



Agency Priority Goal | Action Plan | FY 2023 – Q2

Cybersecurity Agency Priority Goal (APG)

Goal Leader(s):

Kelly E. Fletcher, Chief Information Officer
Bruce R. Begnell, Principal Deputy Chief Information Officer
Donna S. Bennett, Enterprise Chief Information Security
Officer

Goal Overview

The U.S. Department of State aims to ...

Through implementation of the Federal Zero Trust Strategy, the Department will improve its security posture by fully securing its infrastructure, networks, and data against internal and external cyber threats. By September 30, 2023, the Department will improve the maturity of all five Zero Trust pillars to the Advanced level as defined by the CISA Zero Trust Maturity Model.

Goal Overview

Problem to Be Solved

- As noted in the newly released Federal Zero Trust Strategy, the Federal Government can no longer depend on conventional perimeter-based defenses to protect critical IT systems and data.
- The Department must address the increased frequency and potential severity of cyber-attacks by modernizing the underpinnings of our IT resource access mechanisms.

What Success Looks Like

- By building maturity in all five pillars, the Department will develop a capacity to authenticate/protect users, and to dynamically control which devices can access resources. It will ensure all data is encrypted and is managed according to sensitivity and treat all applications as if they are public facing.

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	Improve the maturity level to the "advanced" level in all five zero trust pillars.	Number of pillars* at the "advanced" level** *The 5 pillars are Identity, Device, Network/Environment, Application Workload, Data **The 3 maturity levels are Traditional, Advanced, and Optimal	5 pillars	0	0*	Quarterly

* Individual Pillar targets on slide 9 are based on reaching an “Advanced” maturity by September 30, 2023

** As of 10/1/2021

Goal Team

Preliminary Maturity Baseline Assessment

- Senior Leader: IRM/OPS
- Contributing IRM partners: E-CISO, FO
- Contributing Outside Partners: S/ES, CA, DS, CIO Council

Implementation Plan

- Senior Leader: E-CISO
- Contributing IRM partners: CO, FO, OPS
- Contributing Outside Partners: S/ES, CA, DS, CIO Council, CISA

Non-.gov hostnames

- Senior Leader: IRM/OPS
- Contributing partners: BMP, CO, FO, OCA
- Contributing Outside Partners: All DOS System Owners

Categorizations for sensitive electronic documents

- Senior Leader: CDO
- Contributing partners: BMP, CO, E-CISO, FO, OCA, OPS
- Contributing Outside Partners: CISO Council

Password/Authentication Policies

- Senior Leader: E-CISO
- Contributing partners: E-CISO, FO, OCA, OPS
- Contributing Outside Partners: CISO Council

Operate FISMA moderate application on the internet

- Senior Leader: OPS
- Contributing partners: CO, FO
- Contributing Outside Partners: All Bureau IT POCs

Legend: CDO – Chief Data Officer; CO – Cyber Operations;
E-CISO – Enterprise Chief Information Security Office; FO – Foreign Operations;
OCA – Office of the Chief Architect; OPS – Operations

Goal Strategies

Multiple organizations across the Department will work under the guidance of the E-CISO to contribute to the implementation of the [Federal Zero Trust Strategy](#), starting with the FY 2022 Q2 issuance of a Zero Trust Implementation Plan. Progress is achieved by advancing the maturity of activities within each pillar, with the goal of each pillar achieving optimal maturity. Maturity assessments will use the rubric defined in the [CISA Maturity Model](#). A long-term effort, full implementation of a Zero Trust framework will exceed the period of this APG but should be achieved by the end of FY 2024.

Zero Trust Pillars

As noted in the [Federal Zero Trust Strategy](#), the five Zero Trust pillars envision the following:

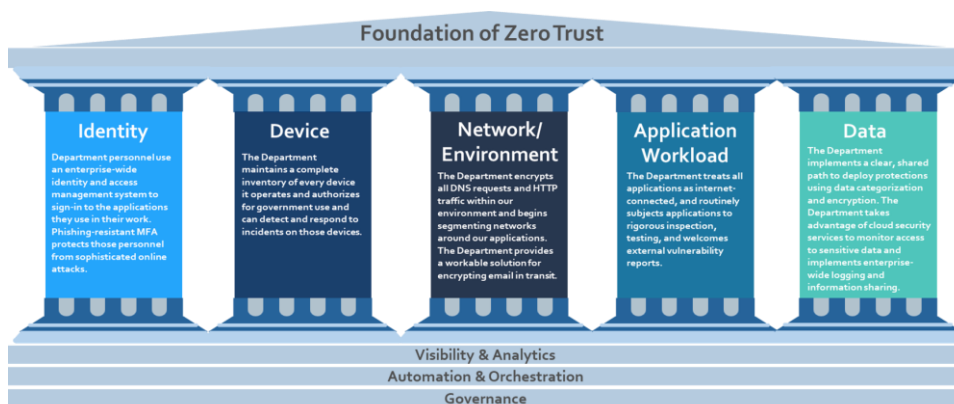
Identity: Use enterprise-managed identities to access the applications in our work. Phishing-resistant MFA protects personnel from sophisticated online attacks.

Device: Maintain a complete inventory of every device authorized and operated for official business; and prevent, detect, and respond to incidents on those devices.

Network: Encrypt all DNS requests and HTTP traffic within our environment and begin executing a plan to break down perimeters into isolated environments.

Applications and Workloads: Treat all applications as internet-connected, routinely subjecting applications to rigorous empirical testing, and welcoming external vulnerability reports.


Data: Embark on a clear, shared path to deploy protections that make use of thorough data categorization. Take advantage of cloud security services and tools to discover, classify, and protect sensitive data, and implement enterprise-wide logging and information sharing.



Zero Trust Pillar Maturity Levels

Traditional – manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response and mitigation deployment.



 **Advanced** – some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to pre-defined mitigations, increased detail in dependencies with external systems, some least-privilege changes based on posture assessments.



Optimal – fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, centralized visibility with historian functionality for point-in-time recollection of state.

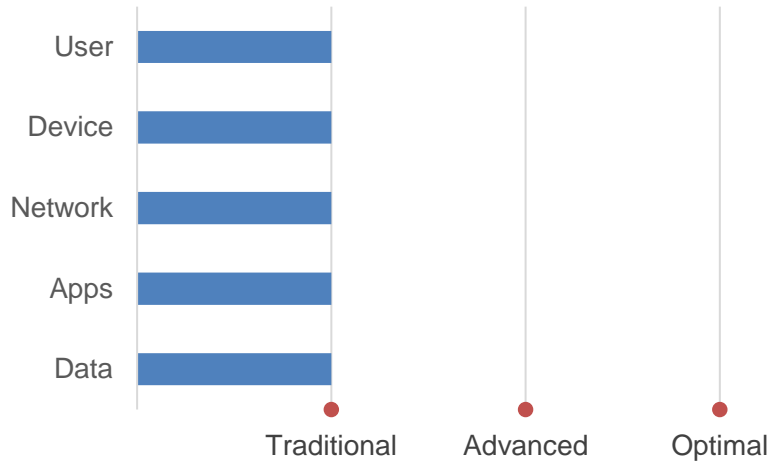
Key indicators

Indicator Title	Current Value	FY 2022 Target	FY 2023 Target
Zero Trust Maturity			
Number of individual pillars advancing to the “Advanced” maturity level each year. (Traditional, Advanced, Optimal)*	0	2	5
Number of activities advanced within Pillar 1 – Identity	3	3	12
Number of activities advanced within Pillar 2 – Device	3	3	12
Number of activities advanced within Pillar 3 – Network/Environment	3	3	12
Number of activities advanced within Pillar 4 – Application Workload	1	4	14
Number of activities advanced within Pillar 5 – Data	3	3	12

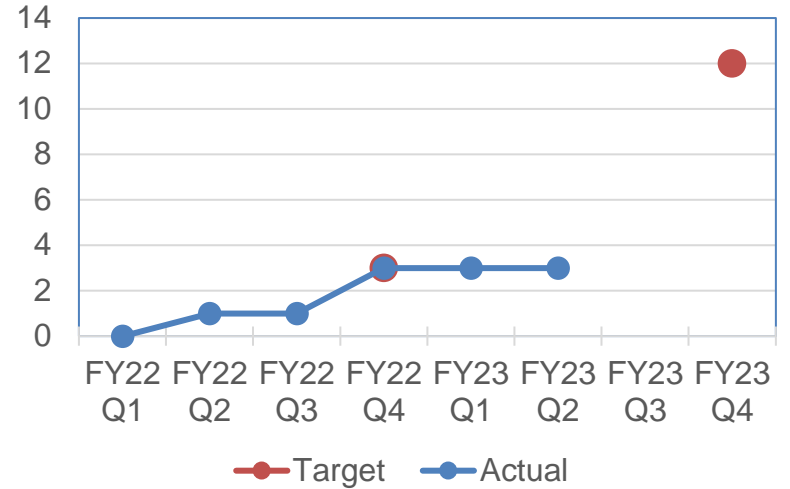
* The Department’s starting point in the CISA model is “Traditional.” During the CISA assessment phase, we determined that our investments in Identity, Credential, and Access Management (ICAM) contributed toward an advancement in the Identity Pillar. For the remaining pillars, we reset our cybersecurity baseline at Traditional during the assessment.

Key indicators

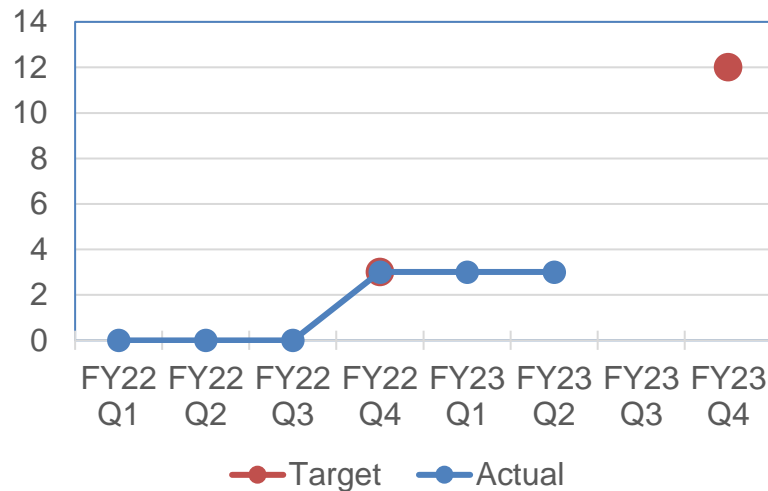
Maturity Level of Each Zero Trust Pillar



Number of Advancements in Identity Pillar

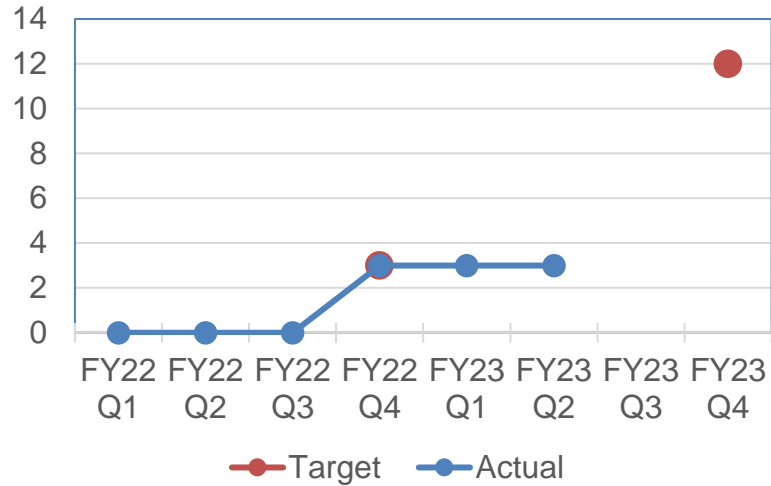


Number of Advancements in Device Pillar

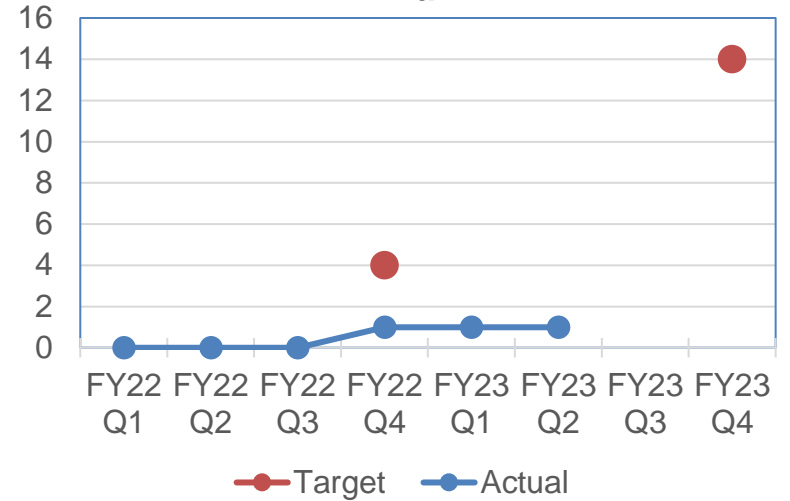


Key indicators

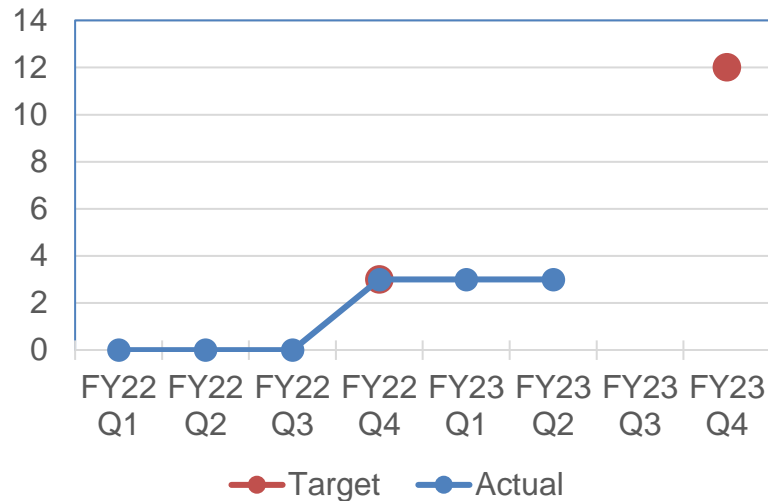
Number of Advancements in Network Pillar



Number of Advancements in Application Pillar



Number of Advancements in Data Pillar



Key milestones

Milestone Summary			
Key Milestone*	Milestone Due Date <i>[e.g., Q2, FY 2017]</i>	Milestone Status <i>[e.g., Complete, On-Track, Missed, Ongoing]</i>	Comments <i>[Provide discussion of Progress, changes from last update, Anticipated Barriers or other Issues Related to Milestone Completion]</i>
Complete a Preliminary Zero Trust Maturity Baseline Assessment.	Q1, FY 2022	Complete	We completed an assessment of three target systems. The results will help us identify maturity gaps and develop a Zero Trust architecture.
Submit to OMB and CISA an implementation plan for FY 2022-FY 2024 for OMB concurrence, and an implementation budget estimate for FY 2023-2024.	Q2, FY 2022	Complete	The CIO submitted the Zero Trust Implementation Plan for the Department on March 29, 2022.
Build and submit to CISA and GSA a list of internet accessible systems utilizing domains other than “.gov”.	Q2, FY 2023	Complete	An initial list of DNS names has been established. As part of the continuous monitoring effort, IRM continues to discover through research that all department websites are tracked and reported in the iMatrix system tool, a request was made to update the necessary fields to create the other than ".gov" list. Furthermore, E-CISO receives weekly reports for non.gov websites.
Develop a set of initial categorizations for sensitive electronic documents.	Q3, FY 2022	Complete	The Department enables information protection within Azure Information Protection (AIP) Office 365 and MS Office Product suite.
Deploy phishing-resistant authentication mechanism for all multi-factor enabled public-facing Department systems.	Q2, FY 2023	Missed/Delayed	OKTA is still in the process of being installed as an enterprise solution to enforce phishing-authentication flows for applications. In addition, IRM is working to update the FIDO2 implementation plan.

* These Milestones for Zero Trust Implementation originate from M-22-09 “Federal Zero Trust Strategy”

Key milestones

Milestone Summary			
Key Milestone*	Milestone Due Date <i>[e.g., Q2, FY 2017]</i>	Milestone Status <i>[e.g., Complete, On-Track, Missed]</i>	Comments <i>[Provide discussion of Progress, changes from last update, Anticipated Barriers or other Issues Related to Milestone Completion]</i>
Remove from all systems password policies that require special characters and regular password rotation.	Q2, FY 2023	Missed/Delayed	Multi-factor authentication is being deployed across the Department but is not yet complete. Once password policies and DTMs have been drafted, actions can be taken on implementation and adding policy language to the 19 FAM.
Select at least one FISMA Moderate system that requires authentication and is not currently internet-accessible, and securely allow full-featured operation over the internet.	Q3, FY 2023	Complete	IRM identified SAFE as the moderate system. SAFE is also a High Valued Asset (HVA) system. Planning has begun on the Zero Trust implementation process for the SAFE application.

* These Milestones for Zero Trust Implementation originate from M-22-09 “Federal Zero Trust Strategy”

Narrative – FY 2023 Q2

The Department continues to collaborate with key stakeholders to implement Zero Trust capabilities throughout the enterprise. In FY 2022 Q4, a decision was made to focus efforts on the Identity pillar in order to speed up this foundational element of Zero Trust. The State Enterprise Identity, Credential Asset Management (SE-ICAM) team continues to work towards the goal of maturing and advancing the identity capabilities in a phased approach, allowing the Department to enter the advanced maturity level as described in CISA's Draft Zero Trust Maturity Model. The following activities were addressed by the SE-ICAM team and Enterprise Chief Information Security Officer's (ECISO) team to incrementally advance capabilities:

- Continues to work towards the Initial Operating Capability (IOC) for the **Master User Record (MUR)** project to standardize enterprise identity management. IOC goal is scheduled for Q3/FY23. Work continues across several Department bureaus to collect and sanitize required attributes.
- Continues to implement **Multi-Factor Authentication (MFA)** using OKTA as the enterprise identity provider for 13 additional cloud-based applications for a total of 418 applications complete to date. The SE-ICAM team is working through a backlog of applications while aligning with system owner readiness. The ECISO is making initial recommendations for **phishing resistant MFA solutions** in cases where Personal Identity Verification (PIV) card access is not possible or practical.
- The Zero Trust (ZT) Engineering team is building the strategy for assessing the projects supporting the **Network pillar** and how they will advance ZT across the Enterprise. Initial projects include Network Mapping, Endpoint Management, Cloud Assessment Security Broker, Network Segmentation, Active Directory Redesign, Privileged Access Management, and the Transport Only Network upgrade.

Narrative – FY 2023 Q2 (continued)

Some capabilities at the enterprise will be operating at the advanced maturity level. Therefore, the Department intends to have some functions available by the end of FY2023. Zero Trust is an ongoing process and the efforts to fully mature across all pillars and functions will be a multi-year effort. The various ZT functions/activities outlined within the CISA ZT Maturity Model will be operating between initial operating capability (IOC) level and full operating capability (FOC) level.

Progress is being made across all zero trust pillars, but complexities across organizational boundaries have delayed milestone completions targeted for completion by the end of FY23 Q3. More work is being done to align schedules for Enterprise service updates with individual system roadmaps.

Data accuracy & reliability

Definitions

Accuracy

- High – Very few false negatives and few false positives. Data in the system is correct and up to date.
- Medium – Acceptable number of false positives and negatives. The data in the system is useful in aggregate and reliable when combined with other systems.
- Low – Unacceptable false positives and negatives. The data cannot be trusted.

Reliability

- High – Data includes all enterprise objects of one type in one view. Data does not rely on a trust relationship, for example a software agent or manual data entry.
- Medium – Data is nearly complete. Manual entry or software agents have been verified.
- Low – Partial view of the enterprise.

Data accuracy & reliability

Data Source on	Accuracy (see definitions slide)	Reliability (see definitions slide)	Notes
Network Management Tools	High	High	These tools monitor network health, security, and configuration across the enterprise.
Configuration Master Data Base (CMDB)	High	Low	Commercial off the shelf software catalogs all assets on the network. Requires trusted connection to an agent. Partial implementation and capture of data on October 1, 2021.
Authority to Operate Tracking (ATO) System	High	Med	Catalog of FISMA applications and their ATO status
Capital planning database	Med	Med	Database of IT investments
FISMA Reporting	High	Med	Department of Homeland Security (DHS) quarterly Cybersecurity Risk Management Assessment report

Additional information

Contributing Programs

Organizations:

- Bureau of Information Resource Management (IRM); CIO Council (Leadership Stakeholders across the Department of State)

Program Activities:

- Development of Zero Trust enterprise policies and standards
- Development of Zero Trust enterprise solution architecture

Regulations:

- Executive Order (EO) 14028: *Improving Nation's Cybersecurity*; Executive Order (EO) 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*; Federal Information Security Management Act (FISMA);

Policies:

- 5 FAM and 12 FAM

Other Federal Activities:

- OMB memorandum M-22-09, President's Management Agenda (PMA), CISA's Zero Trust Maturity Model, DoD's Zero Trust Framework

Stakeholder / Congressional Consultations

- IRM regularly reports status to OMB and, upon request, briefs Senate and House committees.