Agency Priority Goal | Action Plan | FY 2023 – Q3

Cybersecurity Agency Priority Goal (APG)

Goal Leader(s):

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

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 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

MORE GUIDANCE

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	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 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.

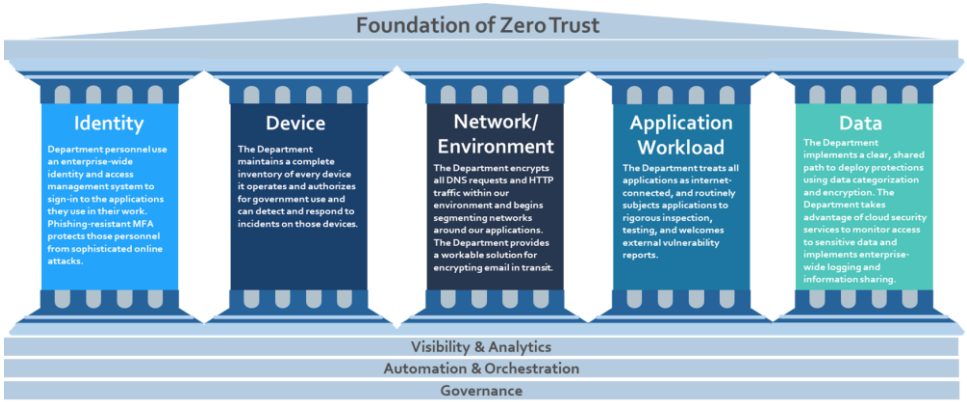
Zero Trust Pillars

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.

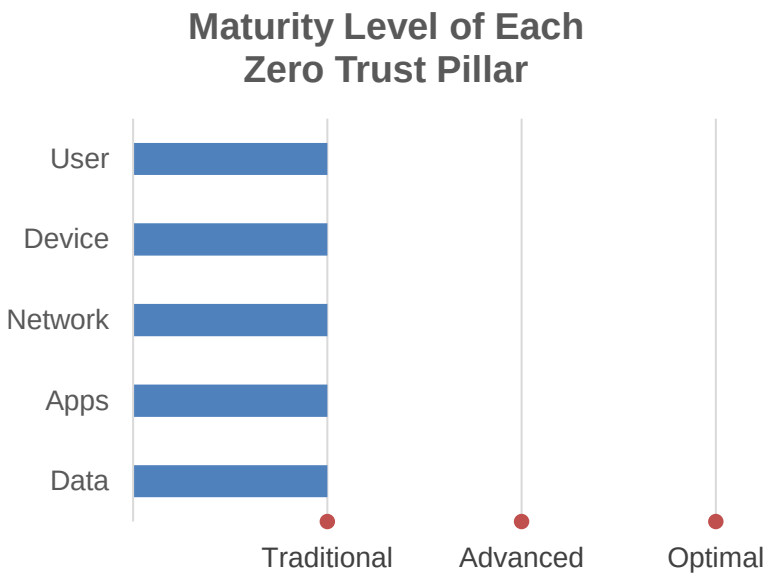
Optimal – fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, centralized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

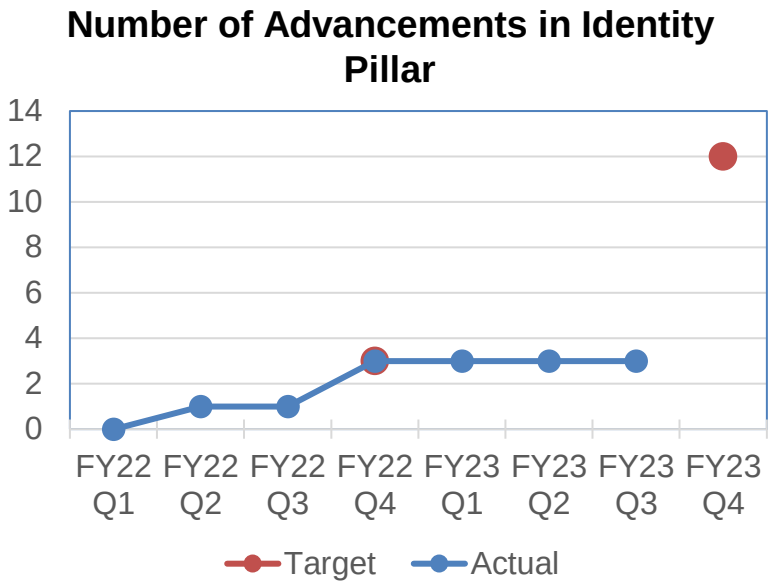
Key indicators

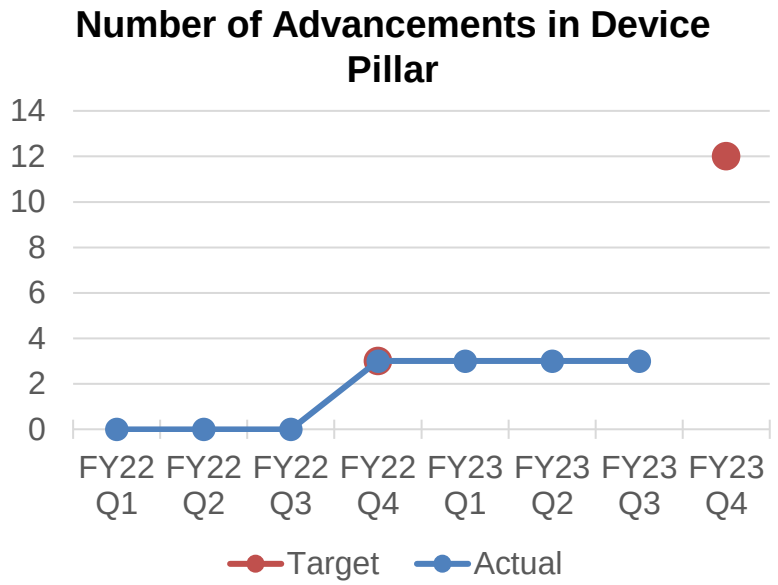
Indicator Title	Current Value	FY 2022 Target	FY 2023 Target
Zero Trust Maturity			
Number of individual pillars advancing to the “Advanced” maturity level each year. (Traditional, Advanced, Optimal)*	0	2	5
Number of activities advanced within Pillar 1 – Identity	3	3	12
Number of activities advanced within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

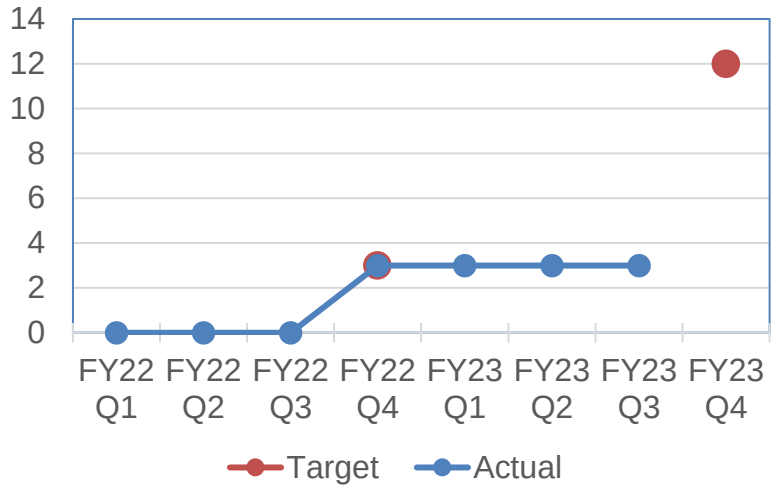




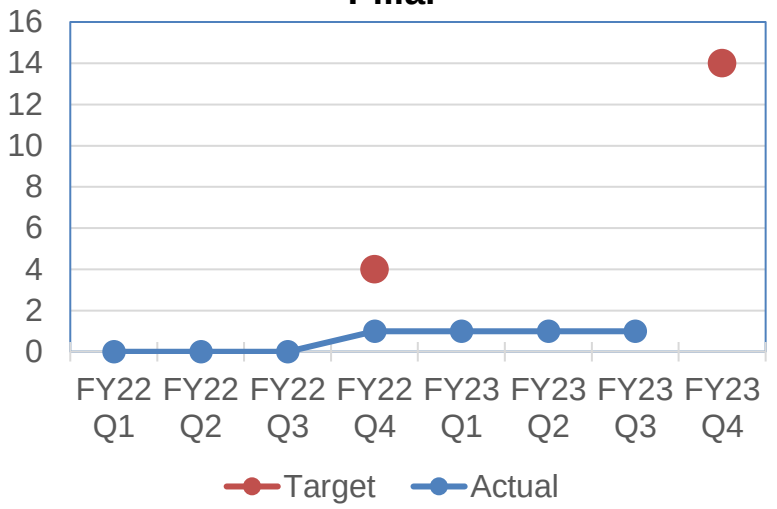


Key indicators

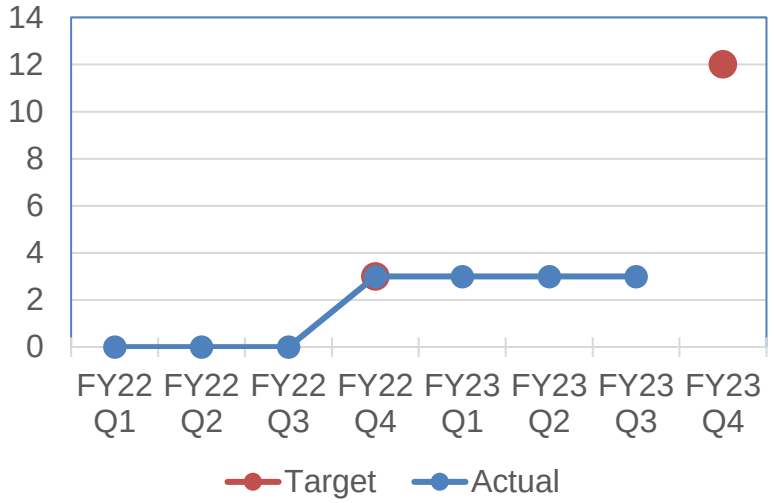
Number of Advancements in Network Pillar



Number of Advancements in Application Pillar



Number of Advancements in Data Pillar



Key milestones

Milestone Summary			
Key Milestone*	**Milestone Due Date** *[e.g., Q2, FY 2017]*	**Milestone Status** *[e.g., Complete, On-Track, Missed, Ongoing]*	**Comments** *[Provide discussion of Progress, changes from last update, Anticipated Barriers or other Issues Related to Milestone Completion]*
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	The Department leverages PIV cards for phishing-resistant MFA while partnering with other government agencies to test and certify Okta FastPass as additional option by October 2023.

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

Key milestones

Milestone Summary			
Key Milestone*	**Milestone Due Date** *[e.g., Q2, FY 2017]*	**Milestone Status** *[e.g., Complete, On-Track, Missed]*	**Comments** *[Provide discussion of Progress, changes from last update, Anticipated Barriers or other Issues Related to Milestone Completion]*
Remove from all systems password policies that require special characters and regular password rotation.	Q2, FY 2023	Missed	As with last quarter, multi-factor authentication is being deployed across the Department but is not yet complete. Once password policies and Directive Type Memos (DTMs) have been drafted, implementation actions can be taken, and policy language can be added 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	Missed	System has been identified. Currently, working with SAFE system owners and stakeholders to identify risks and develop an implementation plan for enterprise services by October 2023.

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

Narrative – FY 2023 Q3

Collaboration continues with key stakeholders to implement Zero Trust capabilities across the Department. The Department has widened its focus beyond the Identity Pillar and has now begun efforts to assess and implement Zero Trust principles and practices to the Network, Device, and Data Pillars as well. The following activities were addressed to incrementally advance Zero Trust capabilities:

- **Identity Pillar:** The Department implemented **Multi-Factor Authentication (MFA) using OKTA as the Enterprise Identity Provider** for a total of 463 applications. We continue to extend identity capabilities by adding Signal-Sign-On (SSO) for all systems, automating user governance, and standardizing Privileged Access Management (PAM).

  Completed the initial assessment for the **Cyber Engineering Identity Pillar Planning pilot**, and currently developing detailed implementation plans for the five mission critical systems surveyed to employ Enterprise Identity Capabilities at the Advanced maturity level on the systems, in accordance with CISA Zero Trust Maturity Model.

- **Network Pillar**: The Department completed an **Initial Network Assessment Report** which provided an in-depth view of the multiple networks and Enterprise capabilities currently in use by the Department. Further deep dives are scheduled to be provided in 30-day sprints. Currently investigating Non-Enterprise Network (NEN) consolidation and encryption across all network layers.

Narrative – FY 2023 Q3 (continued)

- **Data and Device Pillars:** Working to complete initial assessments for both pillar capabilities, while still meeting with stakeholders to identify and understand current implementation projects and uncover areas for advancement. During these initial pillar assessments, the Department identified relationships and dependencies that were shared across multiple pillars and functions. As a result, the Department has established a **Cross Pillar Working Group** to ensure that stakeholders working on multiple pillar efforts are able to easily communicate and work together to overcome potential issues that arise with cross-pillar initiatives.

The path to Zero Trust is not linear; as we assess the Department's current state and implement new technology across the enterprise, we are uncovering dependencies and complexities that we must further evaluate in order to achieve the advanced maturity level as defined in the CISA ZT Maturity Model. Our current progress is delayed due to these complexities, but we are making progress to achieve the Advanced Maturity level across the five pillars. We are planning to continue the journey as we establish our FY 2024 - 2025 APG goals.

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	Low	Low	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