**Agency Priority Goal** | Action Plan | FY 22 – 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, 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- Outdated and legacy technology poses risk of increased vulnerabilities associated with weak authentication exposure and unpatched software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% | 78% | 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

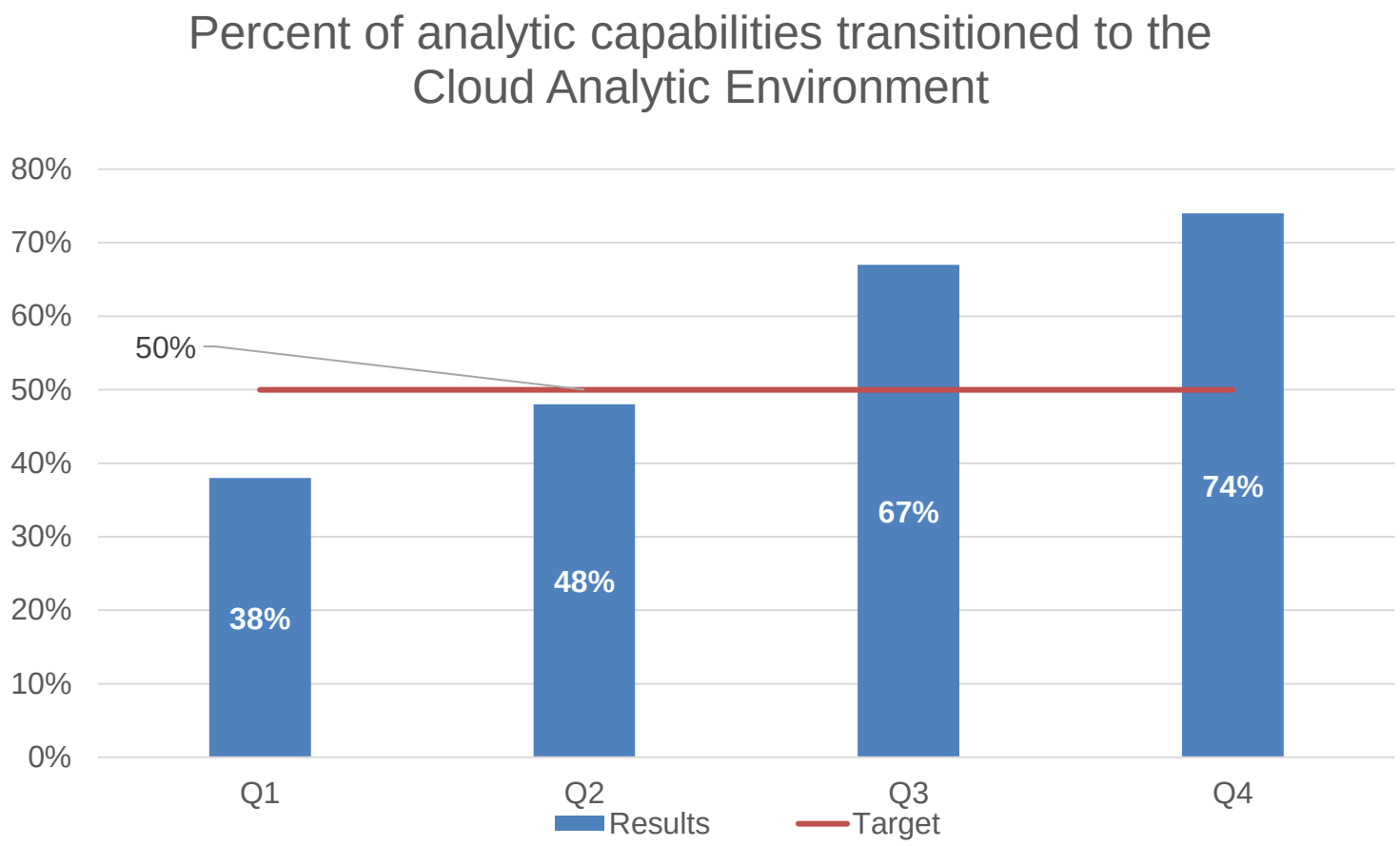
**Provide Tools and Services**

- 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**

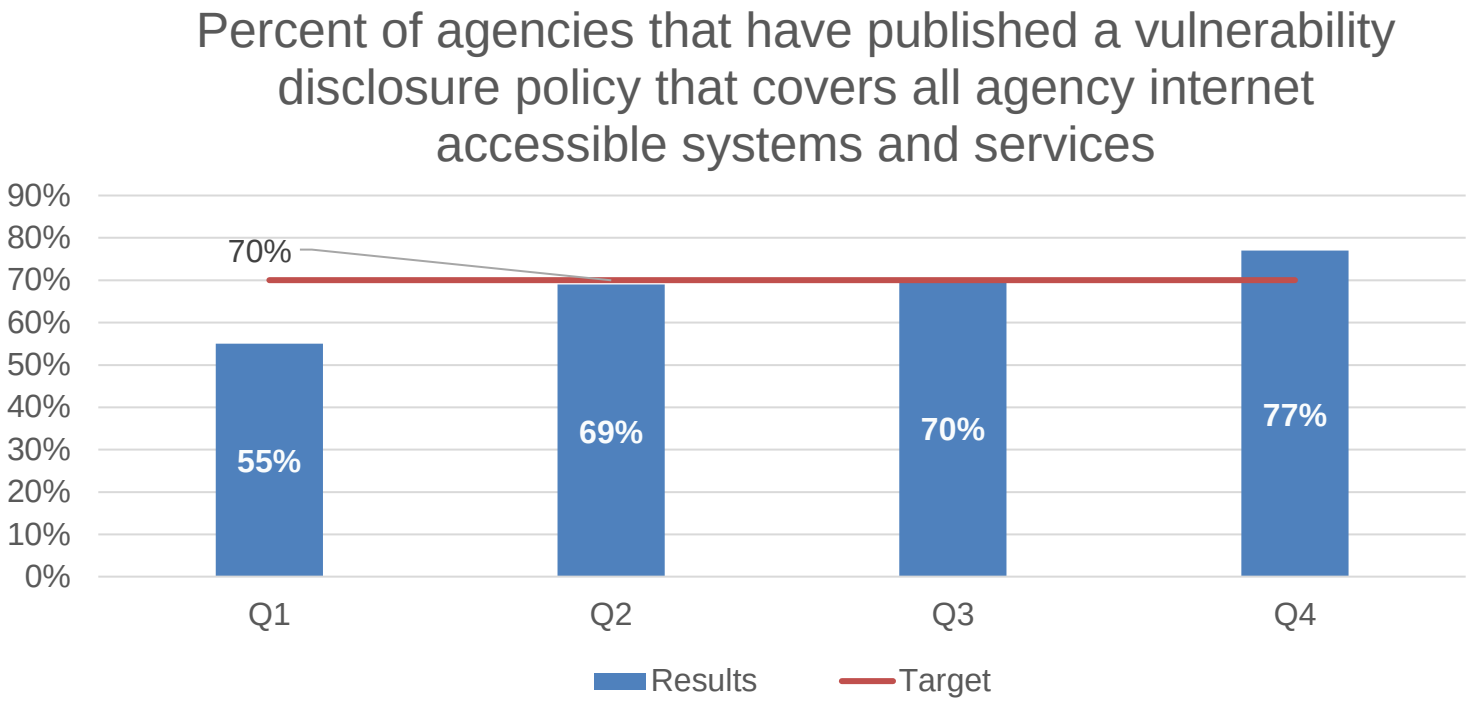
- Coordinate engagement with FCEB stakeholders to address priorities on cyber defense, risk management, and service needs and incorporate feedback into future service offerings.

# Key indicators




By the end of Q4, 20 of 27 tools have completed migration to the Cloud Analytic Environment. Six additional tools are in progress and one tool is on the backlog to be planned at a later date.

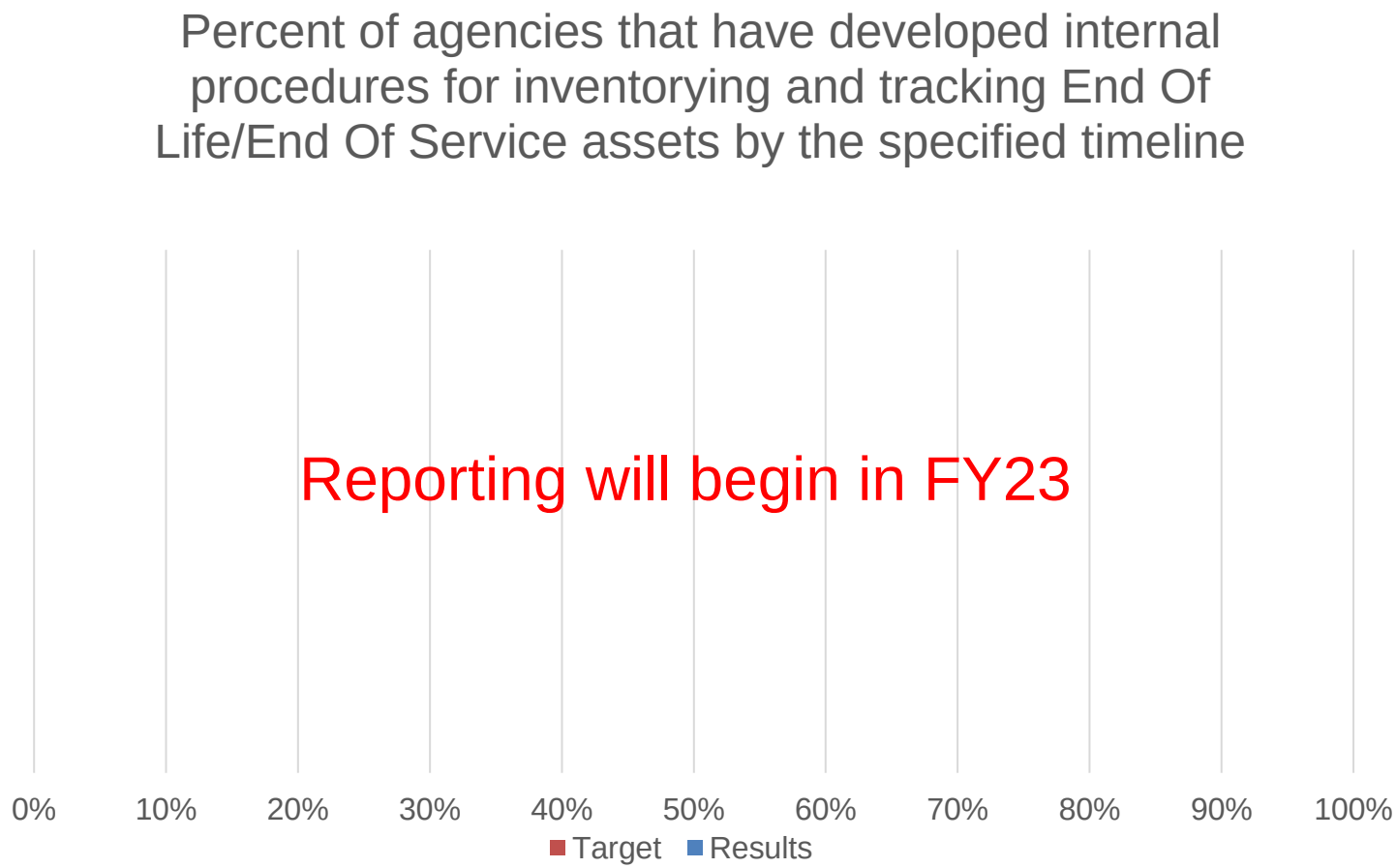
# Key indicators




This measure is based on a requirement from BOD 20-01: Develop and Publish a 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 (99% met). 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.

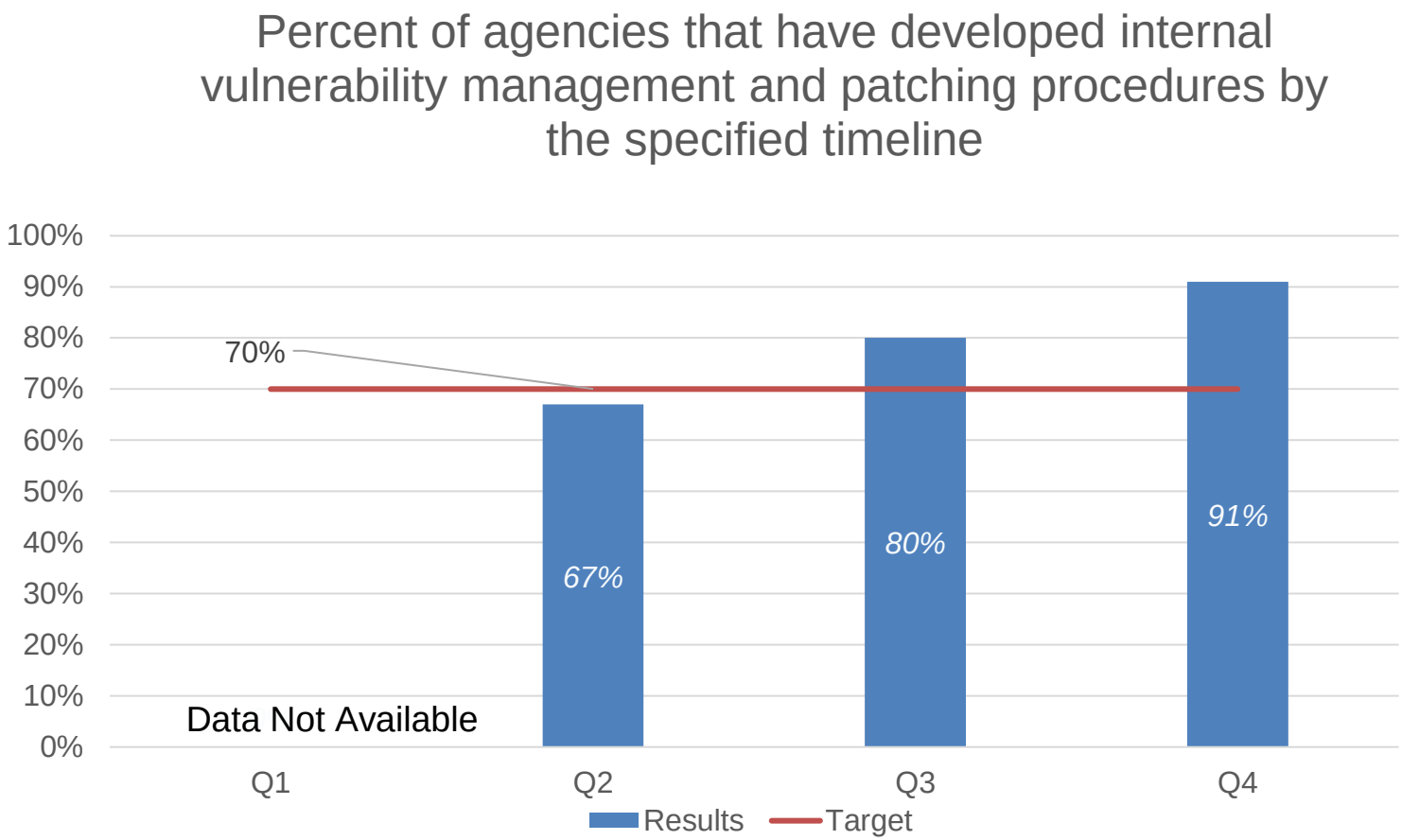
As of Q4, 77% (78 of 101) of agencies have completed the second phase, meeting the goal for end of FY22. CISA is working to bring the remaining agencies into compliance on a case-by-case basis.

# 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 Binding Operational Directive (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 Q4 reporting, 92 of 101 (91%) of agencies have completed this requirement, exceeding the goal for FY22.

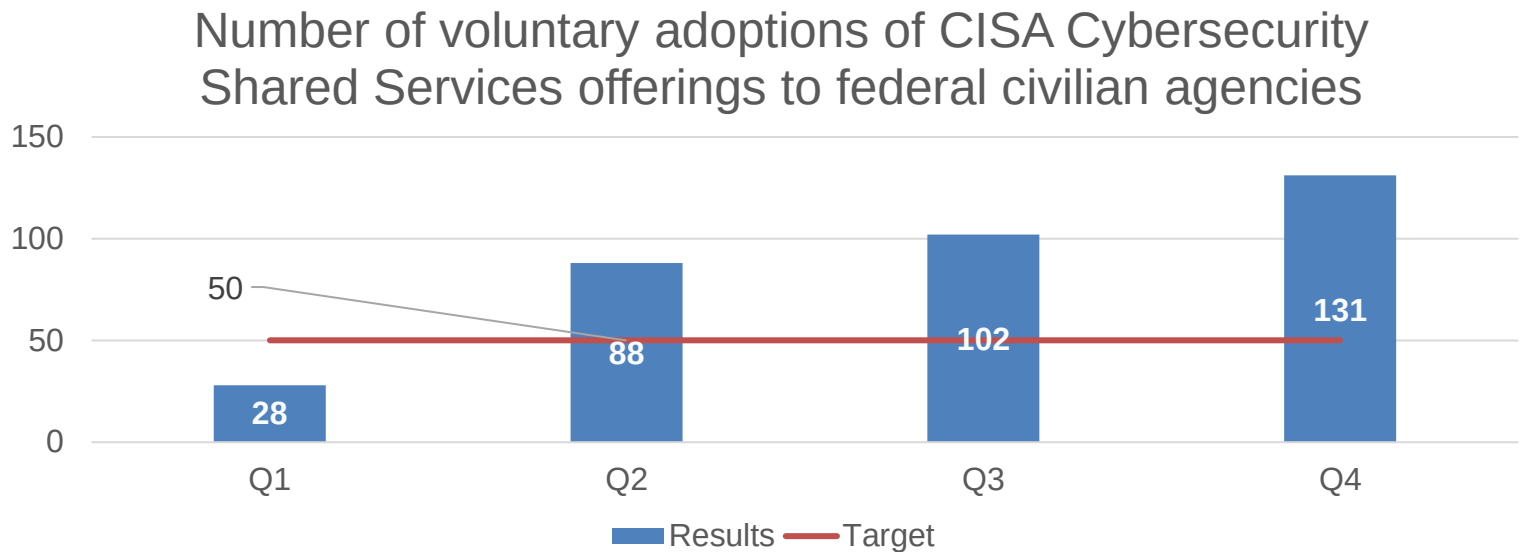
# Key indicators


For Q4, ten out of ten agencies passed the final FY22 DQM assessment. They include:

- Board of Governors of the Federal Reserve (BGSF)
- National Archives and Records Administration (NARA)
- Consumer Product Safety Commission (CPSC)
- Denali Commission (DENALI)
- Department of State Office of the Inspector General (DOSOIG)
- Federal Mine Safety and Health Review Commission (FMSHRC)
- Inter-American Foundation (IAF)
- Corporation for National and Community Service (CNCS)
- Council of the Inspectors General on Integrity and Efficiency (CIGIE)
- Gulf Coast Ecosystem Restoration Council (GCERC)

The Q4 result is cumulative resulting in 14 agencies out of 18 total passing the FY22 DQM assessment for a result of 78%. This measure did 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 year.

# Key indicators



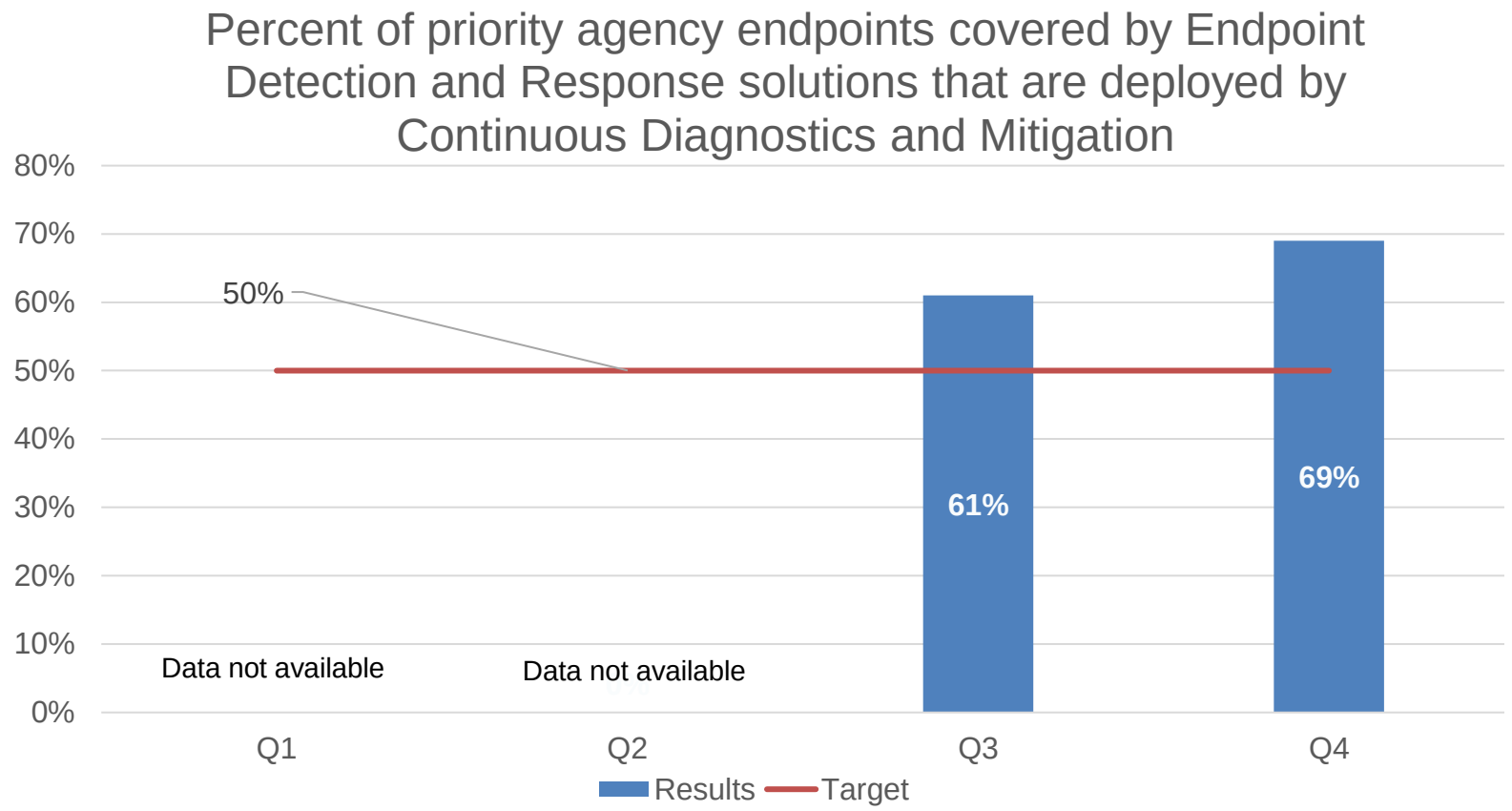

CISA was formally designated as the lead for bringing a shared cyber security services model to federal agencies in April 2020, through which a series of cybersecurity service offerings are being gradually made available for Federal civilian agencies to help them prioritize and manage cyber risks. This measure tracks the total number of adoptions across the FCEB.

As of Q4, the current service offerings are Automated Indicator Sharing (added Q2), Mobile Application Vetting, Protective Domain Name Service Resolver, Shared Cybersecurity Services (added Q2), Traveler-Verified Information Protection, Vulnerability Disclosure Policy Platform and E3A services (added Q4).

The cumulative total of adoptions for FY22 is 131, with 77 new adoptions added throughout the year, exceeding the target of 50. The program also inherited new services: 54 adoptions were added to the baseline with the addition of Automated Indicator Sharing and Shared Cybersecurity Services in Q2.

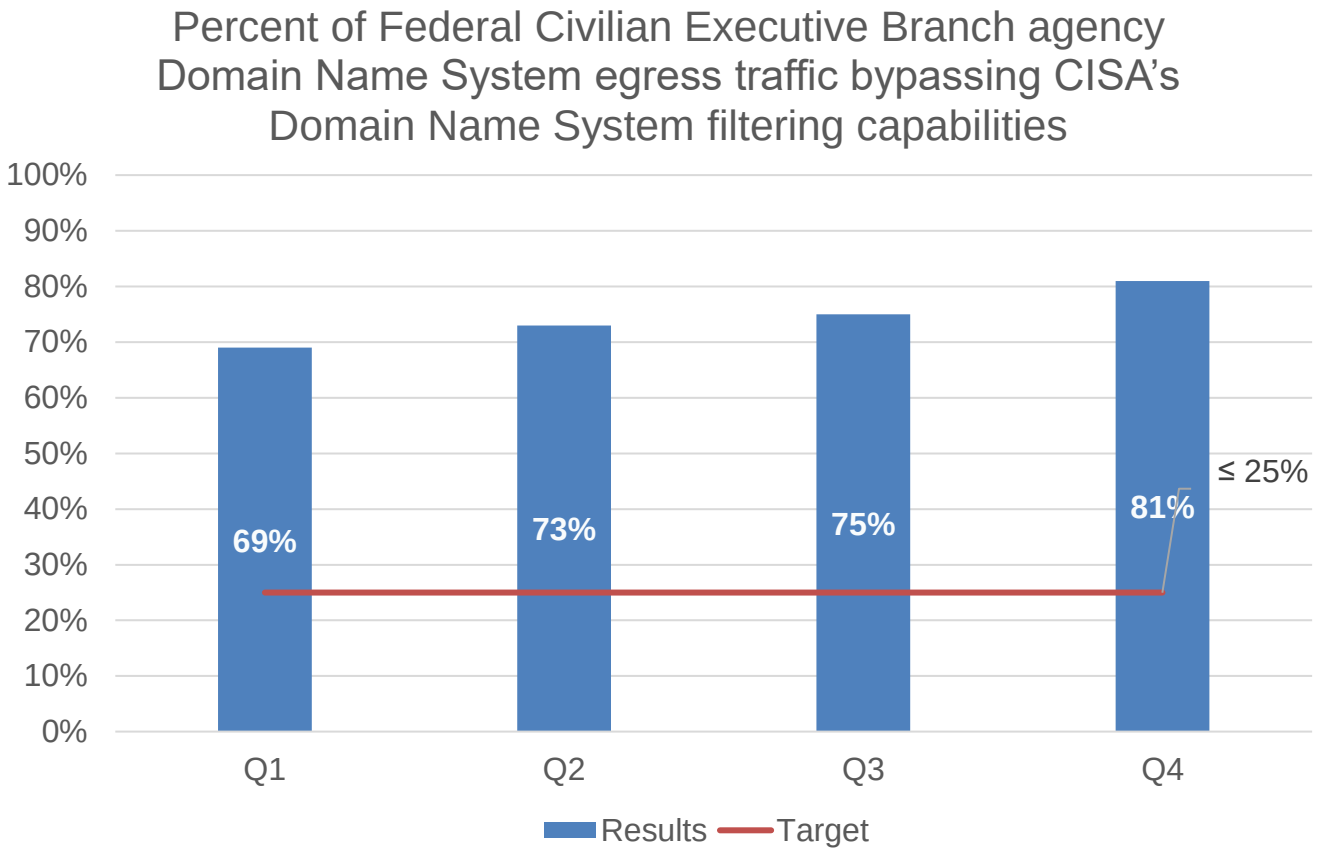
Automated Indicator Sharing 58; Mobile Application Vetting 1; Protective Domain Name Service Resolver 12; Shared Cybersecurity Services 40; Traveler-Verified Information Protection 1; and Vulnerability Disclosure Policy Platform 19.

# Key indicators




Priority agencies have identified a need for a total of 446,546 licenses (endpoints) within the established lead time for Q4. CDM has deployed 307,082 licenses, which constitutes 69% of identified EDR licenses deployed. One license covers one endpoint.

# Key indicators




In collecting the Q4 data, CISA discovered two software bugs that had artificially inflated the traffic count. One of the bugs was cumulative; larger counts resulted in larger distortions than smaller counts. The net effect of this was to cause all calculated percentages to be artificially depressed. These issues have been corrected and the previous quarters' statistics have been updated.

# 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 | Complete | There are ten completed and/or started deployments. |
| 2.5 | Directive is still in development. Have draft for review. | Q4 | Complete | Draft Directive is complete, currently pending final review. |
| 3.1 | All services develop and submit Unfunded Requirements (UFRs) for prioritization | Q2 | Complete | Services have submitted their UFRs for FY22 and have been prioritized by branch leadership for Acquisition and Budget Branch. |
| 3.2 | 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. |
| 3.3 | Complete Data Certification Submission Cycle 3 (SC-3) | Q4 | Complete | The SC-3 Data Certification assessment was completed on 9/30/2022. |

# Narrative

Overall, CISA has met most of its FY22 targets, and these will be revised for FY23. Five measures have met their target and all Q4 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 Q4 (74%). It is on track to meet its FY23 target of 100% analytic capabilities transitioned to the Cloud Analytic Environment in FY23.
- Percent of priority agency endpoints covered by EDR solution(s) deployed by CDM: the program has deployed 69% of the requested EDR tools as of the end of Q4, exceeding the end-of-year target of 50%. In FY23 the program plans to expand the measure to include all agencies, not just priority agencies.
- Number of voluntary adoptions of CISA Cybersecurity Shared Services offerings to federal civilian agencies: At the end of Q4, there were 131 adoptions of services, with 77 new adoptions added throughout the year, exceeding the target of 50. The program also inherited new services: 54 adoptions were added to the baseline with the addition of Automated Indicator Sharing and Shared Cybersecurity Services in Q2 and 94 adoptions were added to the baseline with the addition of E3A (a related service to Protective DNS) in Q4.
- Percent of agencies that have developed internal vulnerability management and patching procedures in compliance with CISA provided scope and timelines: as of Q4, 91% 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: this measure has exceeded its target of 70% with Q4 results at 78%.

Measures that did 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 did 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 year.
- Percent of Federal Civilian Executive Branch agency Domain Name System egress traffic bypassing CISA's Domain Name System filtering capabilities: In collecting the Q4 data, CISA discovered two software bugs that had artificially inflated the traffic count. One of the bugs was cumulative; larger counts resulted in larger distortions than smaller counts. The net effect of this was to cause all calculated percentages to be artificially depressed. These issues have been corrected and the previous quarters' statistics have been updated.