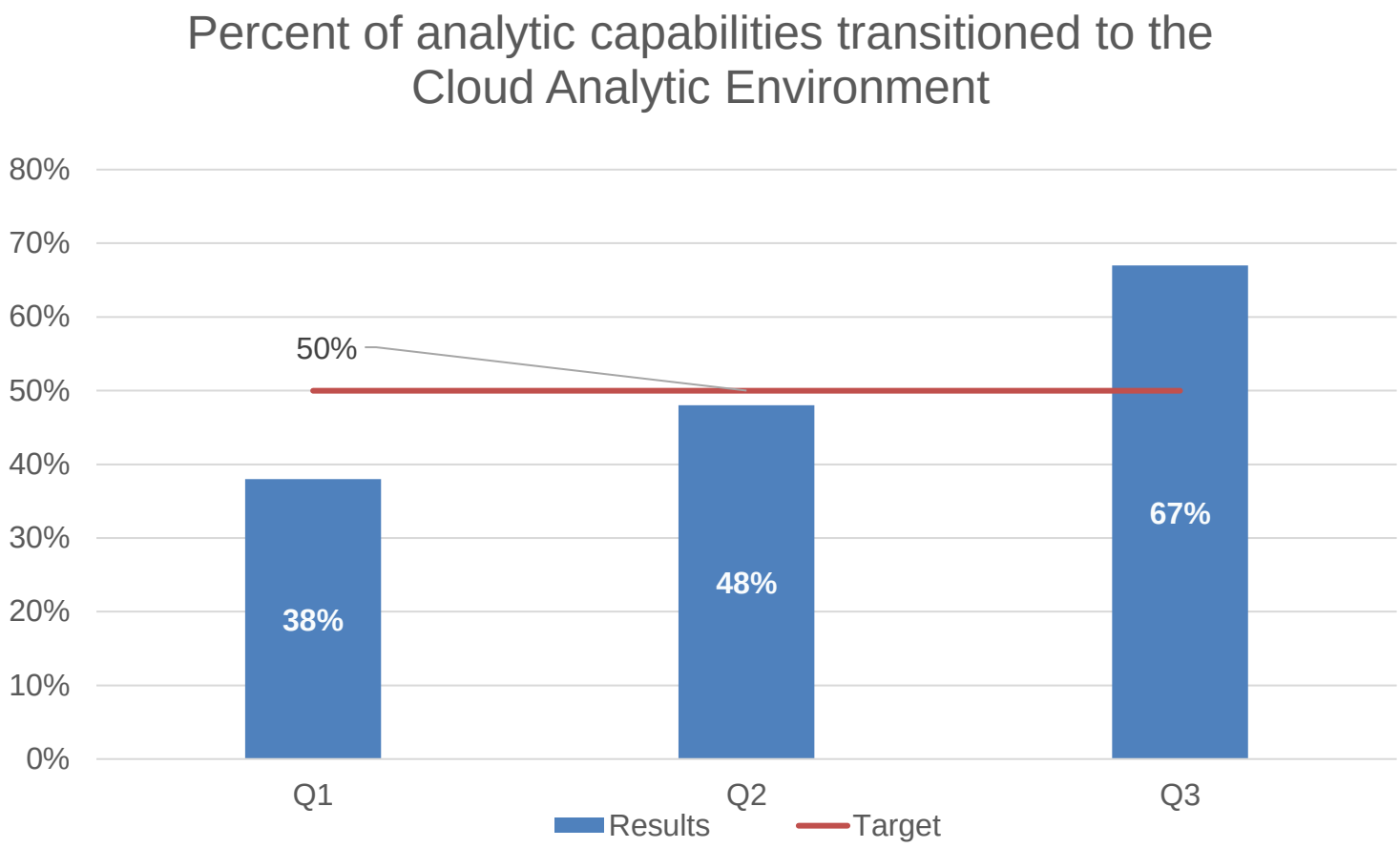
Provide Tools and Services

- Offer cybersecurity tools and services to FCEB agencies to assist them in achieving efficiencies, affordability, and standardization and quickly develops, deploys, and scales 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

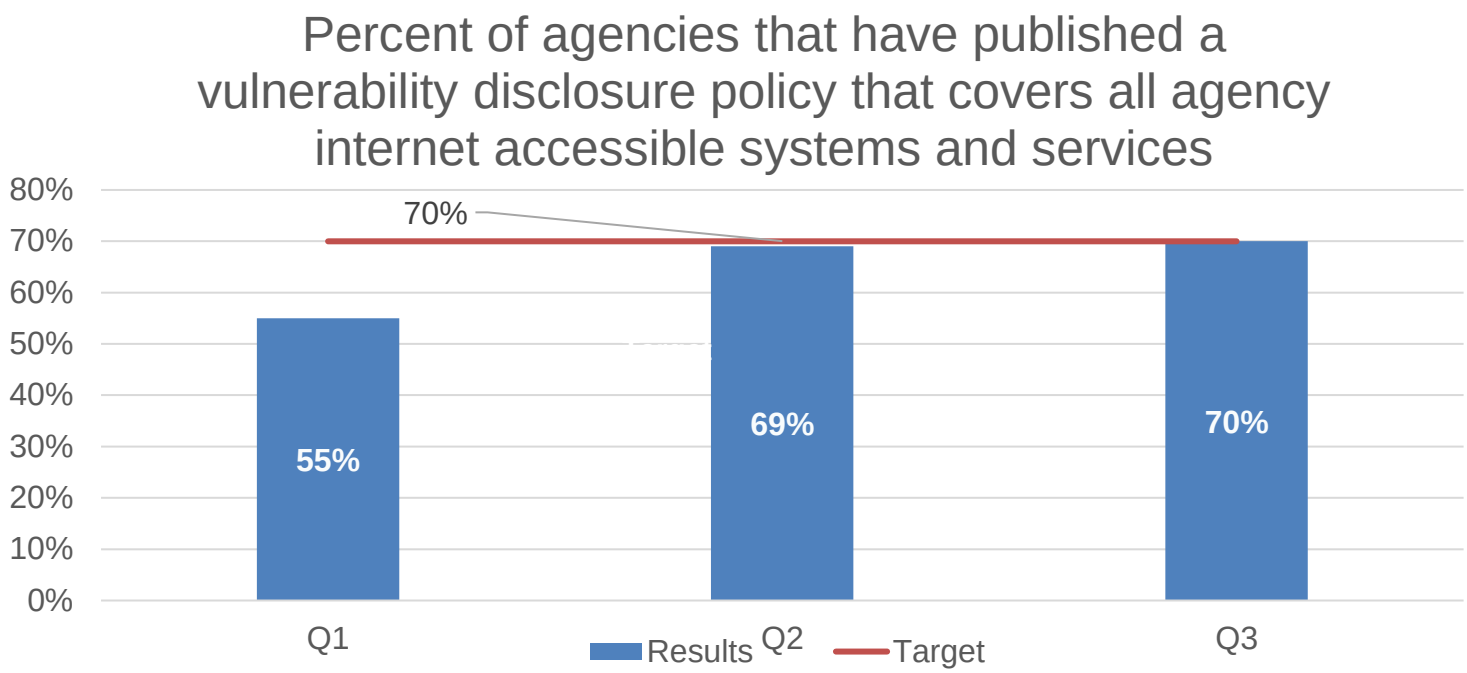
- Coordinate engagement with FCEB stakeholders to address priorities on cyber defense, risk management, and service needs and incorporate feedback into future service offerings.

Key indicators



By the end of Q3, 18 of 27 tools have completed migration to the Cloud Analytic Environment. Five additional tools are in progress and four tools are on the backlog to be planned for a later date.

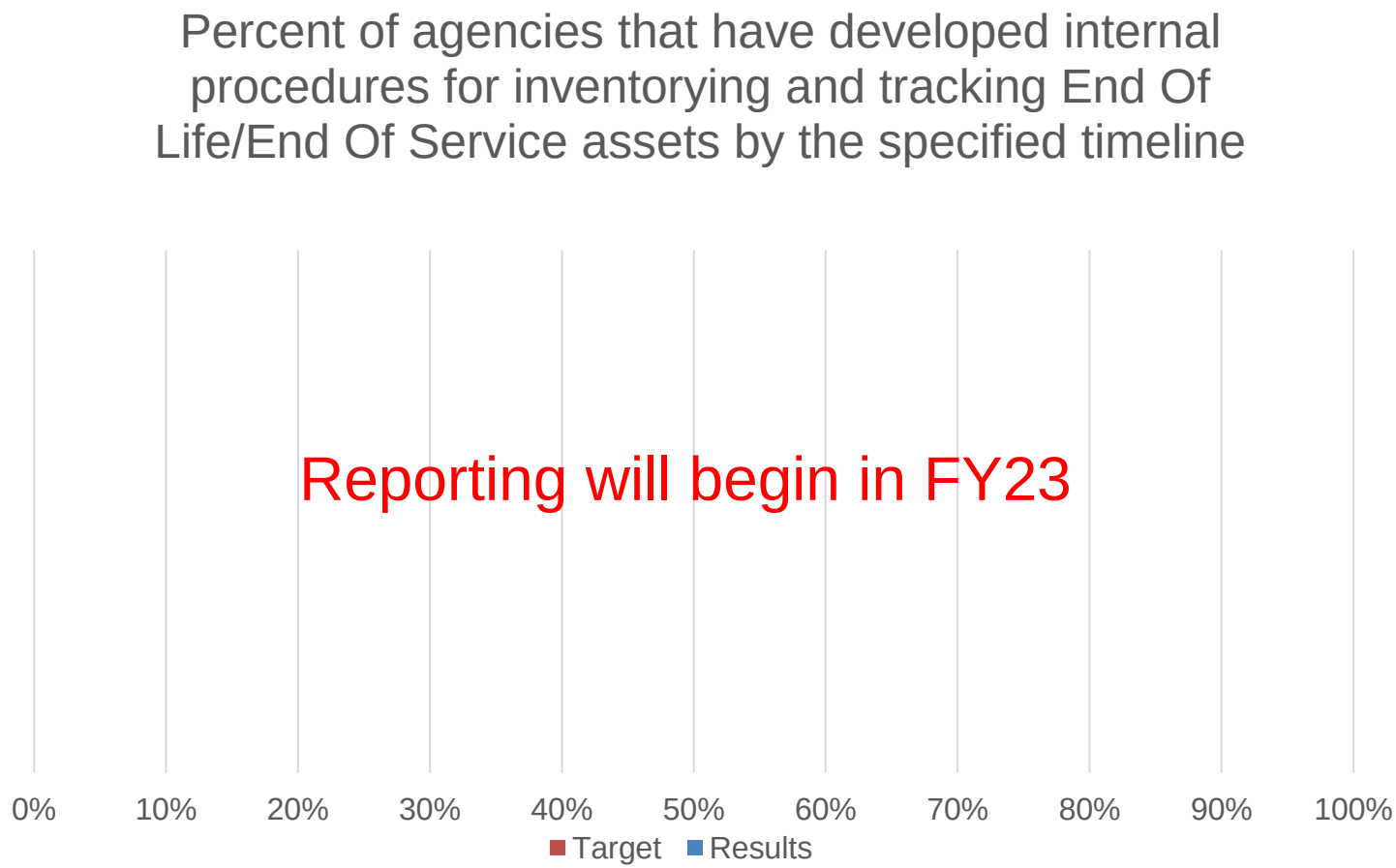
Key indicators



This measure is based on a requirement from Binding Operational Directive (BOD) 20-01: Develop and Publish a vulnerability disclosure policy (VDP), issued on September 2, 2020, in support of OMB Memo 20-32.

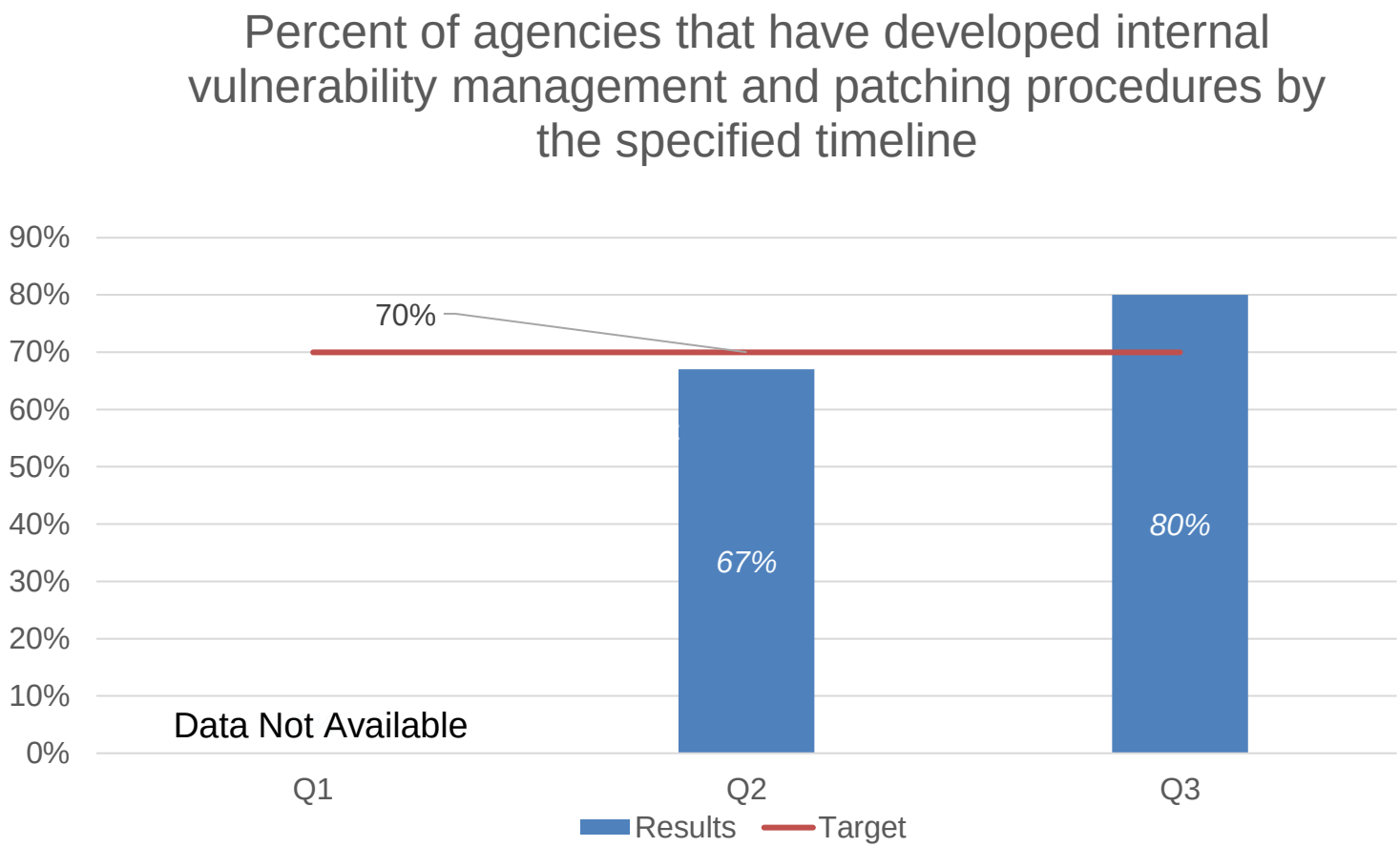
The Directive had phased requirements; the first phase required agencies to publish a VDP. The second phase requires agencies to have all agency internet accessible systems and services be covered by their VDP by September 2022 – the focus of this measure. As of the Q3 reporting date on July 15, 2022, 70% (71 of 101) of agencies had completed the second phase, meeting the goal for end of FY22.

Key indicators



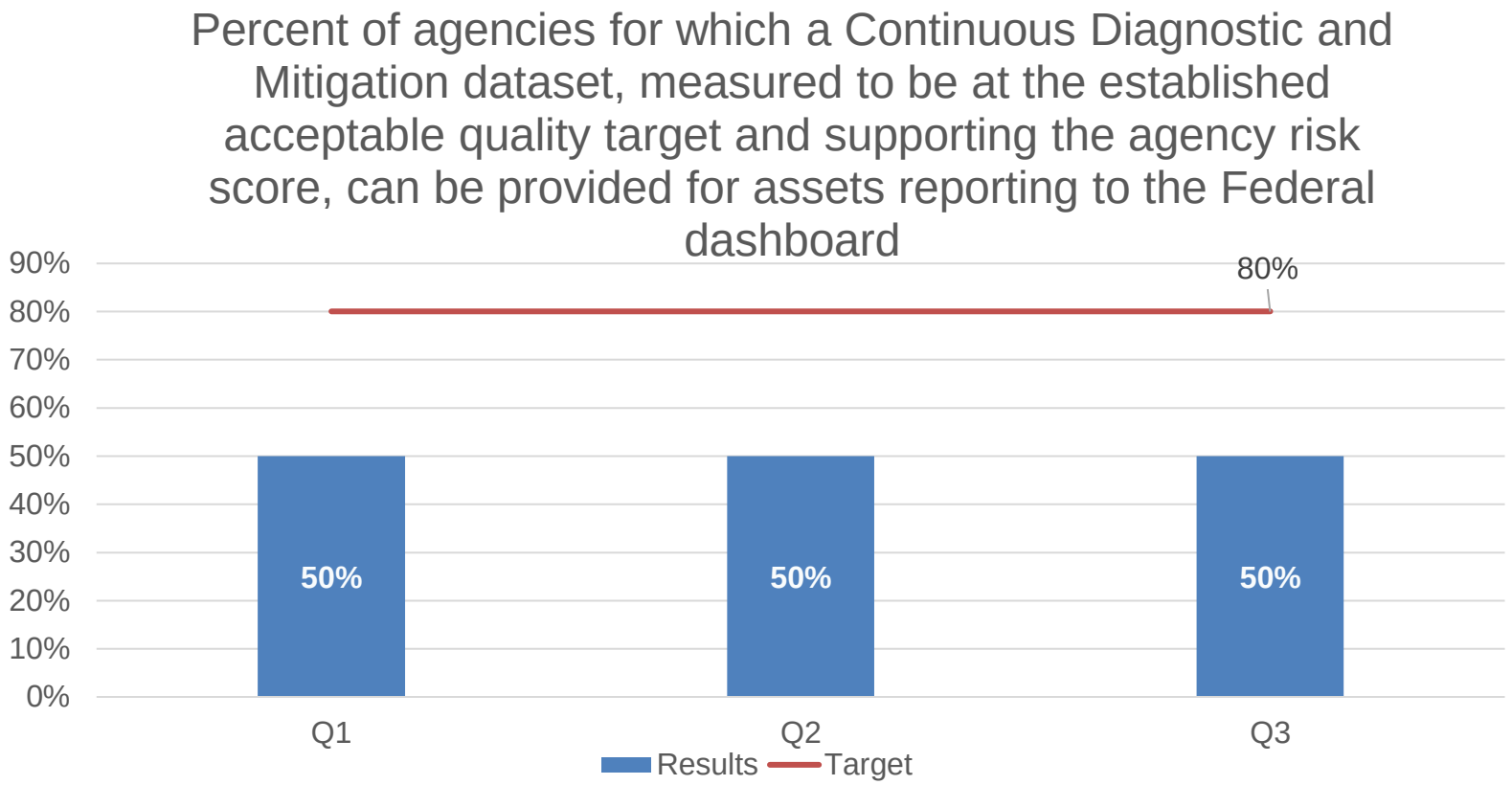
This metric is based on a requirement from CISA's draft Lifecycle Management BOD, which is still under development. Once the BOD is issued, agencies will have six months to comply. This measure is expected to begin reporting in FY23. It is included here to show all measures included in the Federal Cybersecurity Agency Priority Goal (APG).

Key indicators



This metric will track compliance with CISA's Managing Unacceptable Risk Vulnerabilities BOD, released in November 2021. The first requirement from the directive is for agencies to develop or update internal vulnerability management procedures. The requirement to develop or update comes into effect 60 days from issuance, and reporting began in Q2. As of Q3 reporting on July 15, 2022, 81 of 101 (80%) of agencies have completed this requirement, exceeding the goal for FY22.

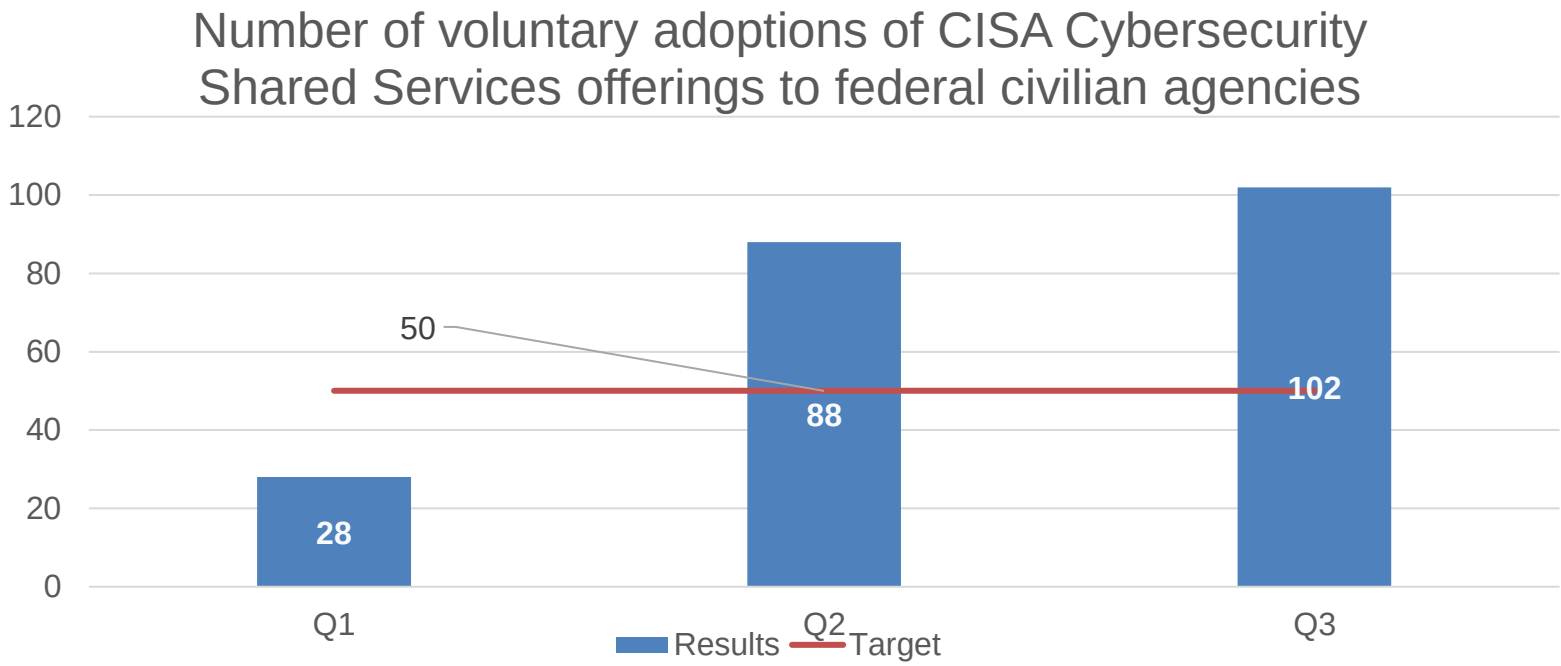
Key indicators



No change from the previous quarter. The Continuous Diagnostic and Mitigation (CDM) program initiated the next round of agency Data Quality Management (DQM) assessments on 26 June for 10 non-CFO Act agencies, and the assessment period will run for 30 days. There will be a 30-day period following this to adjudicate and address issues. The results and scorecard for this assessment should be available in September 2022 and will be reported for Q4.

The four agencies (out of eight assessed) currently reporting reliable data to the federal dashboard are:
- CFO Act: Nuclear Regulatory Commission (NRC) and General Services Administration (GSA)
- Non-CFO Act: National Capital Planning Commission (NCPC) and the Railroad Retirement Board (RRB)

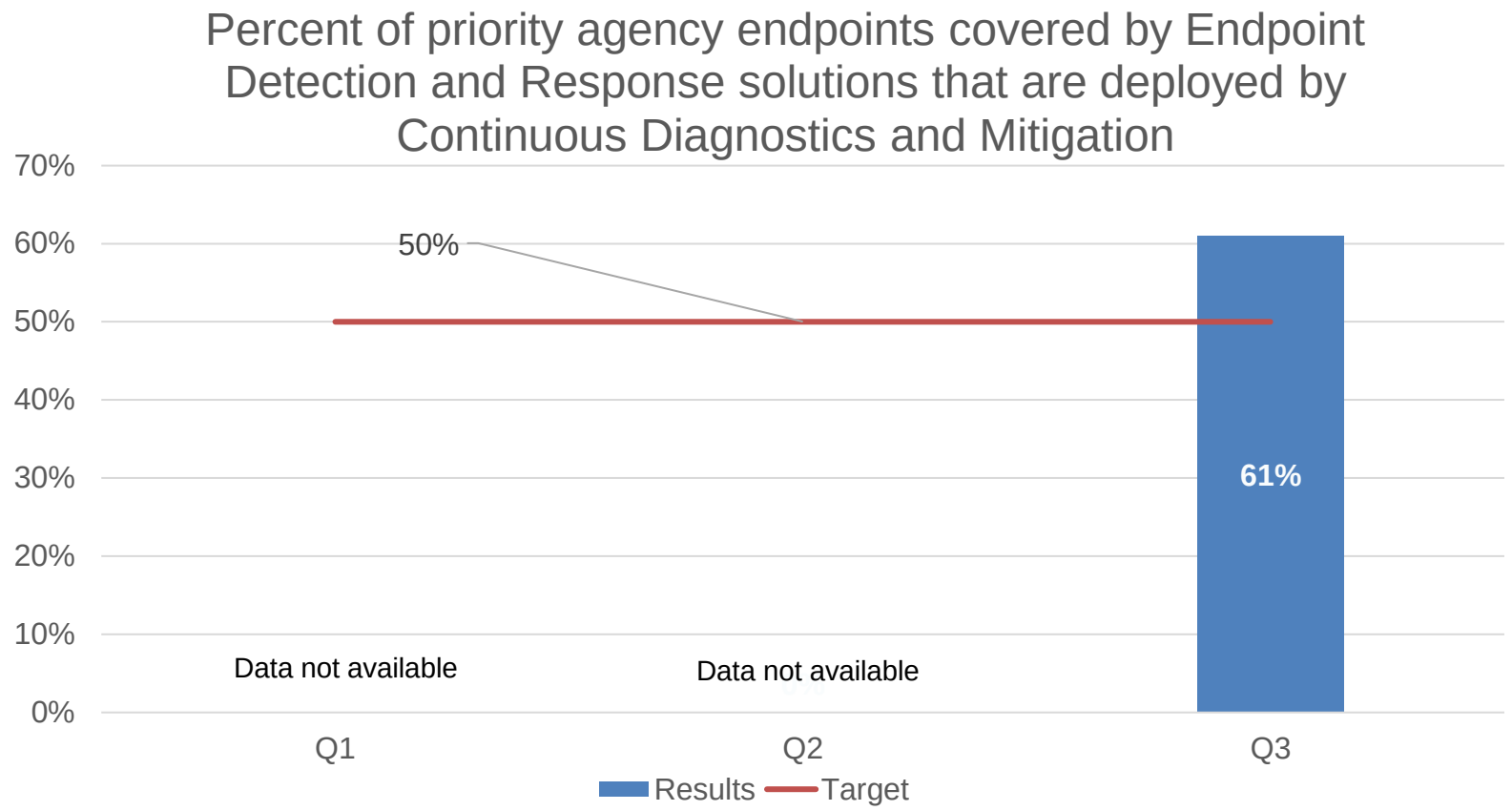
Key indicators



CISA was formally designated the Cyber Quality Services Management Office (QSMO) in April 2020, through which a series of cybersecurity service offerings will be gradually made available for Federal civilian agencies to help them prioritize and manage cyber risks. This measure tracks the total number of adoptions across the Federal Civilian Executive Branch (FCEB). Current service offerings Automated Indicator Sharing, Mobile Application Vetting, Protective Domain Name Service Resolver, Shared Cybersecurity Services, Traveler-Verified Information Protection, Vulnerability Disclosure Policy Platform services as of today. QSMO is expected to expand to 8-10 services total in FY22.

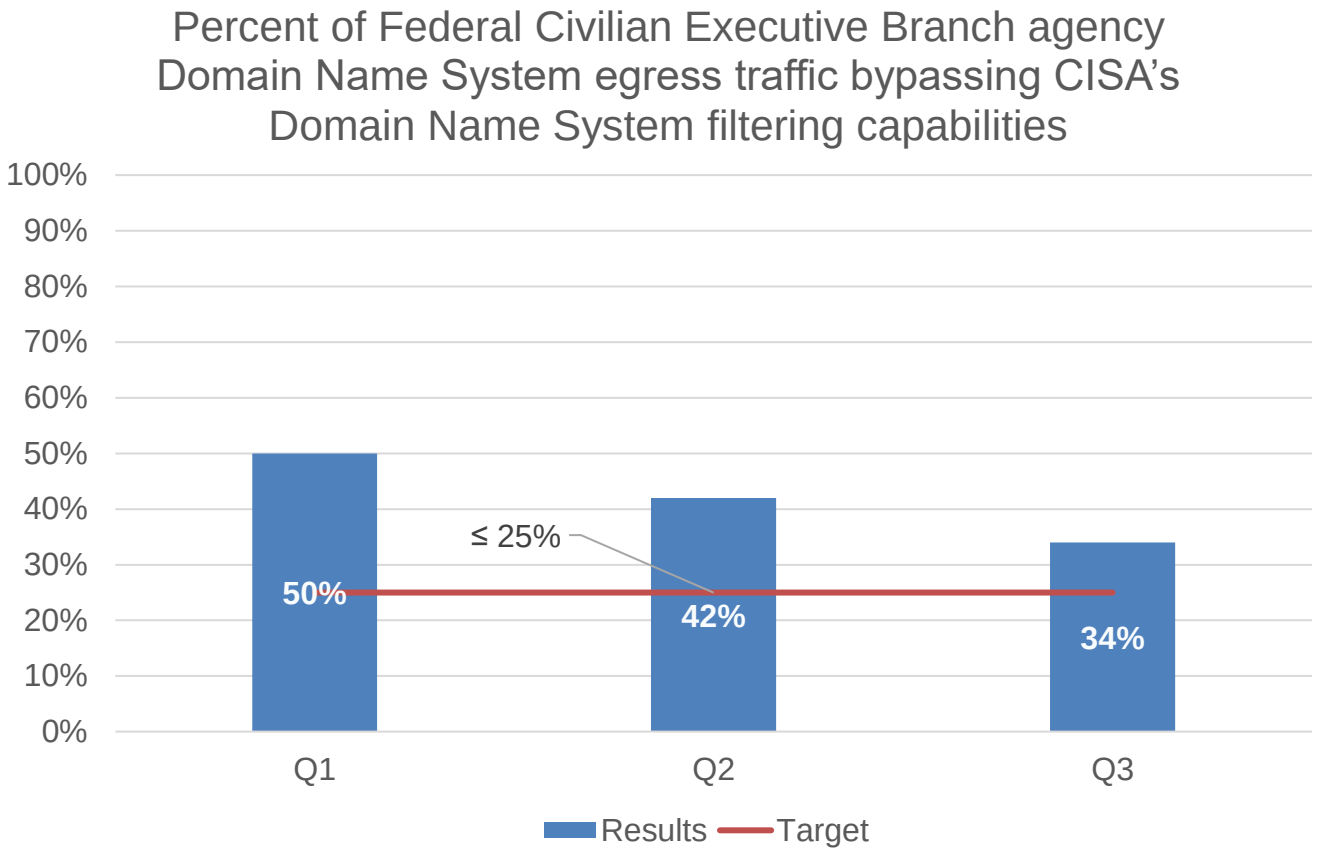
Automated Indicator Sharing 15
Mobile Application Vetting 10
Protective Domain Name Service Resolver 11
Shared Cybersecurity Services 39
Traveler-Verified Information Protection 3
Vulnerability Disclosure Policy Platform 24

Key indicators



Per the Endpoint Detection and Response (EDR) metric definition, three priority agencies have identified the need for 446,546 additional EDR tools to complete EDR coverage requirements per American Rescue Plan Act (ARPA) language. At the end of Q3, 273,836 EDR tools have been deployed by CDM. This constitutes 61% of identified EDR tools deployed.

Key indicators



In Q3, 34% of FCEB Domain Name System (DNS) egress traffic bypassed CISA's DNS filtering capabilities, continuing a positive downward trend towards the 25% end-of-year target.

Overall, 84 of 84 FCEB entities experienced some amount of measurable bypass for Q3. The agency count is out of 84 this quarter because American Battle Monuments Commission is no longer covered by EINSTEIN1 (all collectors inactive) and the Institute of Museum and Library Services had no qualifying traffic (very little traffic of any kind; no DNS, no user-initiated traffic, circuits are mostly inert).

Key milestones

Milestone Summary				
#	Key Milestone	Milestone Due Date	Milestone Status	Comments
1.1	Establish a baseline Analytic Capabilities roadmap	Q1	Complete	The Baseline Roadmap was delivered in December 2021. This roadmap is used to inform planning and migration tracking for on-premise analytic capabilities that are migrating to the NCPS Cloud Analytic Environment.
2.1	Complete Gap Assessments for All 9 Priority Agencies	Q1	Complete	An EDR agent gap analysis has been completed for all 9 priority agencies.
2.2	Begin deployment of EDR tools at 3 Priority Agencies	Q2	Complete	EDR deployments are underway at 3 priority agencies; an additional 4 are still in the planning stages. Two agencies have self-attested that they have full coverage already.
2.3	Complete deployment at 1 Priority Agency; and begin deployment at 3 additional Priority Agencies	Q3	Complete	EDR deployments are still underway at 3 priority agencies with completion between 50-78%; an additional 4 are still in the planning stages. The remaining two priority agencies have 100% coverage.
2.4	Complete deployment at 2 additional Priority Agencies; begin deployment at 4 remaining Priority Agencies	Q4		
2.5	Lifecycle Management Directive is still in development. Have draft for review	Q4		
3.1	Finalize Annual Data Quality Management Plan Update	Q3	Complete	The FY22 DQM plan has been published and is supporting the current rounds of data quality assessments.
3.2	Complete Data Certification Submission Cycle 3 (SC-3)	Q4		

Narrative

Overall, CISA has made substantial progress towards its FY22 targets. Five measures have already met their target and all Q3 milestones have been completed. Notable accomplishments include:

- *Percent of analytic capabilities transitioned to the Cloud Analytic Environment*: Progress towards the completion of the migration is ahead of schedule and the 50% target was met in Q3 (67%).
- *Percent of priority agency endpoints covered by EDR solution(s) deployed by CDM*: deployments are well underway for additional EDR coverage requested by three of the nine priority agencies; the program has deployed 61% of the requested EDR tools as of the end of Q3, exceeding the end-of-year target.
- *Number of voluntary adoptions of CISA Cybersecurity Shared Services offerings to federal civilian agencies*: In Q3, there were 102 adoptions of services, exceeding the target of 50.
- *Percent of agencies that have developed internal vulnerability management and patching procedures in compliance with CISA provided scope and timelines*: as of Q3, 80% of agencies have completed this requirement, exceeding the 70% target.
- *Percent of agencies that have published a vulnerability disclosure policy (VDP) and have all agency internet accessible systems and services covered by their VDP*: as of Q3, this measure met its target of 70%.

Measures that are likely to not meet target:

Percent of agencies for which a CDM dataset, measured to be at the established acceptable quality target and supporting the Agency-Wide Adaptive Risk Enumeration (AWARE) score: This measure will not meet its target for FY22. It took longer than anticipated to update and revise the CDM Data Quality Management Plan, and CDM was only able to pilot the assessment strategy and success criteria with a small cohort this quarter, making the sample size too small to meet the target. CDM will not get into the bulk of the CDM population until next FY.