SAF/CN
Publication: 14 DEC 2023

DAF ENTERPRISE ZERO TRUST ROADMAP | COVER PAGE

Adapting and Modernizing DAF's Cybersecurity Architecture to enhance security and mission performance for the warfighter

Increasing competition on the global stage necessitates a more modern security architecture to protect our critical business and mission systems and promote digital readiness. The DAF intends to implement a Zero Trust (ZT) security posture in alignment with the DoD Zero Trust Strategy.

Implementing Zero Trust Will Advance the CIO Strategic Priorities and Address the DoD ZT Mandate

Implementing a Zero Trust architecture touches many areas of our IT delivery ecosystem and encapsulates everything DAF delivers.

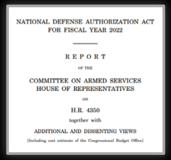
CIO Strategy LOEs

The DAF CIO Public Strategy was published in September of 2022 and introduced six primary Lines of Effort (LOEs) to support DAF's IT priorities through FY23-FY28.

The LOEs directly address the needs of DAF's emerging strategic and technological environment. The implementation of Zero Trust is critical to the advancement of the three LOEs highlighted below.

1. Accelerate Cloud Adoption
2. **Future of Cybersecurity**
3. Workforce
4. IT Portfolio Management
5. **Excellence in Core IT & Mission Enabling Services**
6. **Data and AI**

September 2021



NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2022

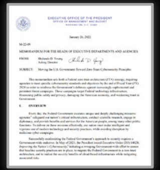
REPORT OF THE COMMITTEE ON ARMED SERVICES HOUSE OF REPRESENTATIVES ON H.R. 4350 together with ADDITIONAL AND DISSENTING VIEWS

[Including cost estimate of the Congressional Budget Office]

Sec. 1528 of NDAA for FY22

Instructed DoD CIO and US Cyber Command to jointly develop an implementation strategy for zero trust architecture across DoD's information network.

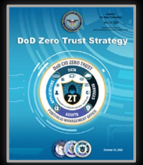
January 2022



OMB Policy Memo 22-09

Provided strategic guidance to departments and agencies and directed the achievement of specific zero trust security goals by the end of FY24.

October 2022



DoD Zero Trust Strategy

DoD Zero Trust Strategy

*DoD published a ZT Strategy on October 21, 2022, defining an approach for agencies to adopt and accelerate toward a modern ZT architecture. The DoD ZT Strategy requires all agencies to adopt, integrate, and operationalize baseline capabilities across **7 DoD-defined ZT Pillars by FY27**.*

What is the Current State of DAF Zero Trust?

USER
Inconsistent and inadequate authentication and access management controls

DATA
Leveraging data brokers and platforms to provide policy enforcement around granular data pieces

VISIBILITY & ANALYTICS
Need for integrating application-layer enforcement events with operational tools and processes

AUTOMATION & ORCHESTRATION
API support is nascent as early data automation lacks standardization and expansion

APPLICATION & WORKLOADS
Application protections are inconsistently applied across the enterprise

NETWORK & ENVIRONMENT
VPN as the primary tool to secure remote access, combined with legacy network practices

DEVICE
Device management is decentralized and disconnected from authorization decisions

What is the Current State of Zero Trust Execution?

ACC/A60 stood up the DAF ZT FMO to facilitate ZT implementation efforts across-DAF following the publication of the DAF Enterprise ZT Roadmap v.1.0 in February 2023.

BUILT THE INFRASTRUCTURE

- ✓ Drafted ZT I-Plan IAW Roadmap and DoD's Strategy
- ✓ Pin-pointed funding disconnects across DAF ZT future solutioning
- ✓ Built real-time, streamlined task management system
- ✓ Submitted I-Plan to DoD for final review

CENTRALIZED ZT EXECUTION EFFORTS

- ✓ Aligned ZT Roadmap Milestones to DoD-mandated Capabilities
- ✓ Assigned EIT stakeholders across-DAF to champion individual ZT Milestones
- ✓ Hosting weekly ZT Milestone Champion engagement for progress updates
- ✓ Conducting bi-weekly ZT implementation progress report out to Senior Leaders

The DAF Enterprise Zero Trust Roadmap serves as the strategic guide to operationalize Zero Trust and shift DAF away from network-based telemetry and establish an application-centric architecture with homogenized data exchange processes and increased visibility, monitoring, and alerting.

DAF ENTERPRISE ZERO TRUST ROADMAP

Impact to the DAF

- *Disrupt adversaries through enhanced cyber readiness*
- *Increased resilience across all mission areas*
- *Provides rigorous authentication and authorization that takes into account numerous risk factors*

Publication: 14 DEC 2023

Services and Strategic Narratives

User
Deliver a single enterprise ICAM solution serving all communities and environments with enhanced authentication and controls

Data
Integrate data ecosystem and provide support via Enterprise ZT services (e.g., NPEs)

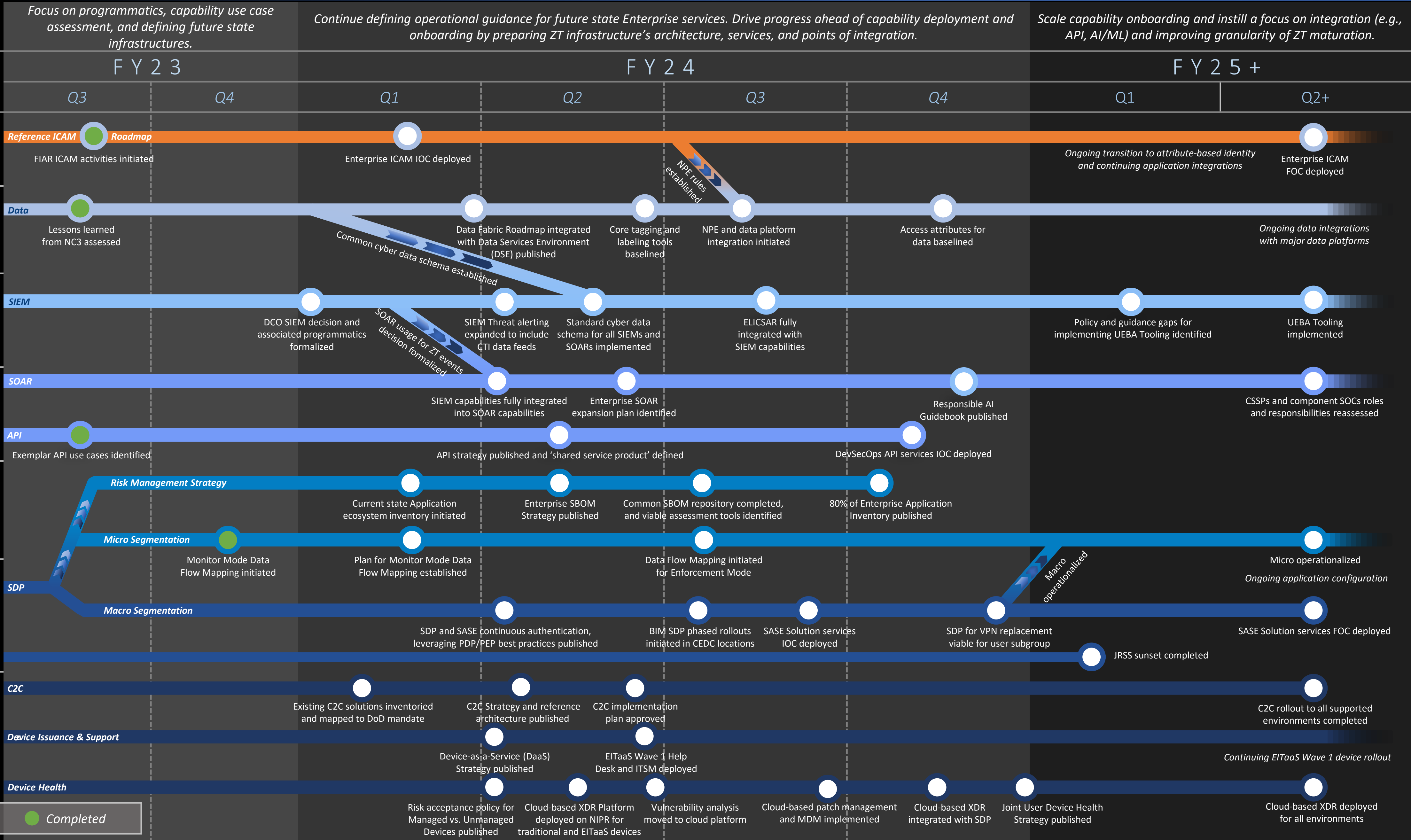
Visibility & Analytics
Enable SIEM to process ZT relevant visibility data and exploiting data that includes application events and user behavior patterns

Automation & Orchestration
Establish SOAR as a major component of operational cybersecurity leverage; support APIs via enterprise services

Application & Workloads
Standardize security control measures across enterprise applications

Network & Environment
Enforce micro segmentation with generally available SASE solution; deploy SDP solution at base level and tailor to applications

Device
Automate and migrate tools to Cloud that manage device health and feed access decisions with Device-as-a-Service (DaaS) rolled out



Focus on programmatics, capability use case assessment, and defining future state infrastructures.

Continue defining operational guidance for future state Enterprise services. Drive progress ahead of capability deployment and onboarding by preparing ZT infrastructure's architecture, services, and points of integration.

Scale capability onboarding and instill a focus on integration (e.g., API, AI/ML) and improving granularity of ZT maturation.

Reference ICAM Roadmap
- FIAR ICAM activities initiated
- Enterprise ICAM IOC deployed
- NPE rules established
- *Ongoing transition to attribute-based identity and continuing application integrations*
- Enterprise ICAM FOC deployed

Data
- Lessons learned from NC3 assessed
- Common cyber data schema established
- Data Fabric Roadmap integrated with Data Services Environment (DSE) published
- Core tagging and labeling tools baselined
- NPE and data platform integration initiated
- Access attributes for data baselined
- *Ongoing data integrations with major data platforms*

SIEM
- DCO SIEM decision and associated programmatics formalized
- SOAR usage for ZT events decision formalized
- SIEM Threat alerting expanded to include CTI data feeds
- Standard cyber data schema for all SIEMs and SOARs implemented
- ELICSAR fully integrated with SIEM capabilities
- Policy and guidance gaps for implementing UEBA Tooling identified
- UEBA Tooling implemented

SOAR
- SIEM capabilities fully integrated into SOAR capabilities
- Enterprise SOAR expansion plan identified
- Responsible AI Guidebook published
- CSSPs and component SOCs roles and responsibilities reassessed

API
- Exemplar API use cases identified
- API strategy published and 'shared service product' defined
- DevSecOps API services IOC deployed

Risk Management Strategy
- Current state Application ecosystem inventory initiated
- Enterprise SBOM Strategy published
- Common SBOM repository completed, and viable assessment tools identified
- 80% of Enterprise Application Inventory published

Micro Segmentation
- Monitor Mode Data Flow Mapping initiated
- Plan for Monitor Mode Data Flow Mapping established
- Data Flow Mapping initiated for Enforcement Mode
- Micro operationalized
- *Ongoing application configuration*

SDP

Macro Segmentation
- SDP and SASE continuous authentication, leveraging PDP/PEP best practices published
- BIM SDP phased rollouts initiated in CEDC locations
- SASE Solution services IOC deployed
- SDP for VPN replacement viable for user subgroup
- Macro operationalized
- SASE Solution services FOC deployed
- JRSS sunset completed

C2C
- Existing C2C solutions inventoried and mapped to DoD mandate
- C2C Strategy and reference architecture published
- C2C implementation plan approved
- C2C rollout to all supported environments completed

Device Issuance & Support
- Device-as-a-Service (DaaS) Strategy published
- EITaaS Wave 1 Help Desk and ITSM deployed
- *Continuing EITaaS Wave 1 device rollout*

Device Health
- Risk acceptance policy for Managed vs. Unmanaged Devices published
- Cloud-based XDR Platform deployed on NIPR for traditional and EITaaS devices
- Vulnerability analysis moved to cloud platform
- Cloud-based patch management and MDM implemented
- Cloud-based XDR integrated with SDP
- Joint User Device Health Strategy published
- Cloud-based XDR deployed for all environments

Legend: ○ *In Progress / To Do* ● *Completed*

SAF/CN
12/14/2023

DAF ENTERPRISE ZERO TRUST ROADMAP

RELEASE NOTES

EDITORIAL NOTES

The SAF initially published the Zero Trust Roadmap in February 2023 and followed up the initial publication with a second release in June 2023. This roadmap update reflects the status of Zero Trust progress as a snapshot in time and will continue to serve as a guide for cross-enterprise adoption and execution.

SAF/CN has engaged with the DAF Zero Trust FMO (out of ACC/A6) to compile real-time adjustments to ensure this update encapsulated progress when viewed against the multi-faceted ZT plan. Changes to Roadmap milestones' timing and language provide an accurate snapshot of projected plans and an increased level of clarity and specificity.

✓ WHAT'S BEEN ACCOMPLISHED?

- ZT FMO submitted the first-ever DAF ZT I-Plan to DoD for final review before it goes to Congress for approval in early 2024
- Initiated FIAR ICAM Activities in preparation for enterprise-wide deployment of the DAF's ICAM solution
- Documented lessons learned from NC3 to inform planning artifacts for DAF-wide ZT Implementation
- Identified exemplar API use cases through extensive workflow mapping and strategic dialogue across various organizations
- Initiated monitor mode data flow mapping and deployed VENs to 300+ servers via micro segmentation PACAF pilot
- Selected Enterprise solution for micro segmentation across NIPR, SIPR, and Cloud One and procured licenses
- Activated EDR in passive mode in 50+ devices with plans to proceed to deploy active mode at pilot bases

IDENTIFIED ROADBLOCKS

IDENTIFIED ROADBLOCK	C2C Scalability Issues Due to Increased Cost and Manpower Shortfalls	Pending SIEM Integration Plan and Architecture	Strong Dependencies on EITaaS Wave 1 Deployment	Unclear Definition of Enterprise ICAM IOC and Associated Funding Disconnects
MITIGATION PLAN	*SAF/CN and ACC/A6 to build reference architecture and increase funding efforts*	*Operational community to formalize platform selection and build associated plan*	*DAF Senior Leaders to continue driving urgency for EITaaS Wave 1 delivery*	*SAF/CN and HNI PEO to deliver ICAM Zero Trust integration plan*

NEXT QUARTER'S PRIORITIES...

- Continue development of DAF Enterprise Zero Trust Strategy, with particular focus on non-EIT systems
- Continue FIAR application migration for ICAM and formalize FOC definition
- Document Comply-to-Connect (C2C) architectural and operational concepts, and drive efforts to resolve disconnects
- Engage Senior Leaders and implementation teams to remove any remaining blockers to EITaaS Wave 1 deployment
- Formalize SIEM solution decision and way forward for SOAR integration
- Initiate XDR solution in active mode and expand number of devices

DAF ENTERPRISE ZERO TRUST ROADMAP | *ACRONYMS AND DEFINITIONS*

SAF/CN
12/14/2023

Acronym/Term	Definition
AI	Artificial Intelligence
API	Application Programming Interface
BIM	Base Infrastructure Modernization
C2C	Comply-to-Connect
CEDC	Component Enterprise Data Center
CSSPs	Cloud Software Service Providers
CTI	Cyber Threat Intelligence
DAF	Department of the Air Force
DaaS	Device-as-a-Service
DCO	Defensive Cyber Operations
DevSecOps	Development, Security, and Operations
DSE	Data Services Environment
EDR	Endpoint Detection and Response
EITaaS	Enterprise Information Technology-as-a-Service
ELICSAR	Enterprise Logging Ingest and Cyber Situational Awareness Refinery
FIAR	Financial Improvement and Audit Readiness
FOC	Full Operational Capability
IAW	In Accordance With
ICAM	Identity, Credential, and Access Management
IOC	Initial Operational Capability

Acronym/Term	Definition
ITSM	Information Technology Service Management
JRSS	Joint Regional Security Stacks
LOE	Level of Effort
MDM	Mobile Device Management
ML	Machine Learning
NC3	Nuclear Command, Control, and Communications
NDAA	National Defense Authorization Act
NIPR	Non-secure Internet Protocol Router
NPE	Non-Person-Entity
PDP/PEP	Policy Decision Point/Policy Enforcement Point
SASE	Secure Access Service Edge
SBOM	Software Bill of Materials
SDP	Software-Defined Perimeter
SIEM	Security Information & Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
UEBA	User and Entity Behavior Activity
VPN	Virtual Private Network
XDR	Extended Detection and Response
ZT	Zero Trust