Department of the Air Force Zero Trust Strategy

Version 1.0

OPR:
DAF CIO

VENICE M. GOODWINE, SES, DAF
Chief Information Officer
Office of the Chief Information Officer

This page intentionally left blank.

Executive Summary

Decades of technological evolution and persistent competitors and adversaries have diminished the relevance and effectiveness of the perimeter-centric cybersecurity model. After years of addressing cyber vulnerabilities, insider threats, and design shortcomings with short-term solutions, the Department of the Air Force (DAF) network has evolved into an operationally complex, technically challenging environment that neither meets the standards of modern Airmen & Guardians, nor the requirements for current and future warfighting environments. Continuing to sustain this security model jeopardizes the ability to preserve its operational effectiveness and lethality.

The Department of Defense (DoD) aims to revolutionize its network-focused defense-in-depth "castle and moat" cybersecurity strategy into one that focuses on individual data as a strategic asset. To achieve this, the DAF must evolve towards a data centric Zero Trust cybersecurity strategy. Zero Trust is a data and application access strategy that assumes all connections, regardless of network origin, come from untrusted sources. Access to each resource is only granted after explicitly requesting, establishing, and continuously re-verifying confidence in the requestor's identity, device, and context of each connection.

This strategy aims to strengthen the DAF's cybersecurity posture and provide to the warfighter assured and secure data access at the speed of war, while simultaneously denying adversary efforts to achieve information dominance. Commanders and individuals will have a choice in how and where they connect. It reduces the number of DAF architectures improving security and promoting interoperability. It unlocks warfighters' access to next-generation, globally connected Combined Joint All-Domain Command & Control (CJADC2) capabilities. This strategy forces malicious cyber actors to treat every connection as a total attack. Under Zero Trust, rather than simply leveraging the success of previous exploits to further gains, malicious actors must find and successfully exploit vulnerabilities in every resource they want to access, improving chances to identify, stop, and successfully respond to these attacks. The Zero Trust effort will also include evolving to dynamic risk management as an essential component of leveraging the advanced technical capabilities to be pursued via this strategy. This evolution includes standardizing on a risk maturity model to measure risk management effectiveness, and shifting from system-based to mission thread-based risk management to complement automated and autonomous prevention, protection, and remediation capabilities. Together, these capabilities accelerate the adoption of next-generation warfare by simplifying digital access, without sacrificing speed or security.

Ultimately, this strategy makes the warfighting changes we need to evolve as a department possible by simplifying access for our Airmen & Guardians and imposing higher costs on our competitors and adversaries. The seven pillars capability elements, and activities, focus DAF resources to align with the DoD Zero Trust Strategy and industry leading Zero Trust models.

<u>Applications and Workloads Goal</u>: *Application-Level Visibility and Control*

<u>Data Goal</u>: *Data As The New Perimeter*

<u>Users Goal</u>: *Right Access, To The Right Entity, For The Right Reason*

<u>Device Goal</u>: *Reduce The Risk Created By Any Single Device*

<u>Network and Environment Goal</u>: *Access To Protected Resources Anytime, Anywhere*

Automation and Orchestration Goal: *Automated Security Responses based on Security Policies*

Visibility and Analytics Goal: *Improve Detection and Reaction Time*

Table of Contents

This page intentionally left blank.

1 Introduction

For decades, the Department of Defense (DoD) has assumed a trusted and permissive operational cyberspace environment. However, in the current and future global security environment, this assumption is no longer valid. Continuing this approach creates significant opportunities for our enemies to gain unimpeded access to data across networks and leaves the DoD poorly postured to compete, deter, and win against swiftly evolving competitors and adversaries and sophisticated cyber threats. Modern opponents to U.S. interests routinely exploit the weaknesses of current perimeter-based network defenses, which over time has led to a diminishing warfare advantage.

Malicious actors will continue capitalizing on this weakness in an era where the Department of the Air Force (DAF) increasingly depends upon secure access to shared, trusted information. In today's technology-constrained environment, the perimeter-centric model also introduces insurmountable inefficiencies to a substandard user experience, where countless threats limit information sharing and mobile access. Instead, Air and Space professionals should be able to leverage modern cloud, mobile, artificial intelligence (AI), and other emerging technologies to dramatically improve both routine productivity and warfighting advantages. To accelerate these necessary changes, the DAF must relentlessly pursue an inherently distrustful strategy fueled by security, simplicity, and accessibility. Collectively, the U.S. military and commercial industry are converging on Zero Trust as the transformative cybersecurity construct to meet this need. "The Zero Trust effort will also include evolving to dynamic risk management as an essential component of leveraging the advanced technical capabilities to be pursued via this strategy. This evolution includes standardizing on a risk maturity model to measure risk management effectiveness, and shifting from system-based to mission thread-based risk management to complement automated and autonomous prevention, protection, and remediation capabilities."

In February of 2022, the Secretary of the Air Force (SECAF) defined an operational imperative to "identify the extent of gaps in cybersecurity […] and close the most serious" in order to "transition to a wartime posture against a peer competitor".[1] This imperative is the SECAF's answer to the DoD's 2019 Digital Modernization Strategy, the 12 May 2021 Executive Order (EO) on Improving the Nation's Cybersecurity, the Office of Management and Budget's (OMB) M-22-09 Zero Trust directive, the 2022 National Security Memo-8, and the 2022 National Defense Authorization Act.[2] In addition, this strategy is tied to the DAF CIO Public Strategy LOE 2 Cybersecurity, to create and continuously enhance a secure and resilient digital environment that protects our data and critical assets from adversaries. Each of these directives seeks to revolutionize our cybersecurity posture, transforming the network-focused, defense-in-depth "castle and moat" strategy of today into a Zero Trust Architecture that focuses on data as a strategic asset.

Zero Trust is not a capability you can purchase off the shelf. Zero Trust is a data and application access strategy that assumes all connections come from untrusted sources. Access is only granted after explicitly requesting, establishing, and continuously re-verifying enough confidence in the

[1] Priority Department of the Air Force (DAF) Operational Imperatives, 7 Feb 2022

[2] DoD Digital Modernization Strategy, 12 Jul 2019; Executive Order 14028: Improving the Nation's Cybersecurity, 12 May 2021; OMB, M-22-09, 26 Jan 2022; NSM-8, 19 Jan 2022; U.S. National Defense Authorization Act for Fiscal Year 2022, Sect 1528: Zero Trust Strategy, Principles, Model Architecture, and Implementation Phase, 27 Dec 2021

user's identity, device, and context of each connection. The guiding principles of Zero Trust require us to *Assume Breach; Never Trust, Always Verify; and Implement Least Privilege Access*.[3]

1.1 Purpose

A Zero Trust culture lays the rock-solid digital foundation that connects all Air and Space Force members across a trusted digital force. DAF must institutionalize a Zero Trust culture in order to enact the warfighting changes necessary to recapture our warfare advantage and evolve to meet the operational imperatives of today. This strategy describes the concept for establishing a DAF Zero Trust capability, delivering a future cybersecurity posture that simplifies access for our Airmen & Guardians and imposes higher costs on our competitors and adversaries, to accelerate the adoption of next-generation warfare technologies. This vision requires a scalable, resilient, auditable, globally accessible, and defendable framework centered on the protection of our most critical, mission-essential data, applications, assets, and services (DAAS), to prevent, detect, respond to, and recover from malicious cyber activity in multiple operating environments.

1.2 Scope

This strategy aligns with the DoD Zero Trust Strategy scope and includes the range of activities described. Section headings will be annotated for those directly tied to a DoD element. This strategy applies to the data security of all DAF portions of the DoD Unclassified, Secret, Collateral Top Secret, National Security Systems (NSS), and US owned releasable networks, systems, and operational technologies (OT) under the SECAF authority, including the Special Access Program (SAP) element unless explicitly excluded in policy,.[4] Information systems include those owned and operated by, or on behalf of the DAF, including systems hosted at DAF data centers, mission systems/OT systems, stand-alone systems, contractor-operated systems at cleared defense contractor locations and on the AF Information Network (AFIN), cloud-hosted systems, and systems hosted on closed operational or development networks with no AFIN connection. It includes all entities accessing the systems.[5]

As the DAF Zero Trust construct evolves, the need for separate classification networks will also evolve. Outside research and development, Zero Trust principles are not uniquely configurable to individual environments and are agnostic to data classification. Therefore, DAF envisions a fully mature Zero Trust environment, where solutions could collapse multiple network fabrics (e.g., NIPR, SIPR, JWICS, and SAP) into one. In this construct, only the data and applications make up what we know as the different network fabrics today. Each user, device, and context attribute set may be granted access to each authorized connection, rather than a specific network fabric.

Additionally, this strategy requires whole of government interoperability between DAF networked systems and mission partner systems, to include other DoD Service Components, the Intelligence Community (IC), U.S. Government Agencies, mission partners, and allies. However, it also requires strong partnership and flexibility, as each specific organization progresses along its own Zero Trust maturity. DAF, through respective assigned authorizing officials, will

[3] NIST Special Publication 800-207, Zero Trust Architecture, 11 Aug 2020

[4] While the strategic principles of this document include SAP systems, the SAP community will execute their own I-Plan.

[5] Includes endpoints (e.g., server, PC, laptop, phone, tablet, mobile, and virtual machines), computing services, and digital identities consisting of attributes that make up person and non-person entities (NPE) (i.e., service accounts, machine-to-machine, application programming interface (API) calls, and Internet of Things (IoT))

specifically coordinate all efforts to integrate Zero Trust into any DAF-IC, joint, and Mission Partner Environment shared network fabrics.

2 Evolving from Network-Centric to Data-Centric Security

2.1 Current State

For decades, the United States' national security interests assumed a trusted and permissive operational cyberspace environment. However, the United States now faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, national security, and ultimately the American people's way of life. The traditional and prevailing perimeter-centric cybersecurity paradigm to counter this threat requires multiple, overlapping, broad, and complex security capabilities at the edge of an enterprise network, for each level of classification – "The Castle & Moat". Today, a growing technological evolution and persistent malicious cyber actors diminished the relevance and effectiveness of this model.

The DAF has become hyper-focused on defensive cyberspace measures and capabilities at the perimeter, aiming to keep bad actors out. This focus deprioritized defensive capabilities and visibility for the internal network, which created an interior environment that implicitly granted trust, based on location, rather than validated assertions. Additionally, in this model, mission system owners implement "hands off," compliance-based security, relying on cybersecurity service providers to meet their needs. However, competitors, adversaries, and insider threats have rapidly evolved their cyber capabilities, enabling them to further exploit the access control and device management weaknesses of this approach. These malicious actors have also enjoyed unimpeded freedom of maneuver in cyberspace. Over time, this has led to an increasingly contested operational environment and a diminishing U.S. military advantage.

Connecting the "military Internet of Things (IoT)" promised by CJADC2, to this environment creates an even more highly connected and globally accessible attack surface. Cyber threats in this environment could easily amplify the impacts of exploiting a single cyber vulnerability across this entire system of systems, into insidious all-domain, warfighting effects. In an era where the DAF and its partners must increasingly rely upon secure access to trusted, shared data, particularly in denied, degraded, intermittent, and limited (DDIL) environments, malicious cyber actors will continue to target and capitalize on this deficiency, leaving the DAF poorly postured to compete, deter, and win.

The abrupt COVID-19 pandemic also forced personnel into extended remote work scenarios that rapidly overwhelmed existing remote access technologies. This unprecedented event, along with the promise of secure, efficient, low cost, and globally accessible data centers fueled an explosion of cloud technology adoption, and Virtual Private Networks (VPN) and virtualized desktop infrastructure. Together, these technologies extended secure access to a growing number of protected apps and data outside of the perimeter. However, while it solved critically needed access to enterprise resources, it came with a less relevant perimeter and larger attack surface.

After years of addressing these cyber vulnerabilities and design deficiencies with short-term, bolt-on solutions, the DAF network has devolved into an operationally complex, functionally stove piped and technically challenged environment. Ultimately, this network no longer meets the standards of modern Airmen & Guardians, nor the requirements for the future warfighting environment. Continuing to sustain this model jeopardizes DAF's ability to preserve its operational effectiveness and lethality.

2.2 End State

The DAF must adopt a continuously evolving strategy to meet the challenges of the current environment and recapture its warfighting advantage. This strategy should outline a progressive, but uninterrupted, transition from network-centric to both mission and data-centric defensive postures which never trusts and always verifies.

This transition gives commanders and individuals a choice in how and where they connect for more productive daily business and warfighting operations. By treating data as the new perimeter, the cyber domain can deliver access to protected resources anytime, anywhere, and under the harshest DDIL conditions. This operational environment also sets the right conditions to safely collapse the myriad DAF warfighting network environments into one, connecting people and processes, partners, and allies more easily.

Achieving application-level visibility, control, analytics, and governance across every endpoint reduces the overall risk from any single device, while cloaking and micro-segmentation simultaneously shrink the attack surface and impair an adversary's lateral movement and privilege escalation. Security stack design drives strong integration among functional communities and development, security, and operations (DevSecOps) environment, ensuring security is always "baked in" from inception. Under this network-agnostic paradigm, defensive cyberspace operators, administrators, data stewards, and mission owners all share continuous endpoint confidence and identity authorization, authentication and monitoring responsibilities over their data and resources.[6] These security services are delivered as automated, highly visible, strongly auditable, and are validated prior to establishing every connection – ensuring the right access, to the right entity, for the right reason.

Under Zero Trust, rather than simply leveraging the success of previous exploits to further gains, malicious actors must find and successfully exploit vulnerabilities in every resource they want to access, improving chances to identify, stop, and successfully respond to these attacks. This forces malicious actors to treat every connection as a total attack, imposing substantial time, resource, and payoff costs on their decision to attack. While no single approach can prevent every conceivable attack, this paradigm reduces the risk of compromise and dramatically mitigates the impact of any successful attack.

Finally, this transition safely unlocks warfighters' access to the next-generation, globally connected CJADC2 capabilities that are changing the face of future warfare and generating powerful operational effects and lethality across all mission areas. Ultimately, this future cybersecurity posture simplifies access for our Airmen & Guardians, allowing the DAF to rapidly transition to a persistent wartime posture, ready to compete, deter, and win against a peer competitor in the future warfighting environment.

[6] Mission owner - The OSD or DoD Component having responsibility for the execution of all, or part of a mission assigned by statute or the Secretary of Defense. (DODD 3020.40 – Mission Assurance, 11 Sep 2018).

3 Strategic Goals and Objectives

Inspired by industry-leading models and tied to the DoD Zero Trust Strategy, this vision matures across seven pillars.[7] Each pillar integrates strong governance, continuous visibility and analytics, and robust automation and orchestration as critical enablers, throughout their maturity. The DoD's 7-pillar Zero Trust model addresses these enablers as individual pillars.[8] Dynamic risk management objectives will be described as cross-cutting objectives affecting all pillars. Each pillar matures at its own pace, while also interconnecting with each other:

- Objective #1: Applications and Workloads: Application-Level Visibility & Control
- Objective #2: Data: Data As The New Perimeter
- Objective #3: User: Right Access, To The Right Entity, For The Right Reason
- Objective #4: Devices: Reduce The Risk Created By Any Single Device
- Objective #5: Network and Environment: Access To Protected Resources Anytime, Anywhere
- Objective #6: Automation and Orchestration: Automated Security Responses based on Security Policies
- Objective #7: Visibility and Analytics: Improve Detection and Reaction Time

At a baseline maturity, DAF focuses on security and access – through direct cloud access, software defined perimeters, dynamic access control policies, and datacenter segmentation. At an intermediate maturity, DAF moves toward automated management – through CAC and non-CAC multi-factor authentication, cloud-native management, control and access, basic data protection, and more granular attribute, policy, and risk-adaptive-based access controls. At advanced maturity, focus shifts to include non-IP-based systems/control systems and cyber operations integration – distributed and resilient digital assets and a command-centric cyber operations tempo.

3.1 Objective #1: Applications and Workloads: Application-Level Visibility and Control

To improve our mission effectiveness, the DAF must prioritize application and resource availability to warfighters, while cloaking them from malicious actors. Under a Zero Trust model, combining authentication and authorization of identities, devices, and context-based attributes helps derive confidence for graduated resource-access decisions. Adopting a principle of least privilege in this model further reduces application compromise, while providing direct access to warfighters, mission partners, and allies. Together, these capabilities impair lateral movement and privilege escalation, mitigating the impact of any successful malicious cyber activity.

[7] DoD Zero Trust Strategy dated 7 Nov 22 (https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf), 18.
[8] Ibid

3.1.1 Objective #1.1: Continuous Application Discovery

In order to control access and visibility to applications, preventing back doors, DAF must discover and map all current application activity on the AFIN, as a foundational and ongoing mission in order to identify legacy capabilities and tools, and prioritize modernization efforts. Foremost, this requires strong governance between cyber operation units and mission owners, as critical partners. While initial efforts may be manual, DAF must evolve to a real-time, automated, and domain less visibility and analytics capability available for universal consumption. Maps to DoD ZT Capability 3.1

3.1.2 Objective #1.2: On-Board Applications and Mission Owners to Zero Trust

A critical objective going forward, managing every application and mission partnership requires clear policy, procedures, and tools. DAF must define the evolving roles, responsibilities, and expectations for DAF cyber operators, as well as data stewards & mission owners for migrating into this new paradigm. It must address new and legacy applications - identifying and prioritizing which applications will and will not on-board. Many applications will need both technical and business process re-engineering to adopt better security practices. Any on-boarding process must also crucially identify mission owners' current and future access attribute requirements (e.g., users, devices, and context) recognizing automating any part of this process will drastically accelerate this goal's maturity.

3.1.3 Objective #1.3: Tightly Control Application Visibility and Access

In order to mitigate the impact of any successful attack and achieve application-level control, DAF must implement centralized application permissions and control. Transitioning to attribute-based access control will prevent applications from query and provides access only to authorized and authenticated warfighters, mission partners, and allies. Creating micro perimeters around data, applications, assets, and services (DAAS) based on criticality. Enforce network segmentation. Encrypting data at rest and in transit. Additionally blocking non authorized users and devices from the appropriate application. Once fully automated, we need to work towards streamlining and eventual elimination of the DD Form 2875 process, incorporating the many known workflows. These workflows can be applied and enforced on Software Defined Perimeters (SDP) during on-boarding. Mission owners will maintain these rulesets, along with continuous, Machine Learning (ML) and AI-driven behavioral analytics to monitor the application throughout its lifecycle. Maps to DoD ZT Capability 1.2.

3.2 Objective #2: Data: Data As The New Perimeter

The future of information dominance depends on the quality, visibility, accessibility, understandability, linkages, trustworthiness, interoperability, and security (VAULT-IS), of data as a strategic asset. To transform how the DAF protects and defends resources, in line with the DAF Implementation Plan of the DoD Data Strategy[9], DAF must extend the protect surface by defining data, down to the cellular level, as the new perimeter and adopting dynamic data tagging, labeling and encryption technology that empowers data stewards and consumers, and

[9] Department of Air Force Implementation Plan of the DoD Data Strategy dated Feb 21.

assures access from anywhere, anytime. Together, this provides the potential to collapse the number of DAF warfighting environments.

3.2.1 Objective #2.1: Continuous Data Discovery

In order to control access and visibility to prioritized business and mission data, preventing any back doors, DAF must first discover all data on the AFIN, including newly created data, as a foundational and ongoing mission. Foremost, this effort requires strong governance between cyberspace operation units, mission owners and data stewards, as critical partners. While initial efforts may be manual or semi-automated, DAF must evolve this into a real-time, automated visibility and analytics capability, available for DoD or DAF consumption and managed through the data lifecycle. Maps to DoD ZT Capability Maps to DoD ZT Capability 4.2 and 4.4.

3.2.2 Objective #2.2: Implement and Govern Continuous Tagging As Data is Created

Managing all data and mission partnerships requires clear policy, procedures, and tools. DAF must define the evolving roles, responsibilities, and expectations for the DAF Chief Data and AI Office (CDAO), 16 AF organizations and operators, as well as mission owners and information and data stewards, in line with a DAF Data I-Plan. It must address which data is critical and define initial, manual, or semi-automated data tagging & auditing processes to start today, while working towards a ML and AI-driven process. Policies must include governance structures, defining how to tag data, how to share, who has stewardship of certain types of data, minimum data tagging and labeling standards, as well as human audit requirements. Crucially, mission owners & data stewards must identify access attribute requirements (e.g., users, devices, and context). All newly created data must adhere to these processes, but DAF must also address all existing data. Maps to DoD ZT Capability 4.3.

3.2.3 Objective #2.3: Tightly Control Data Visibility & Access

To mitigate the impact of successful attacks & achieve data-level control, DAF must implement strong role, labeling, and attribute-based access controls, based on the discovered and tagged data access attribute requirements. Implementing least privilege provides data privacy and provides access only to authorized and authenticated requests. Once fully automated, these access rules can be applied and enforced on SDPs as data is created. Mission owners & data stewards will maintain these rulesets, throughout the data lifecycle. Maps to DoD ZT Capability 4.7.

3.2.4 Objective #2.4: Implement Data Loss Prevention Analytics

Treating data as strategic assets requires strong protection and orchestration, throughout its lifecycle. DAF must redefine and implement data loss prevention techniques through strong encryption in transit and at rest. These capabilities must be integrated from first data exposure throughout the data lifecycle to facilitate governance over critical mission data and their associated continuous data monitoring missions. Maps to DoD ZT Capability 4.6.

3.3 Objective #3: Users: Right Access, To The Right Entity, For The Right Reason

A unified, reliable, and federated identity model is fundamental to DAF Zero Trust. Federation is essential as it simplifies process for users to access multiple systems of services, increasing security, improving efficiency, while enhancing interoperability. Evolving into a continuous authorization, authentication and monitoring approach, DAF Identity, Credential, and Access Management (ICAM) capabilities empower Air & Space professionals, partners, and allies with seamless and secure, user-friendly access to resources. Strong governance, automated authorization services, and support for modern authentication tools, protocols, and standards ensure the right people and systems have the right level of access to appropriate resources. Continuous monitoring and analytics drive risk assessments that revoke access, when needed.

3.3.1 Objective #3.1: Enforce Enterprise Access and Policy Management Services

To save Airmen and Guardians time with faster access request responses, the DAF must evolve to balance security and usability via centralized dynamic role and attribute-based access. DAF will implement centralized access management to automate and audit account provisioning, de-provisioning, and privileged access management, reducing mission risk exposure. DAF will also implement access management, leveraging data tagging, labeling, policy enforcement/decision points (PEP/PDP) and SDPs, providing authorized identities lower-risk, on-demand access to resources anytime, anywhere. PEP/PDP's will carry out or enforce all access policy decisions. Maps to DoD ZT Capability 1.2 and 1.7.

3.3.2 Objective #3.2: Enable Universal Multi-Factor Authentication

In order to deliver an improved user experience, the DAF must eliminate the weakness of username and passwords and allow multiple DoD-approved authenticators (e.g., hardware tokens and mobile authenticators), that support a wide range of users, devices, partners, security, and access levels across a spectrum of mission environments and scenarios (e.g., airborne, terrestrial, etc.). The DAF will also deliver a public-facing, self-service, enterprise ICAM identity interface where military, retirees, dependents, and partners can map additional authenticators to their identity. Maps to DoD ZT Capability 1.3.

3.3.3 Objective #3.3: Standardize Continuous Authentication and Authorization

Knowing who or what is accessing DAF resources requires strong governance, providing the programmatic oversight, as well as technical policy development and enforcement. Adopting and automating enforcement of ICAM policies and standards provides a uniform security posture, minimizes risk, and realizes manpower savings through risk-informed access decisions across the enterprise. Continuously monitoring and auditing ICAM events, through AI and ML analytics, revolutionizes the DAF approach to cybersecurity for an agile and resilient defense posture - ready to revoke access when necessary. Maps to DoD ZT Capability 1.8.

3.4 Objective #4: Endpoint Devices: Reduce The Risk Created By Any Single Device

Endpoint devices (e.g., server, PC, laptop, phone, controllers, and tablet), of the future must mature to autonomously protect, detect, and respond to cyber threats. This begins with ensuring least privilege access to endpoint devices and proper Identity and Access Management, continuous discovery of endpoints, assessment of security suitability, determination of acceptability to connect, ongoing continuous monitoring reporting of results, ensuring data is encrypted both at rest and in transit, as well as proper use of firewalls, intrusion detection systems and other measures to protect the network that the endpoint devices are connected to.

From this, policy decision points may derive confidence to make role and attribute-based access decisions. The DAF must adopt centralized, platform-agnostic endpoint health management services that unleash warfighters to execute their mission from the most capable device that meets their needs. While no approach prevents every attack, this reduces the risk of compromise and mitigates the impact of any successful attack.

3.4.1 Objective #4.1: Continuous Hardware and Software Discovery

In order to enforce endpoint compliance and prevent back doors, DAF must first discover connected hardware, software, and NPEs operating on the AFIN, leveraging strong, certificate-based, device identities, as a foundational and ongoing mission. Foremost, this effort requires strong governance between cyberspace operation units and mission and system owners, as critical partners. While initial efforts may be manual, DAF must evolve this into a real-time, automated capability, available for universal consumption. Maps to DoD ZT Capability 2.1, 2.2, and 2.6.

3.4.2 Objective #4.2: Enforce Endpoint Asset Compliance

In order to reduce the risk of compromise, DAF application and data stewards must establish and enforce clear patching and policy standards for both managed and unmanaged devices. Efforts should evolve endpoint security and management from single, comply-to-connect decisions (connect/quarantine/no connect) to continuous monitoring procedures which auto-remediate managed and unmanaged devices. Solutions must also yield confidence attributes, which mission owners and data stewards can leverage for graduated access decisions. Advanced maturity must enforce the baseline or deny access through hybrid-cloud solutions, allowing efficient access, no matter the location or DDIL conditions. Maps to DoD ZT Capability 2.2, 2.3.

3.4.3 Objective #4.3: Create a Domain less Environment

Currently, DAF employs single-vendor domain controllers (DC), which require connections to every device on the AFNET domain. The DAF supports two or more DCs at over 180 DAF sites, leaving adversaries over 360 attack vectors to reach the entire department. In order to mitigate the impact of any successful attack, the DAF must eliminate as much as possible, the internal trust, inherent to the concept of a domain. To achieve this, all endpoints must be removed from AFIN DCs – laptops, mobile, servers, etc. Under this paradigm, resource access becomes truly network agnostic, relying only on identity, client health, and context attributes for access decisions. Maps to DoD ZT Capability 2.1, 2.3, 2.5, and 2.6.

3.4.4 Objective #4.4: Continuous Threat Detection and Response

In order to impose further costs on adversaries, DAF must also evolve endpoint protection and a security operation center (SOC) concept to cloud-based, automated endpoint/extended detection and responses (EDR/XDR) for aggregated, context-driven analysis across the AFIN. Combined with AI and ML-driven security orchestration, automation, and response (SOAR) capabilities, operators can fuse real-time data visibility and multi-source intelligence for faster, more effective threat responses. Maps to DoD ZT Capability 2.6, and 2.7.

3.5 Objective #5: Network and Environment: Access To Protected Resources Anytime, Anywhere

Zero Trust assumes the network is untrusted and potentially hostile, shifting the security monitoring and protection focus to data, users, and endpoints. Adopting Software Defined Perimeter (SDP) enables remote, secure, streamlined, and direct worldwide access to resources, through encrypted, authenticated, and authorized channels. This network-agnostic model unlocks the best of multiple commercial, global space and terrestrial transport backbones as viable mission network options. Together, these capabilities provide warfighters and partners with ubiquitous network availability, enabling freedom to operate from anywhere, anytime, and relieving the restraints of the legacy gateway and VPN bottlenecks.

3.5.1 Objective #5.1: Mature Network Discovery and Monitoring for Zero Trust

Before the AFIN network perimeter can pull back from the network down to the datacenter level, DAF must actively manage the best transport path for each resource connection. In order to find and manage any best path, DAF must aim to discover its many physical and logical transport paths (e.g., routing tables, VLAN, P2P, SD-WAN overlays, etc.), as a foundational and ongoing mission.

3.5.2 Objective #5.2: Deploy SDPs as Close to Protected Resources as Possible

In order to streamline secure and direct worldwide access to resources, DAF must evolve the base boundary from the network down to the datacenter level and eventually down to the individual data and microservice level. This is achieved through the PEPs/PDPs that make up an SDP, both in the cloud and on-premises. Using mutual transport layer security (mTLS), and common service access, SDPs consume all individual identity, device, and context attributes required to automatically make granular access decisions, establish, and monitor secure connections. Regardless of where the connection is coming from, the SDP validates the attributes against the data and application requirements from mission owners and application and data stewards. Placing the SDP as close to the protected resource as possible shrinks the attack surface and simplifies the transactional path, eliminating the need for VPNs, improving access for warfighters, and imposing higher costs on adversaries. Maps to DoD ZT Capability 5.2.

3.5.3 Objective #5.3: Migrate Enterprise Services to Hybrid Cloud

In order to provide anytime, anywhere access and security, DAF must migrate enterprise services to a hybrid cloud model. A combination of globally hosted cloud and on-premises services provide resilient and elastic capabilities from anywhere, while automatically synchronized, on-premises, and tactically deployable services provide assured availability under the harshest DDIL conditions. This environment ensures user identity attributes, device health, and access management persist uninterrupted.

3.5.4 Objective #5.4: Mature Segmentation to Lowest Level

Segmentation is the practice of breaking a unified system into smaller, isolated segments, in order to apply more granular visibility and access controls to each segment. To provide the strongest controls, the DAF must evolve from network-based segmentation to datacenter, host-based and micro-service level segmentation. The first priority is to expand segmentation across the AFIN, then apply segmentation down, as close to the protected resources as possible. On top of the added security, such low-level segmentation drives further benefits from DevSecOps code reuse, down to the container level, orchestration, and automated service management. Micro-segmentation will be the first rolled out ZT capability of the DAF, as early as FY23. Maps to DoD ZT Capability 5.1

3.6 Objective #6: Automation and Orchestration: Automated Security Responses based on Security Policies

3.6.1 Objective #6.1: Policy Inventory and Development

To build out robust and responsible automation, current task automation, response, and toolsets must be inventoried, debated, and codified. The DAF requires a cohesive Application Programming Interface (API)–driven mechanism to document, and query (e.g., orchestrate) policies across the enterprise and amongst Zero Trust components for effective automation. Governance will be needed for auditable change control of enterprise assets. Policies within the Zero Trust ecosystem must be continuously refined and matured to ensure effective enforcement against protected resources. Maps to DoD ZT Capability 6.1.

3.6.2 Objective #6.2: Workflow Enrichment

Through the continuous enumeration and analysis of manual processes, the DAF must reduce, and eventually eliminate, these inefficient and slow processes through the unceasing implementation of automation required to operate at speed and scale. The DAF must employ automation methods to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles. Maps to DoD ZT Capability 6.2

3.6.3 Objective #6.3: Automated Defensive Cyber Maneuvers

The DAF requires robust defensive cybersecurity operations to deploy, operate, and maintain security monitoring, protections, and response for protected resources. As the DAF adopts a Zero Trust construct, the amount of security–related data originating from all points of the architecture will quickly overwhelm cyber defenders. Therefore, to defend at speed and scale, the DAF must automate security processes and implement policy–based actions to the greatest extent possible by deploying automated security tooling – such as Security Orchestration, Automation and Response (SOAR) integration with Security Information and Event Management (SIEM) – will substantially decrease response times to detected threats and greatly enhance the enterprise cybersecurity posture. Organizations and system owners must ensure that they have a well-defined and robust investigation and remediation plans in place. In addition, to streamlining the detection and response to cybersecurity incidents, the DAF intends to reduce the number of SOAR solutions through enterprise-wide contracts. This enables professionals to have a federated location for orchestration and automated responses to address potential threats. At the same time, any additional SIEMs not already identified must conform to this SOAR strategy. Finally, all detection and response capabilities should be interoperable with Defensive Cyber Operations (DCO) capabilities to support incident response. Automated security response requires defined processes and consistent security policy enforcement across all environments in a Zero Trust enterprise to provide proactive command and control. Coupled with workflow enrichment, security technologies and policies can be orchestrated to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation. Maps to DoD ZT Capability 6.5.

3.6.4 Objective #6.4: Artificial Intelligence and Machine Learning

The DAF will employ AI/ML to enhance the execution of critical functions such as incident response (i.e., Security Operations Center (SOC) and Incident Response (IR), Security Orchestration, Automation & Response (SOAR)), anomaly detection, identity baselining, and data tagging – and particularly for risk and access determinations and environmental analysis.

3.7 Objective #7: Visibility and Analytics: Improve Detection and Reaction Time

Identifying/detecting and reacting to threats requires proper analytics. A key action on the ZT roadmap is to initiate application events integration into Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) for Financial Improvement and Audit Readiness (FIAR) / audit remediation.

3.7.1 Objective #7.1: Log Collection and Analysis

Log analysis is an important action in identifying system and software anomalies. Collection, processing, and analysis of logs – including network, data, application, device, and user logs – are critical to the monitor, detect, and protect functions for defensive cyber operations. Log analysis must be integrated across multiple data types to unify data collection and examine events, activities, and behaviors. Maps to DoD ZT Capability 7.1.

3.7.2 Objective #7.2: Threat Alerting

To action security violations, alerts must be set to notify a group or software to act. A key action on the ZT roadmap is to develop a shared responsibility model for application events with Cyber Security Service Providers (CSSP) and to establish logs, processes, and data available for CSSPs and Security Operation Centers (SOC). Advanced analytics support detection of anomalous users, devices, and Non-Person Entity (NPE) actions and advanced threats. Integration of threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques, and procedures (TTPs) enriches cyber analytics for enhanced threat detection. Maps to DoD ZT Capability 7.5.

3.7.3 Objective #7.3: Identity and Entity Behavior Baselines

Users and entities interacting with the Zero Trust architecture provide vital, contextual details that provide a greater understanding of performance, behavior, and activity across the enterprise. Baselining, profiling, and correlating individual user and entity behaviors vastly improves detection of anomalous behavior and enables the ability to make dynamic changes to security policy and real-time access decisions based upon changing threat conditions. Investigating beyond network telemetry gains visibility into observable threats that are present and allows orientation of defenses more intelligently. Maps to DoD ZT Capability 7.4.

4 Strategy Execution

The Zero Trust strategy execution is initially driven by the DoD Chief Information Officer (CIO) decision to sunset the Joint Regional Security Stacks (JRSS) by FY25, requiring DAF to provide a sufficiently mature Zero Trust infrastructure replacement and transitory equipment before that date. The implementation roadmap is regularly updated and can be referenced at the link below (Figure 2). The roadmap lays down the critical path for developing unclassified and classified implementation plans that initially will focus on the Indo-Pacific theater. Further efforts should extend to other network fabrics, tactical systems, and disconnected environments, in all other theaters, as progress matures through FY28. For additional specific details, those can be found on the DAF Zero Trust Implementation Plan and additional Implementation Plans per capability going into specific details of implementation. Beyond this time horizon, implementation will collapse network fabrics and integrate IoT devices, non-IP-based OT, SAP, and other non-Enterprise IT (EIT).

As a strategic consideration, it's critical to highlight that every step towards Zero Trust maturity shrinks the DAF's overall cyberspace attack-surface, forcing malicious actors to expend dramatically more resources to achieve fewer operational objectives. One of our highest priorities is enabling mission systems and apps to into the cloud and Zero Trust. We need to reach into the thousands of systems at all classification levels across the enterprise and weapon systems and reduce duplication and/or coalesce around fewer systems. One such path would be digital platforms where workloads can live and work without unique ATOs or security posture. Secondly, we should make Cloud One our priority for Compute and Store (C&S). It makes applications easier to change and is more flexible. As we refresh our on-prem facilities we should prioritize movement to cloud infrastructure. Lastly, we need to treat our newer modern applications and their developers as equals to our legacy applications when it comes to support.

Figure 2 - DAF Zero Trust Roadmap Link

4.1 Implementation

DAF will follow an aggressive Zero Trust Roadmap (Figure 2) which is based upon DoD CIOs Zero Trust Architecture, beginning baseline maturity in FY23, and reaching intermediate maturity by the end of FY28. DAF will begin advanced maturity in FY28, in-line with the 30-year planning choice. However, certain dependencies on the maturity path require particular focus.

First, DAF must begin deploying its Micro-Segmentation capabilities, using the Next Gen Gateways (NGGs) that are essential to the JRSS transition. End Point security will also begin with the adoption of the Microsoft Defender suite and C2C capabilities brought forth as a part of Enterprise IT as a Service (EITaaS) Wave 1. Next, maturing beyond a basic level requires an operational enterprise ICAM solution and deploying an enterprise endpoint management, security, and monitoring solution. SDPs (e.g., Cloud Native Access Point) across the AFIN, prioritizing its most critical Unclassified and Secret missions & data in the cloud and on-premises. Further, in order to begin collapsing networks, DAF requires a basic-level data tagging, labeling, and protection solution, along with approval from classification authorities (e.g., NSA). Mission app and systems owners must work diligently in concert with ZT implementation to ensure their capabilities remain intact during the ZT transition. Finally, DAF plans to transition sustainment and provider responsibilities of existing infrastructure to EITaaS in the FY25 timeframe, however, this transition must remain contingent on the EITaaS vendor's ability to take responsibility of all datacenters. Defensive Cyber Operations (DCO) will remain a DAF responsibility.

At a minimum, the Zero Trust Strategy Implementation-Plan (I-Plan), must include: measures of performance and effectiveness with DAF-wide participation; how it will meet all National Security Memorandum/NSM-8 requirements; and address applicable components of the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) framework. Due to key dependencies, it must also describe the relationship to the DAF CIO Strategy, ZT Roadmap, DAF ICAM Strategy, Data I-Plan, EITaaS, DAF Data Fabric, NSA efforts, Defense Information Service Agency's Thunderdome, SAP Zero Trust I-Plan equities, and DoD CIO's Zero Trust efforts. Any DAF implementation must synchronize and align with these initiatives across agencies, partners, and allies. It must also include tasks and activities describing how legacy technologies will sunset, integrate with or transition to Zero Trust-based policies and technologies.

4.2 Roles and Responsibilities

SAF/CN will provide policy, guidance, and strategic risk mitigation as priorities evolve. SAF/CN will also work with SF/S8 and AF/A8 (Deputy Chief of Staff for Plans and Programs) throughout the Planning, Programming, Budgeting, and Execution (PPBE) processes to advocate for resources.

As Air Force lead command for cyberspace operations, Air Combat Command (ACC) is the overall lead to develop the DAF Zero Trust Strategy I-Plan, execute this strategy, mitigate operational risks, and lead all legacy sunsetting efforts. ACC is the customer-facing organization, leading Zero Trust strategic communications actions, and synchronizing all DAF Zero Trust efforts. ACC will take special care to coordinate with Air Force Material Command (AFMC), as Lead Command and requirements-owner for SAP IT and the SAP Zero Trust I-Plan.

As Space Force lead command for cyberspace operations, Space Systems Command (SSC) in coordination with Space Operations Command (SpOC) lead command for cyberspace operations, and is appointed to develop and integrate space force requirements, architectures, and equities into all DAF lifecycle planning, acquisition, execution, and sustainment efforts.

"As Space Force lead acquisition field command for space mission systems, Space Systems Command (SSC), in coordination with Space Operations Command (SpOC) lead command for cyberspace operations, as well as Field Commands such as Space Development Agency, Space Rapid Capabilities Office, is appointed to develop and integrate Zero Trust (ZT) requirements, architectures, and equities into all DAF lifecycle planning, acquisition, execution, and sustainment efforts.

The Cyber Capabilities Center (CCC) is appointed to develop, coordinate, and deconflict all DAF, MAJCOM, C-MAJCOM, FIELDCOM, and field agency Zero Trust requirements and corresponding architectures, aligned to DoD's reference architecture.

The Air Force Acquisition (SAF/AQ) will develop and execute the acquisition strategy, while mitigating delivery risks and coordinating architectures, designs, and implementation across the EIT and OT portfolio.

16th Air Force is appointed to operate, secure, and defend the AFIN, in-line with this strategy. As this strategy matures, the Zero Trust Transition Team (ZTTT) responsibilities will transition to traditional Lead Command responsibilities, under ACC.[10]

4.3 Risks

Implementing such a radical new paradigm carries various operational, delivery, and strategic risks, which should be well understood from the onset. It is important to communicate these changes via all available means to overcome these risks. The largest operational risk incurred with this strategy could create single points of failure at the access points, which could challenge defensive cyberspace operator effectiveness during the transition period, leaving potential operational blind spots. Operational elements should place extra scrutiny at these points in order to best mitigate this risk. Additionally, since 4,000 non-AFIN contractor networks handle DAF Controlled Unclassified Information (CUI), DAF must explore data management policies and impose requirements to ensure those networks are aligned with the intent of this strategy in order to mitigate this risk.

From a delivery standpoint, developing the automated data tagging and labeling strategy, governance, and solution is lagging other Zero Trust efforts, but is critical to long-term maturity. It is important to communicate these changes via all available means to overcome this risk. Delays in these areas risk preventing DAF’s transition to advanced Zero Trust maturity and collapsing network environments. Additionally, endpoint security for non-IP-based systems and IoT devices is still very nascent. Despite being one of the furthest steps on the roadmap, some of these endpoints are the most critical devices that need Zero Trust protection and risk increasingly greater potential operational impacts as more critical internet of military things devices are connected. More broadly, industry lacks the standards in many of the architectural support components that would allow DAF to interchangeably select and change product vendors in this space without substantial cost. This risks long term lock-in with single vendors, giving them an outsized influence in our future cybersecurity posture. Finally, technologies which offer the most secure segmentation, down to the microservice level, require a complete refitting of our datacenters and are unlikely to occur before the FY28 refresh. Planning, coordination, and development for these particular elements earlier in the strategy execution, will buy down the risks as they come into focus on the roadmap.

The greatest risk to this strategy is institutional resistance to change. This massive cultural shift requires all DAF communities to adapt in uncomfortable ways and participate in its collective cybersecurity mission. Application, data, and mission owners must be active participants in data tagging, attribute definition, and access decision requirements. These are the fundamental elements of Zero Trust that will drive success or failure. Failure to make this cultural change runs the risk that the DAF cannot implement this strategy, which accelerates the warfighting changes demanded by the Chief of Staff of the Air Force and Chief of Space Operations. Failure to implement this strategy bears significantly greater risk in connecting CJADC2 military IoT systems together, increasing the potential impacts an adversary could inflict from data exfiltration and degraded systems to critical mission failure and potential loss of life. Mitigating

[10] DAFPD 10-9, Lead Command/Lead Agent Designation and Responsibilities for United States Air Force Weapon Systems, Non-Weapon Systems, and Activities, 25 May 2021.

this risk requires senior leader champions across the DAF to become partners in the strategy's success.

Ultimately, this strategy must deliver a scalable, resilient, auditable, and defendable framework centered on protection of our most critical, mission essential DAAS, to prevent, detect, respond to, and recover from malicious cyber activity in multiple operating environments. If successfully implemented, this strategy mitigates the risk of being unprepared for the future fight.

Appendix A: References

Cybersecurity and Infrastructure Security Agency. "Zero Trust Maturity Model." (2021, Jun). [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA Zero Trust Maturity Model_Draft.pdf

SAF Chief Data Officer (CDO). "DAF I-Plan of the DoD Data Strategy" (2021, Feb)

DoD Chief Data Officer (CDO). "DoD Data Stewardship Guidebook." (2021, Sep 1)

Department Of The Air Force Policy Directive 10-9. "Lead Command/Lead Agent Designation And Responsibilities For United States Air Force Weapon Systems, Non-Weapon Systems, And Activities." (2021, May 25). [Online]. Available: https://static.e-publishing.af.mil/production/1/af_a8/publication/dafpd10-9/dafpd10-9.pdf

Department of the Air Force, Manual 17-1304. "Identity Credential and Access Management (ICAM)." (2021, August 18). [Online]. Available: https://static.e-publishing.af.mil/production/1/saf_cn/publication/dafman17-1304.pdf

DoD Zero Trust Reference Architecture. (2022, July). [Online\. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

DoD Directive 3020.40. "Mission Assurance." (2018, Sep 11). [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf

DoD Digital Modernization Strategy. (2019, Jul 12). [Online]. Available: https:/media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

Executive Order 14028: Improving the Nation's Cybersecurity. (2021, May 12). [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

NIST Special Publication 800-207. "Zero Trust Architecture." (2020, Aug 11). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

National Security Memorandum 8. "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems." (2022, Jan 19). [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

OMB, "M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." (2022, Jan 26). [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Priority Department of the Air Force (DAF) Operational Imperatives. (2022, Feb 7).

U.S. National Defense Authorization Act for Fiscal Year 2022. "Sect 1528: Zero Trust Strategy, Principles, Model Architecture, and Implementation Phase". (2021, Dec 27). [Online]. Available: https://www.congress.gov/bill/117th-congress/senate-bill/1605/text

This page intentionally left blank.

Appendix B: Acronyms

ACC	Air Combat Command
AF	Air Force
AFIN	Air Force Information Network
AFLCMC	Air Force Lifecycle Management Center
AFMC	Air Force Material Command
AI	Artificial Intelligence
API	Application Programming Interface
CCC	Cyber Capabilities Center
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
C-MAJCOM	Component Major Command
CDO	Chief Data Office
CUI	Controlled Unclassified Information
DAF	Department of the Air Force
DAAS	Data, Applications, Assets, and Services
DC	Domain Controller
DDIL	Denied, Degraded, Intermittent, and Limited
DevSecOps	Development, Security & Operations
DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
EDR	Endpoint Detection and Response
EIT	Enterprise Information Technology
EITaaS	Enterprise Information Technology as a Service
EO	Executive Order
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
IoT	Internet of Things
IT	Information Technology
CJADC2	Combined Joint All-Domain Command and Control
JRSS	Joint Regional Security Stack
JWICS	Joint Worldwide Intelligence Communications System
MAJCOM	Major Command
ML	Machine Learning
mTLS	Mutual Transport Layer Security
NIPR	Non-classified Internet Protocol Router Network

NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
OMB	Office of Management and Budget
OT	Operational Technology
PDP	Policy Decision Point
PEP	Policy Enforcement Point
SAF	Secretary of the Air Force
SAP	Special Access Program
SDP	Software Defined Perimeter
SECAF	Secretary of the Air Force
SIPR	Secure Internet Protocol Router Network
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
US	United States
VAULT-IS	Visibility, Accessibility, Understandability, Linkages, and Trustworthiness – Interoperable, Secure
VPN	Virtual Private Networks
XDR	Extended Detection and Response