Agency Priority Goal | Action Plan | FY 22 – 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, 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- Outdated and legacy technology poses risk of increased vulnerabilities associated with weak authentication exposure and unpatched software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

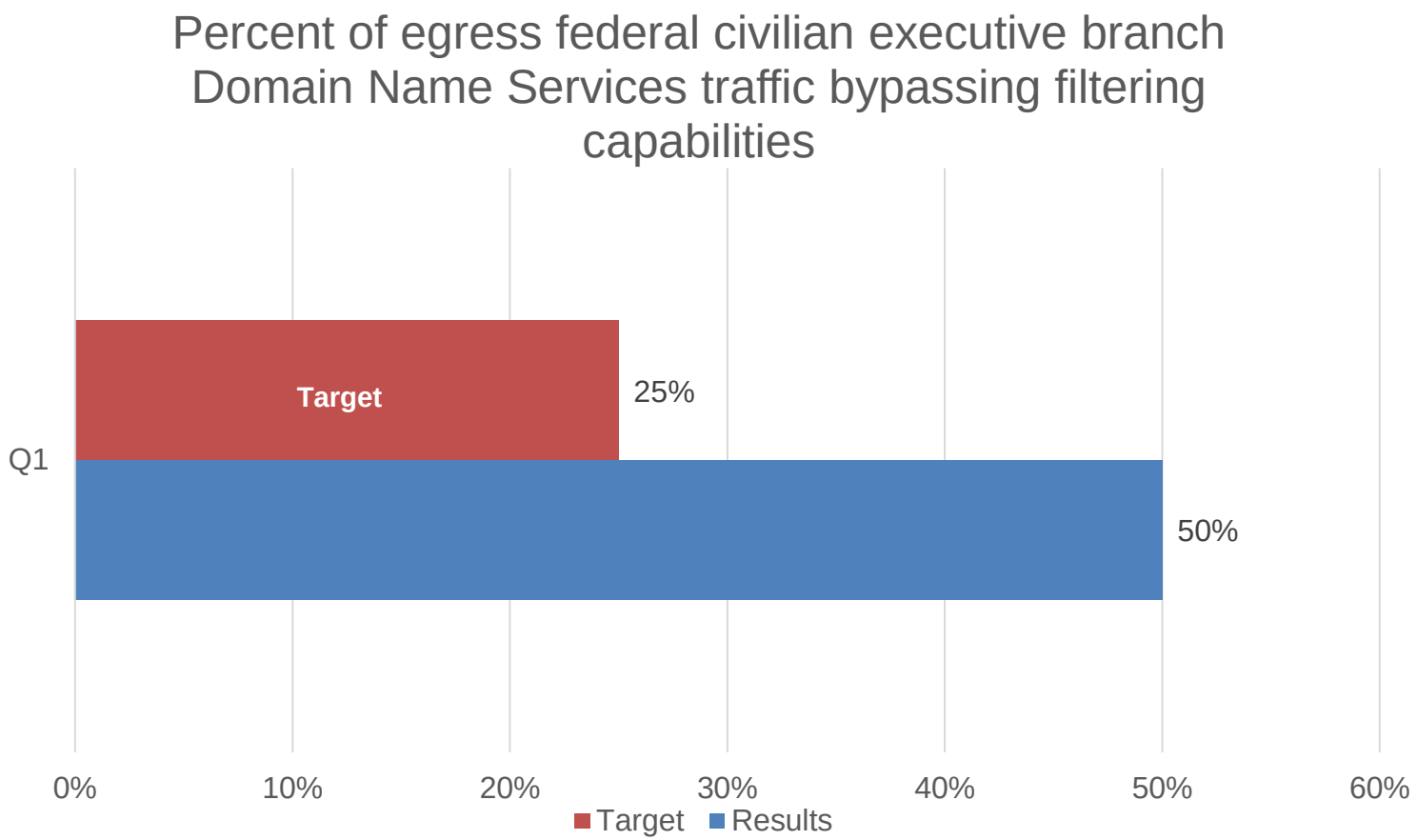
Provide Tools and Services

- 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

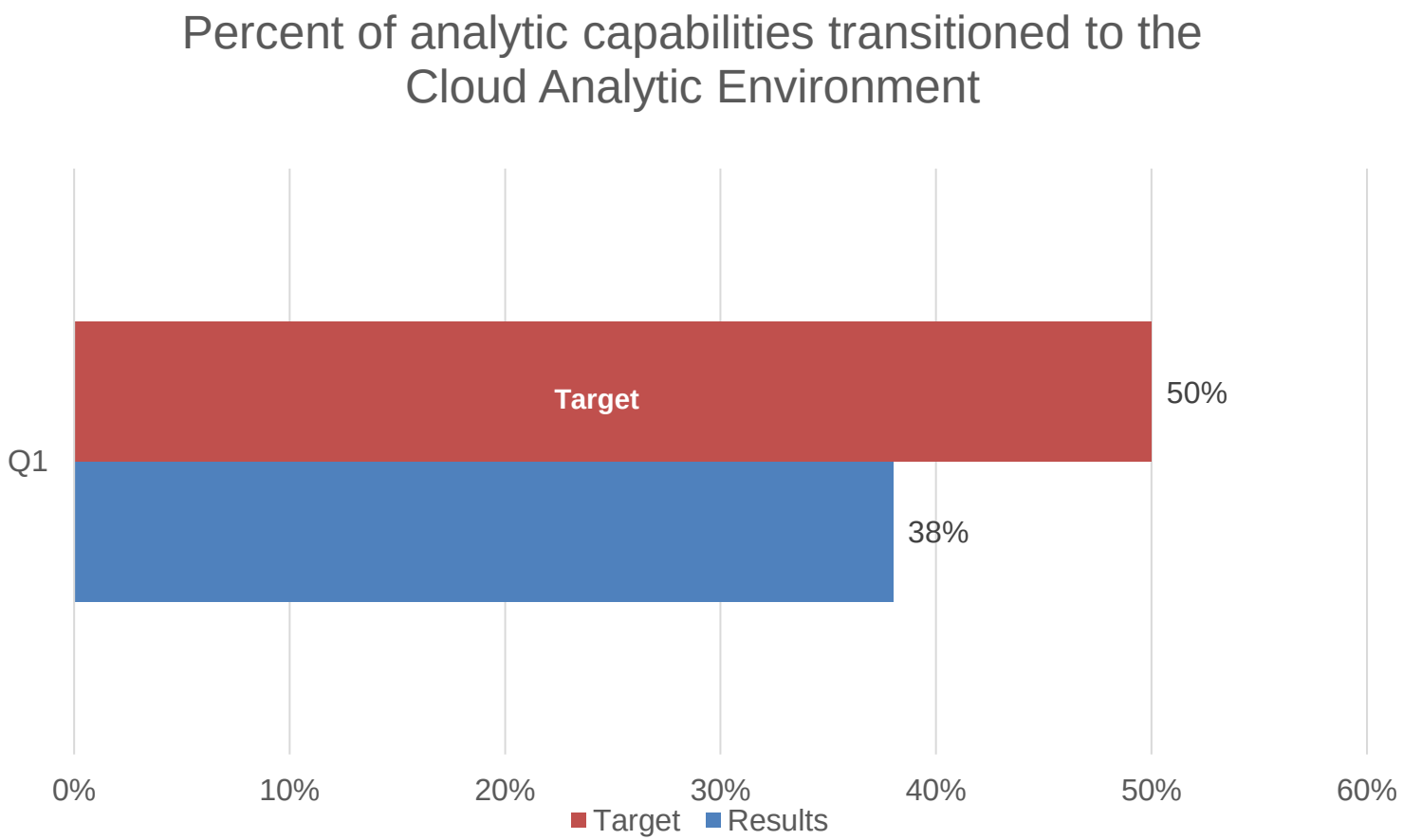
- Coordinate engagement with FCEB stakeholders to address priorities on cyber defense, risk management, and service needs and incorporate feedback into future service offerings.

Key indicators



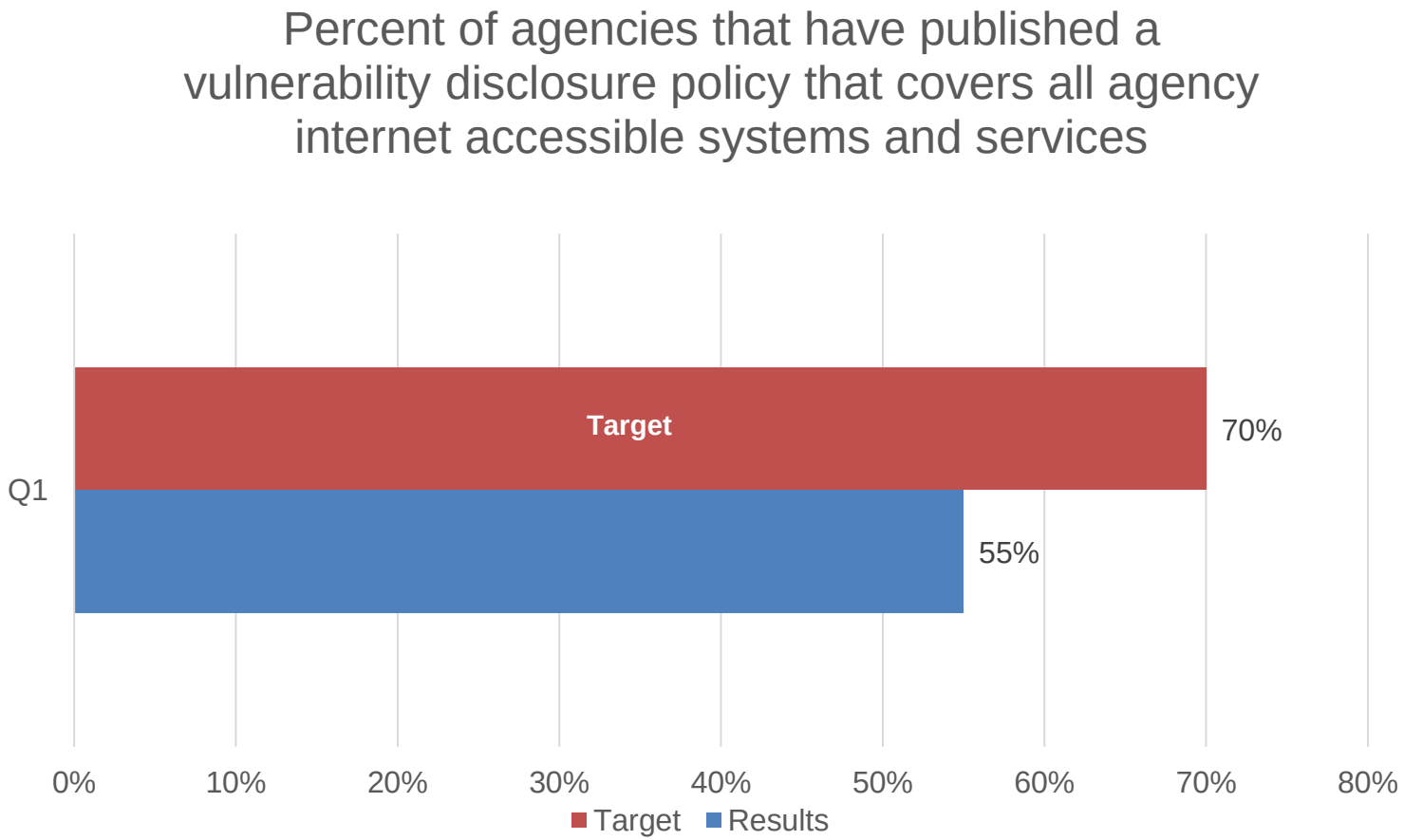
Fifty percent of egress within Federal Civilian Executive Branch (FCEB) Domain Name Services (DNS) traffic was sent to CISA's DNS Filtering capabilities, with 50% bypassing the filtering capabilities. Overall, 85 of 86 FCEB entities experienced measurable bypass in Q1. This measure seeks to track the reduction of traffic bypassing the DNS Filtering capabilities, measuring the reduction of bypass over time towards the 25% target for the fiscal year.

Key indicators



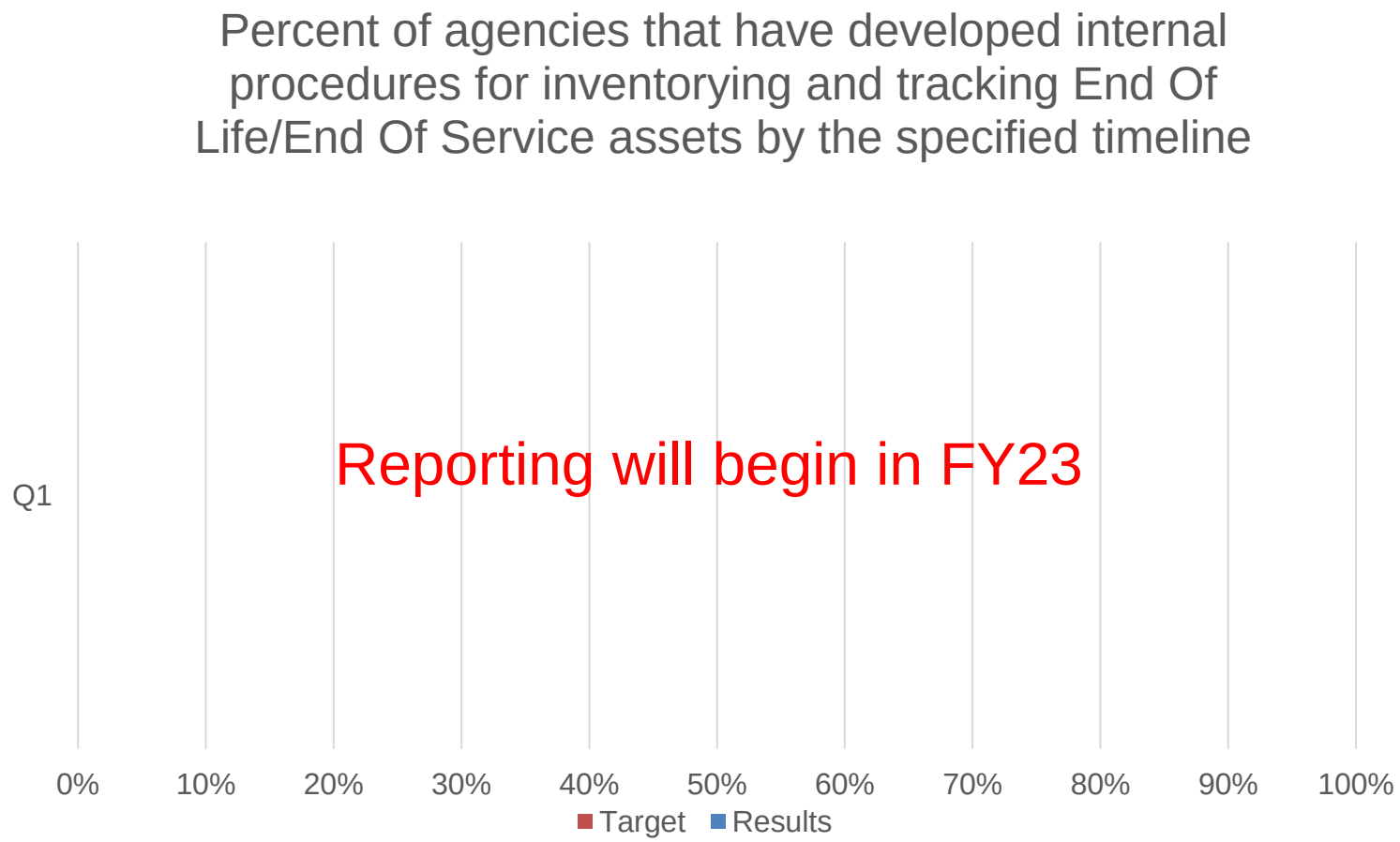
There are 26 analytic tools that were hosted in on-premise environments. By the end of Q1, 10 of 26 tools have completed migration to the Cloud Analytic Environment. Five additional tools are in progress, and 11 tools are on backlog to be planned for a later date.

Key indicators



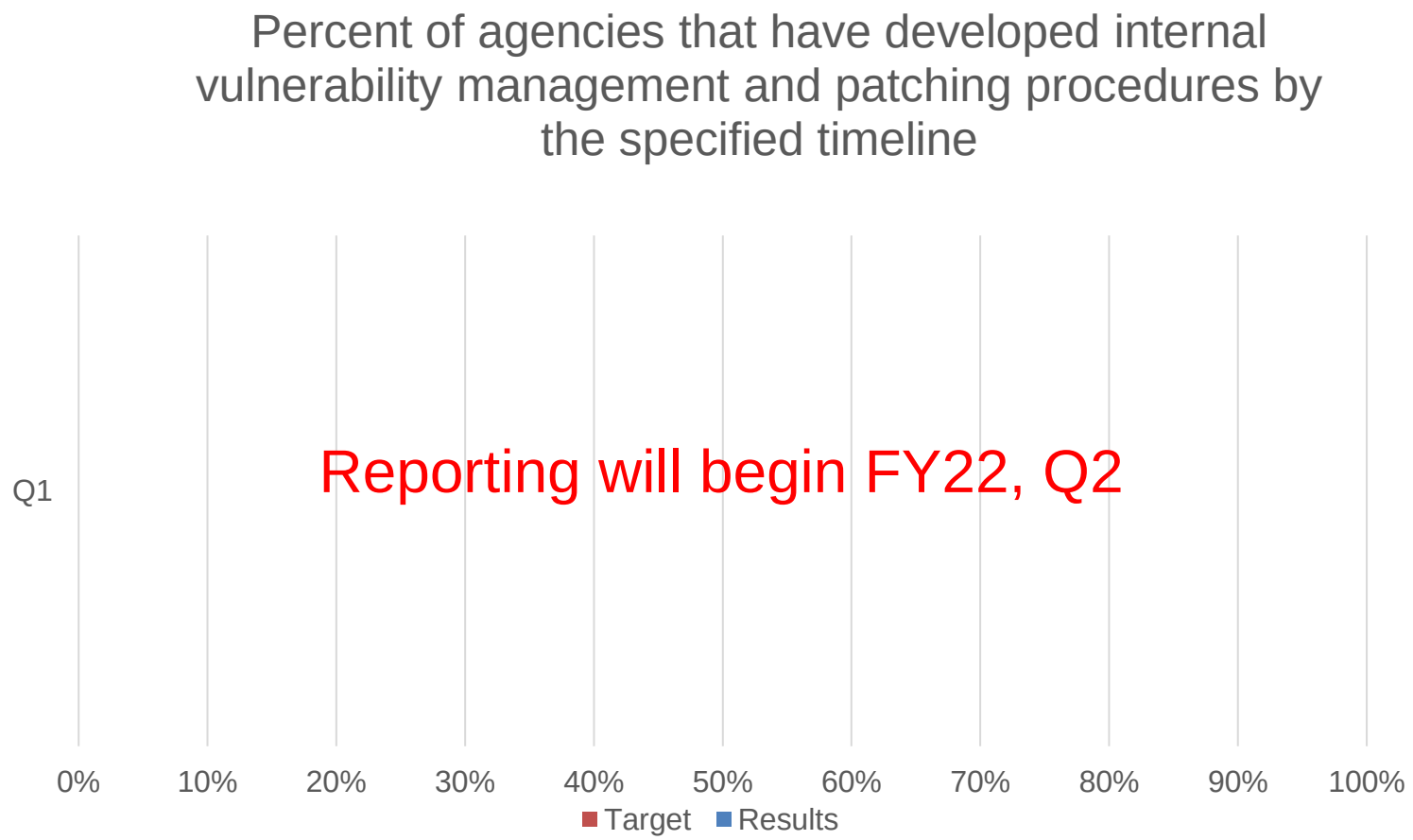
This measure is based on a requirement from Binding Operational Directive (BOD) 20-01: Develop and Publish a vulnerability disclosure policy (VDP), issued on September 2, 2020, in support of OMB Memo 20-32. The Directive had phased requirements; the first phase required agencies to publish a VDP (currently 92% of agencies have developed and published 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 Q1, 55% (56 of 101) of agencies had completed the second phase.

Key indicators



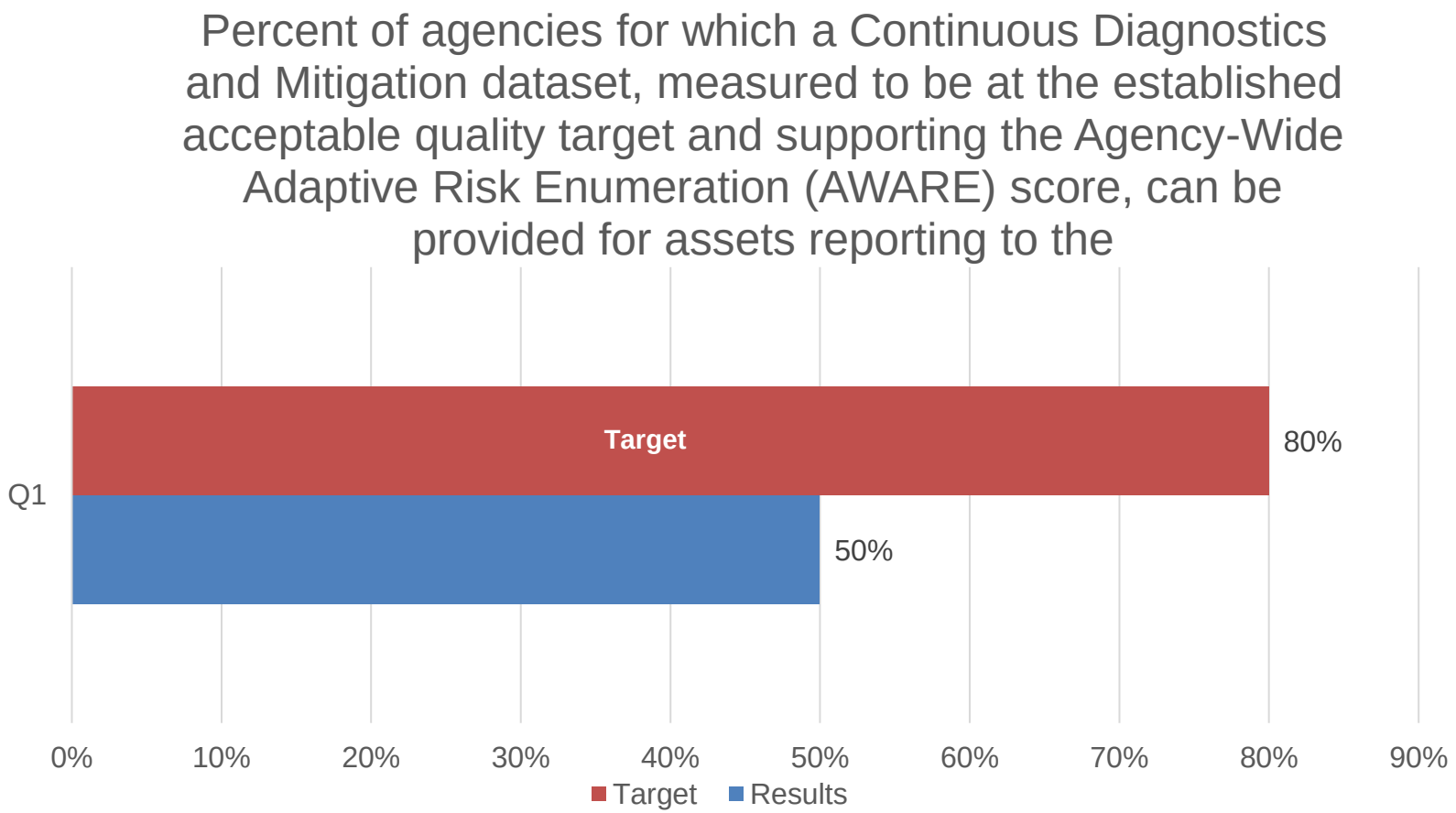
This metric is based on a requirement from CISA's draft Lifecycle Management BOD, which is still under development. Once the BOD is issued, agencies will have six months to comply. This measure is expected to begin reporting in FY23.

Key indicators



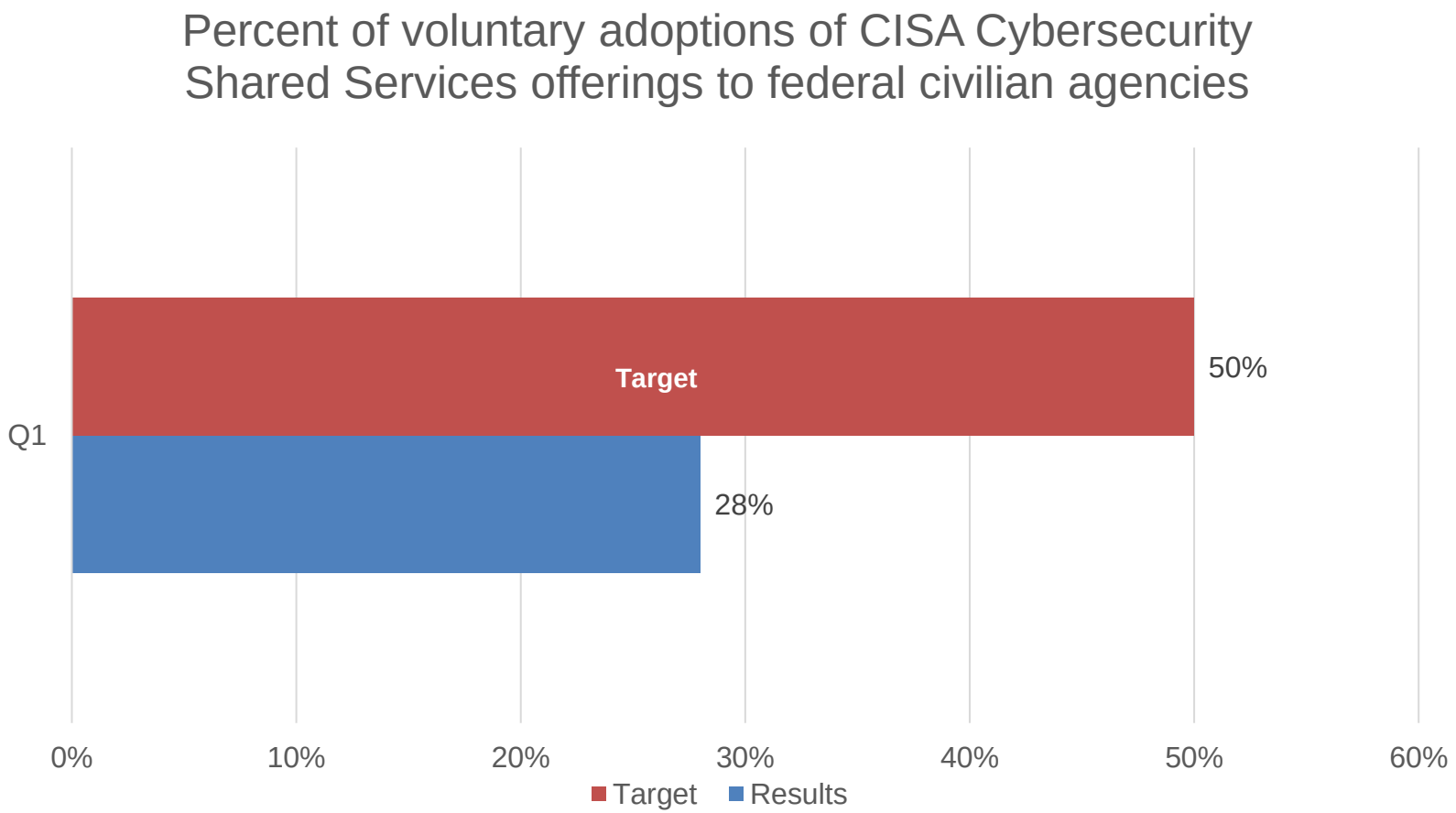
This metric will track compliance with CISA's Managing Unacceptable Risk Vulnerabilities Binding BOD, released in November 2021. The first requirement from the directive is for agencies to develop or update internal vulnerability management procedures. The requirement to develop or update comes into effect 60 days from issuance, and reporting is expected to begin in Q2.

Key indicators



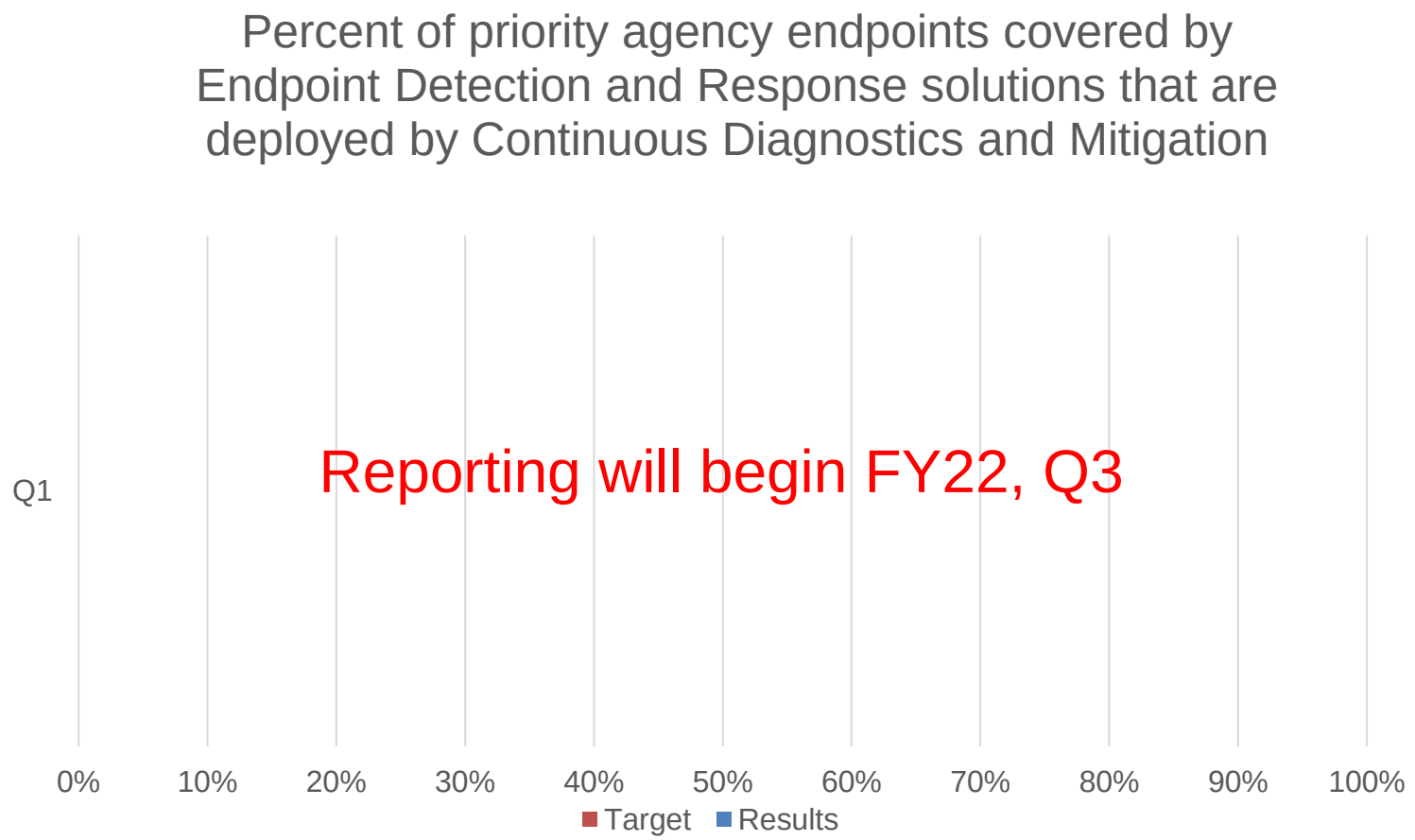
KEY MEASURE: At the end of FY21, eight agencies and/or components (DHS S&T, DHS OIG, DOI, GSA, NCPC, RRB, NRC, and USDA) completed the necessary prerequisites to participate in a Continuous Diagnostics and Mitigation (CDM) Data Quality Management assessment (technical reviews of their Asset Management tools, successful data exchange with the Federal Dashboard, indication of agency readiness).

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 prioritize and manage cyber risks. This measure tracks the total number of adoptions across the Federal Civilian Executive Branches (FCEB). Current service offerings are Vulnerability Disclosure Platform (VDP), Security Operations Center as a Service (SOCaaS), and Mobile services as of today. QSMO is expected to expand to a total of 8-10 services in FY22.

Key indicators



This measure is expected to begin reporting in Q3.

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		
2.3	Complete deployment at 1 Priority Agency; and begin deployment at 3 additional Priority Agencies	Q3		
2.4	Complete deployment at 2 additional Priority Agencies; begin deployment at 4 remaining Priority Agencies	Q4		
2.5	Directive is still in development. Have draft for review	Q4		
3.1	All services develop and submit Unfunded Requirements (UFRs) for prioritization	Q2		
3.2	Finalize Annual Data Quality Management Plan Update	Q3		
3.3	Complete Data Certification Submission Cycle 3 (SC-3)	Q4		

Narrative – FY 22 Q1

Overall, CISA has made substantial progress towards its FY22 targets, and all measures are currently on track. Notable accomplishments include:

- *Percent of analytic capabilities transitioned to the Cloud Analytic Environment*
  - Achieved 76% completion rate in Q1 toward the FY22 target. Overall progress towards the completion of the migration is ahead of schedule.
- *Percent of agencies providing a CDM dataset at the acceptable quality target*
  - Achieved 63% completion rate in Q1 toward the FY22 target. Additionally, during Q1, the CDM program performed an analysis of the data collected during the previous quarter's assessment and gathered lessons learned. Based on these results, the CDM program has updated data sampling methods, quality targets, and scoring processes. This will improve the accuracy of the evaluation while minimizing the potential for sampling errors and will streamline the scoring process
- *Percent of agencies that have developed internal vulnerability management and patching procedures in compliance with CISA provided scope and timelines*
  - CISA is impressed with the number of agencies that have finished this requirement ahead of time. CISA will continue to work with and support agencies to meet the goal of 70% of agencies with all systems and services in scope by the end of FY22