DEPARTMENT OF THE AIR FORCE

NETWORK OF THE FUTURE STRATEGY

SAF/CN
AUG 2025

NETWORK OF THE FUTURE

Strategy for the Network of the Future

The Department of the Air Force's (DAF) Network of the Future must seamlessly integrate **security** and **flexibility**, ensuring resilient continuity of air, cyber, and space operations to defend against our near peer adversaries. Organized by six key objectives, this strategy outlines how the DAF will deliver a resilient & adaptive encrypted network that provides uninterrupted, real time data sharing for the Warfighter–enhancing operational effectiveness and improving **User Experience** (UX) at every touchpoint to empower mission success.

Objectives

● UX Driven — Security — Flexibility

Bolster Network Resilience

Modernize transport methods and routing to ensure flexible data movement in the face of high network demand.

- SD-WAN for Transport Routing
- Varied Transport Methods

1

Increase Operational Scalability and Flexibility

Enable adoption of commercial technology to increase flexibility and speed of deployment.

- CDS
- CSfC ●
- Mesh Network Technologies

2

Secure the Network of the Future

Strengthen the DAF's cybersecurity posture by integrating dynamic access into network architecture.

- NGG ●
- ICAM ●
- C2C ●

3

Streamline Network Management

Increase uniformity and availability to meet growing demand in a way that lowers cost and reduces tech debt.

- BIM Consistency and Enhancements ●
- Centralized SIPR Domain
- IPv6 Availability

4

Integrate the Network Environment

Enable interoperable networking and communications for all DAF Missions anytime, anywhere.

- MPE
- TDC
- NETWORK IN ACTION
  DAF BATTLE NETWORK

5

Enable the Workforce of the Future

Our competitive edge relies on both the Network of the Future and the readiness of our workforce.

- Expeditionary Operations School
- DAF Learning Services
- Next-Gen Virtual Training

6

WARFIGHTER LETHALITY

Integrate state-of-the-art software and hardware across the DAF to supply capabilities necessary to maintain the competitive edge

UBIQUITOUS CONNECTIVITY

Provide Airmen and Guardians real-time data sharing anytime, anywhere via a resilient and encrypted network

CYBER OPTIMIZATION & RESILIENCE

Strengthen the DAF's ability to rapidly execute the warfighter's mission through a strong, durable, and sustainable cyber posture

TABLE OF CONTENTS

I.A. NETWORK STRATEGY THESIS

The DAF faces increasingly advanced technological adversaries with the potential to launch attacks on our networks faster than human operators can respond. Emerging technologies accelerate the ability of adversaries to breach and manipulate our networks—the information technology (IT) upon which all mission success relies [i]. At the same time, the DAF must also contend with a global increase in demand for data access and convenient connectivity. This challenge is compounded by a networking environment characterized by disparate solutions rather than a unified enterprise approach that meets cost, schedule, performance needs, and improves UX satisfaction. As a result, the DAF's network of the future must support secure operations through convergent and divergent environments, ranging from sparsely-connected operational locations to fixed facilities, hybrid remote workforces, and allied nations. It must seamlessly connect the core to the edge, exhibit fundamental resilience to all forms of service disruptions, and be easily reconfigured to adapt to changing mission needs, all while prioritizing the satisfaction and operational effectiveness of our end users.

In the past 5 years, the DAF has shifted response to these realities in two major ways. First, the DAF shifted its wartime posture to address the evolving strategic rivalry between major world powers, driving the need to defend against increasingly advanced attacks on the Network and enhance tactical effectiveness with advanced combat capabilities. Second, recent disruptions to normal operations have driven a significant shift towards hybrid and remote work, which have become necessary to ensure continuity of air, cyber, and space operations. The DAF's Network of the Future must mirror these shifts and encompass both network security and network flexibility. Wherever the DAF introduces **security**, it must also introduce **flexibility** and vice versa, ensuring that both elements work together to enhance and continually improve **UX**.

Security

Flexibility

The DAF's Network of the Future must encompass both **security** and **flexibility**.

I.B. OUTCOMES FOR THE WARFIGHTER

Airmen & Guardians,

The DAF stands at the forefront of technological transformation, committed to harnessing the power of emerging innovations to secure and advance our national defense capabilities. As we look to the future, the DAF recognizes a resilient, adaptive, and integrated digital infrastructure—our "Network of the Future"—is essential for operational superiority and mission success.

The Network of the Future will serve as the backbone for seamless connectivity, real-time data sharing, and rapid decision-making across all domains to provide our warfighters with access to data they need anytime, anywhere. By investing in foundational technologies such as artificial intelligence, advanced cybersecurity, edge computing, and 5G communications, the DAF will lay the groundwork to transform today's emerging capabilities into tomorrow's industry standards. This approach ensures that our Airmen and Guardians are equipped with the tools needed to outpace adversaries and respond to evolving threats with agility and precision. By championing a culture of continuous innovation, the DAF can meet the evolving challenges of today and tomorrow, strengthening our readiness, increasing efficiency, and securing our nation, shaping the future of defense and industry alike.

The DAF Chief Technology Officer (CTO) is dedicated to delivering outcomes that directly enhance the warfighter's effectiveness, with a focus on warfighter lethality, ubiquitous connectivity, and cyber optimization and resilience. This document serves as a forward-looking blueprint for the Network of the Future to enable ubiquitous connectivity across the edge continuum. By illustrating how diverse enabling capabilities integrate into a unified, cohesive architecture, this document demonstrates the critical importance of ensuring that real-time data, secure communications, and adaptive responses are available wherever and whenever the mission demands.

Scott

HEITMANN.SCOTT.A.1231341320

Digitally signed by HEITMANN.SCOTT.A.1231341320
Date: 2025.08.21 15:35:09 -05'00'

SCOTT A. HEITMANN, SES, DAF
Chief Technology Officer

I.C. TODAY'S DAF NETWORK

The DAF faces increasingly advanced technological adversaries with the potential to launch attacks on our networks faster than human operators can respond. Emerging technologies accelerate the ability of adversaries to breach and manipulate our networks—the IT upon which all mission success relies. At the same time, the DAF must also contend with the global increase in demand for data access and convenient connectivity in a networking environment characterized by disparate solutions rather than a unified enterprise architecture that balances dynamic operational requirements, security, flexibility, cost, schedule and performance efficiencies.

What's Being Worked Today

ABMS

- Develop and Acquire Next Gen C3BM capabilities
- Enable JADC2 and decision advantage through connecting data from sensor to effector through C3BM
- Open Architecture, software defined environments

ICAM

- Streamline identity management and access controls for enhanced cybersecurity and interoperability
- Enable secure access to authorized resources based on mission need
- Provides PAM and MFA

NGG

- Modernize the DAF network infrastructure with Zero Trust capabilities
- Designed to ensure continuity of operations in Denied, Degraded, Intermittent, and Limited (DDIL)
- Provide SD-WAN for connectivity across services

BIM

- Transition DAF Base Area Networks (BANs) to mission-aligned performance with "as-a-Service" operations
- Improved flexibility and efficiency with industry-leading IT services
- Holistic BAN refresh to meet future warfighter needs

Scope

This document is intended to guide the DAF on future network capabilities through a unified approach which connects core network services to the edge and exhibits fundamental resilience and adaptability to changing mission needs. It provides high level vision and guidance to improve program decision making, increase interoperability and accelerate use of modern network technologies.

WHAT IT IS

☑ Future state projections

☑ Potential impacts to the warfighter

☑ How the DAF improves & guides implementations

☑ Iterative

WHAT IT IS NOT

☒ Execution plan

☒ Vendor solutions

☒ A guide for how the DAF spends money

☒ Concrete

II.A. Objective 1: Bolster Network Resilience

Modernize transport methods and routing to ensure flexible data movement in the face of high network demand.

Summary

The DAF Network of the Future must exhibit fundamental resilience to all forms of service disruptions. In doing so, it must ensure flexible data movement via a secure and flexible peering architecture to support future mission networks in the face of high network demand. Efforts with the Department of Defense (DoD) Chief Information Officer (CIO) and other service CIOs should focus on migrating to a Software-defined Wide Area Network (SD-WAN) for transport routing and incorporating alternative transport methods, such as satellite and 5G cellular. SD-WAN will make it easier to provide secure connections to cloud and off-site data center applications, enhancing network flexibility and responsiveness, and automating network configurations and processes. Meanwhile, integrating new transport methods such as satellite and 5G technologies will bolster network resilience and bandwidth capacity, supporting the missions of tomorrow. Upgrading hardware and underlying cryptography will help us defend against advanced technological threats, such as quantum computing. These advancements will promote adoption of commercial provided services and improve capacity management to create an agile, robust network infrastructure ready for evolving demands.

Enabling Capabilities

SD-WAN for Transport Routing

Traditional Wide Area Networks (WANs)

- De-centralized
- Limited adaptability to real-time bottlenecks

moving towards

Software-Defined Wide Area Networks (SD-WANs)

- Unified control plane
- Dynamic network traffic management
- Scalable with encryption between routers
- Adoption of meshONE-T

Varied Transport Methods

Satellite Connectivity

- Move critical command & control data from any location
- High-speed network access
- Adoption of commercial satellite providers

5G Connectivity

- Robust, secure connectivity for data and missions
- Increase bandwidth of data sharing in CONUS

Commercial Transport Services

- Easily scalable, rapidly deployable, and provides new technology to the warfighter

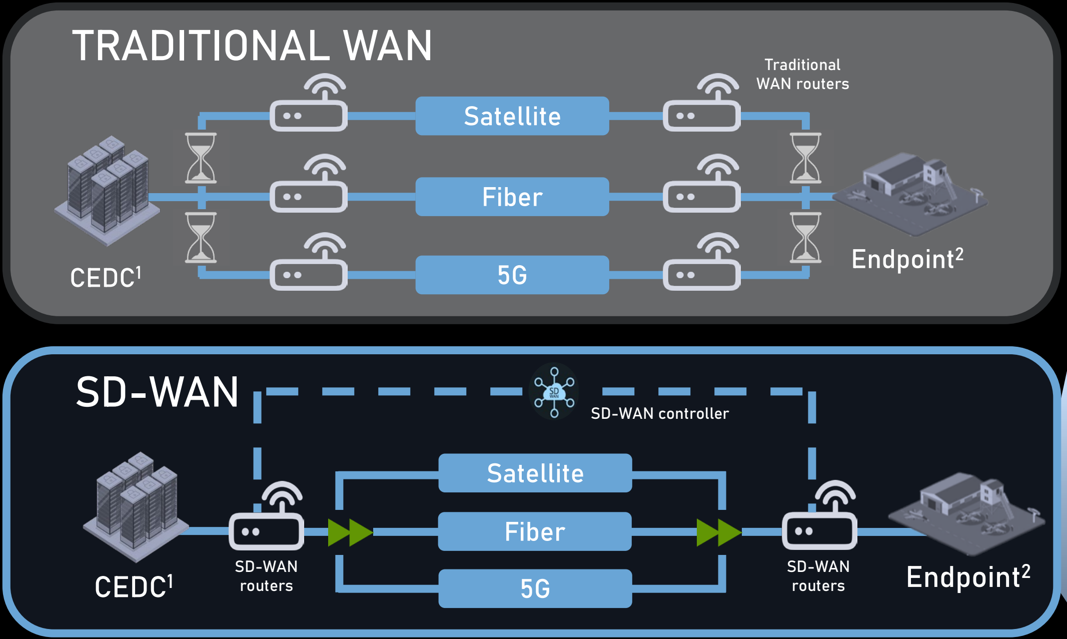
II.A.1. SD-WAN for Transport Routing

Traditional Wide Area Networks (WANs)

- De-centralized
- Limited adaptability to real-time bottlenecks

Software-Defined Wide Area Networks (SD-WANs)

- Unified control plane
- Dynamic network traffic management
- Scalable with encryption between routers
- Adoption of meshONE-T



[1]Component Enterprise Data Center
[2]MOB, GSU, joint location, forward/deployable location, etc.

Figure II.A.1. SD-WAN vs Traditional WAN [1]

SD-WAN Pros:

- Aligned to meet demands of global network usage
- Policy-based forwarding of network traffic to meet operational needs

Example Transport Solution

meshONE-T

SUMMARY | WAN that connects data producers and consumers, providing diversified communication paths built on modern technology and industry standards.

SUPPORTS | *USSF, ABMS, and DAF Mission Partners*

- Part of the DoD's Combined Joint All-Domain Command and Control (CJADC2) initiative

Impact to Warfighters

SD-WANs increase **security** and **flexibility** for the warfighter by enabling content-aware routing and improved throughput leveraging multipath routing. The DoD's push for SD-WAN is driven by the need for a responsive network capable of autonomous decision-making. The goal is to achieve a network that can adapt to congestion or outages and continue to forward mission critical data based on defined policies in a DDIL environment.

WANs have long operated as the backbone of enterprise networking, connecting multiple Local Area Networks (LANs) across geographical areas using hardware-based routers and manual configurations. With SD-WAN, configuration and policy definition is unified. It provides greatly enhanced policy-based forwarding of critical data in constrained environments. SD-WAN is designed to be easily scalable and can integrate across multiple connection types with end-to-end encryption and unified security policies across all locations to simplify security management. SD-WAN is application aware and monitors network traffic, which is collected real-time and used to ensure that traffic prioritization processes can be implemented and informed by mission thread use cases to enhance operational efficiency. Additionally, SD-WAN's unified control and policy definition makes it much more efficient at forwarding mission critical traffic across multiple links, based on real-time information about all available paths.

II.A.2. Varied Transport Methods

Satellite Connectivity

- Move critical command & control data from any location
- High-speed network access
- Adoption of commercial satellite providers

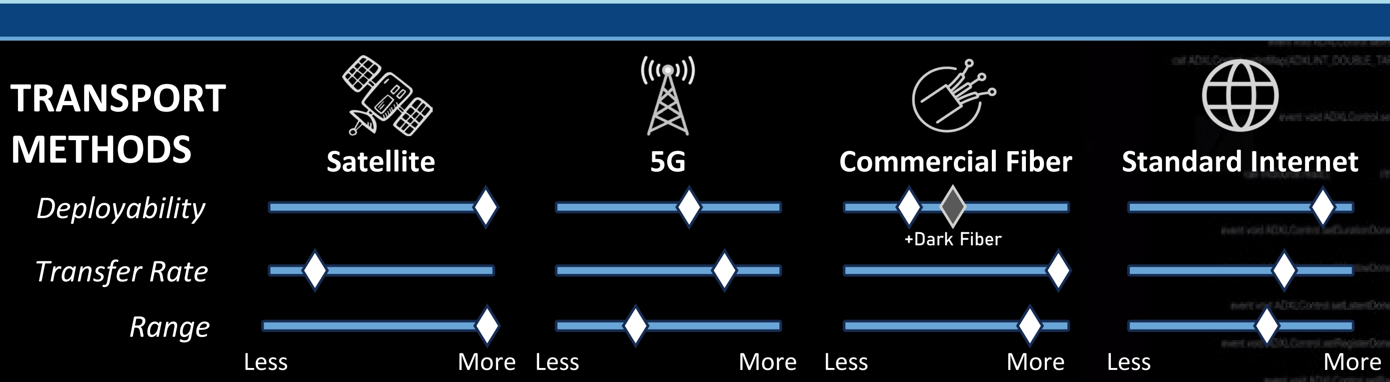
5G Connectivity

- Robust, secure connectivity for data and missions
- Increase bandwidth of data sharing in CONUS*

Availability and effectiveness of **all transport methods (e.g., satellite, 5G, etc.) vary in OCONUS locations dependent on the region.*

Commercial Transport Services

- Easily scalable, rapidly deployable, and offers innovative technology



	Satellite	5G	Commercial Fiber	Standard Internet
+ PROS:	Wide Availability	Fast Speeds	Fast Speeds	Wide Availability
	Quick Deployment	Low Latency	Reliable	Reliable
	Disaster Resilient	High Capacity	Future-proof	Low Cost
− CONS:	High Latency	Degrading in Conflict	High Costs	Variable Speeds
	Degrading in Conflict	Dead Zones	Limited Availability	Vulnerability
	Higher Costs	Compatibility	Longer Installation	Data Caps

Figure II.A.2. Varied Transport Methods [A]

Impact to Warfighters

Transport refers to the physical and virtual infrastructure used to transfer data. As bandwidth demand increases, it is critical that the DAF provide our warfighters the capabilities to both manage available bandwidth transfer increasing amounts of data so the U.S. may retain information and decision advantage. Shifting to alternative transport methods like satellite, 5G, dark fiber, and commercial or cloud transport services enhances **flexibility** for warfighters by allowing seamless movement of high-performance data.

Commercial Low Earth Orbit (LEO) Satellite Communications (SATCOM) providers offer scalable, resilient, and cyber-secure connectivity that is interoperable with the DAF Battle Network and provides network in areas with unreliable or non-existent connectivity. The DAF's move towards 5G supports warfighters by increasing bandwidth and speed, enhancing command and control situational awareness in CONUS environments. Dark fiber offers significant strategic advantages for the DoD, including enhanced security, flexibility, and control over network infrastructure, allowing the DAF to establish dedicated, private networks independent of public infrastructure to reduce cyber threat exposure and enable secure data transmission. To maintain a holistic view of bandwidth requirements and ensure bandwidth sufficiency during wartime, the DAF should increase policy management and clarify contracting efforts, simplifying procurement pathways for satellite and 5G transport.

II.B. Objective 2: Increase Operational Scalability and Flexibility

Enable adoption of commercial technology to increase flexibility and speed of deployment while maintaining secure data transport between nodes.

Summary

Adopting commercial technology enhances the DAF's flexibility, speed of deployment, cost-effectiveness, interoperability, scalability, and security, enabling rapid adaptation to evolving operational needs. Increasing the use of Commercial Solutions for Classified (CSfC) for data security will provide additional mobility, scale, throughput, and flexibility, allowing the DAF to transition away from Type 1 encryptors, negating costs and infrastructure supply chain issues required by Type 1 encryptors. Additionally, CSfC enables Mission Partner Environments (MPEs) by providing Mission Partners the option to purchase commercial products to connect in remotely for secure data access. Cross Domain Solutions enable secure information sharing for mission operations in Enterprise environments. Mesh network technologies support enhanced base and field operations by maintaining connectivity to enable faster decision making.

Enabling Capabilities

CDS

Secure Data Movement

- Enable secure data sharing and comms between different security domains
- Deliver data center services to the tactical edge
- Allow DAF personnel to access data from multiple networks with varying classification levels

Zero Trust Network Segmentation

- Implement ABAC on all resources and data
- Validate authorization every time a resource is accessed
- Monitor activity while resources are being accessed

CSfC

Enterprise CSfC Implementation

- Leverage private sector innovations
- Secure data over unsecured networks
- Rapid deployment and scalability

CSfC Devices for Classification Mobility

- Intermingle traffic of more than one classification level along a single transport network (SIPR, NIPR, and Top Secret (TS))
- Protect classified information using commercial technology, even over public networks

Mesh Network Technology

Enhanced Base Operations

- Maintain connectivity across the entire base delivering access to resources
- Enable faster decision making and continuity of flightline operations

Enhanced Field Operations

- Provide tactical comms in remote and hostile environments
- Enable comms and data sharing among troops, vehicles, drones, etc. using SATCOM
- Enhance redundancy with multipath routing

II.B.1. CDS

Secure Data Movement

- Enable secure data sharing and communication between different security domains
- Deliver data center services to the tactical edge
- Allow DAF personnel to access data from multiple networks with varying classification levels

Zero Trust Network Segmentation

- Implement attribute base access control (ABAC) on all resources and data
- Validate authorization every time a resource is accessed
- Monitor activity while resources are being accessed

Access Solutions

*Allows a user to **ACCESS** differently classified networks from a single machine*

- Ability to display different classified windows on same display
- Ability to access classified networks remotely over unclassified networks via CSfC

VS

Transfer Solutions

*Send or **TRANSFER** data between different security domains.*

- Ability to share different types of information (e.g., file sharing, messaging, email, chat, etc.)

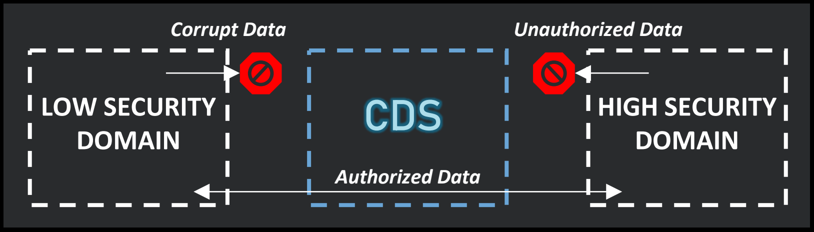


Figure II.B.1. CDS Operational Diagram [2]

Cross Domain Solutions*

SECUREVIEW

ISSE Guard

X-ARBITOR

V2CDS

* Examples of existing CDSs. Note these are NOT enterprise provided.

Impact to Warfighters

Cross Domain Solutions (CDS) are a mechanism to access or transfer information between two or more networks of different security classifications. To maintain **security** of information sharing, CDS's can be deployed across the DAF – anywhere from large data centers with various networks and security enclaves, to the tactical edge to meet mission needs. By implementing CDS with strict access controls, they can act as gateways to manage data flow between security levels.

For weapons systems that operate in secret and TS levels, this results in delayed decision making, limited interoperability, and resource constraints. To securely share critical information between security domains, the DAF should partner with commercial cloud providers to develop a plan to implement enterprise CDS for secure data movement from Impact Level (IL) 2 through IL 6 that meet National Cross Domain Strategy standards and compliance requirements. This will provide weapons systems and other military assets at the tactical edge the strategic advantage to gather, process, and act on intelligence to meet their mission needs.

II.B.2. CSfC

UX Driven

Enterprise CSfC Implementation

- Leverage private sector innovations
- Secure data over unsecured networks
- Rapid deployment and scalability

CSfC Devices for Classification Mobility

- Intermingles traffic of more than one classification level along a single transport network (SIPR, NIPR, and TS)
- Protect classified information using commercial technology even over public networks

PROS:

- Protected and encrypted classified information
- Cost-savings via commercial, scalable products
- Faster deployment through automation

CONS:

- Required calculated risk management
- Potential for performance degradation from the layered approach
- May not be suitable for all environments

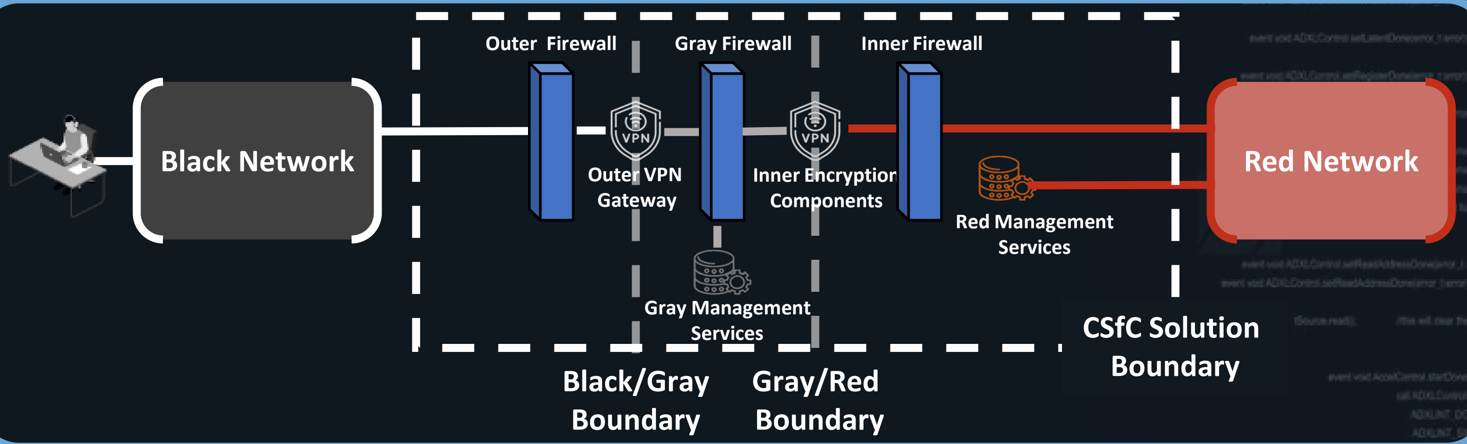


Figure II.B.2. Encryption Tunnels for Data Protection [3]

Impact to Warfighters

Commercial Solutions for Classified (CSfC) will allow Airmen and Guardians to make use of readily available commercial products and technologies for classified data protection at the highest **security** level. Leveraging CSfC through an enterprise implementation will negate the need for custom classified systems and allow the DAF to equip the warfighter faster using existing commercial technology, streamlining access and deployment to improve **UX**. Additionally, an enterprise CSfC implementation will enable enterprise-level management so that classified networks can be provided over the default commercial network. Benefits of CSfC include increased speed of deployment through reduced reliance on Type 1 Encryption, decreased cost, Internet flexibility, scalability, automation, and enhanced UX.

In addition to adopting CSfC architecture, the DAF should also adopt and utilize CSfC devices to extend classified mobility options in conjunction with the enterprise CSfC implementation. By combining CSfC laptop solutions (e.g., SecureView) with Virtual Desktop Infrastructure (VDI), Airmen and Guardians would have access to many networks at once, allowing for reduced development time, faster insertion of new technology, and greater **flexibility** for the warfighter. As CSfC and Commercial-Off-the-Shelf (COTS) products are adopted by the DAF, they should also be consolidated and governed on the enterprise level.

II.B.3. Mesh Network Technologies

Enhanced Base Operations

- Maintain connectivity across the entire base delivering access to resources
- Enable faster decision making and continuity of flightline operations

Enhanced Field Operations

- Provide tactical communications in remote and hostile environments
- Enable communication and data sharing among troops, vehicles, drones, etc. using SATCOM
- Enhance redundancy with multipath routing to guard against single points of failure, jamming, degrading, or denying services

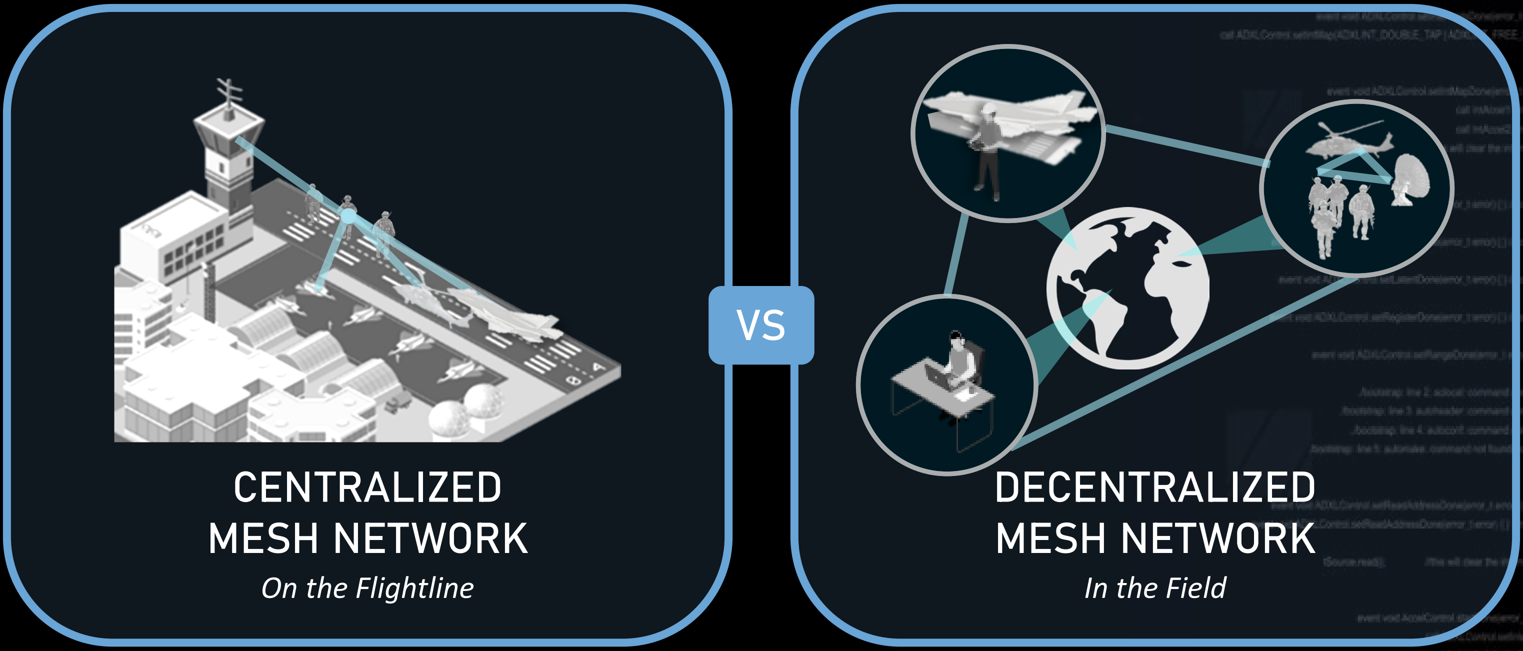


Figure II.B.3. Centralized vs Decentralized Mesh Networks [4]

Impact to Warfighters

In a mesh network, each device in the network in theory sends its own signals and information. Each device or node on the network is connected to the others, and this connection allows information to be relayed across the network from any node. This topology ensures that data has multiple paths to travel between nodes, significantly enhancing the network's reliability and fault tolerance for jamming, degrading, or denying services.

While mesh networks offer numerous advantages, they also present several challenges and considerations. One of the primary challenges is the higher cost associated with implementing a mesh network. As a result, the DAF should provide guidance on priority nodes to include in the mesh network topology, with focus on the Warfighting Mission Area (WMA) initiatives. Additionally, mesh networks can be complex and difficult to install and maintain. As new nodes are integrated into the existing network, there should be sufficient guidance and trained personnel to ensure successful integration. However, when implemented correctly, centralized and decentralized mesh networks have the capability to increase **flexibility** for warfighters in a tactical environment while ensuring greater **security** with redundant path routing to prevent single points of failure, jamming, or degrading.

II.C. Objective 3: Secure the Network of the Future

Strengthen the DAF's cybersecurity posture by integrating dynamic access into network architecture.

Summary

Next-generation gateways deliver Zero Trust capabilities that leverage technologies like AI, SD-WAN, and cloud integration to provide enhanced security, optimized performance, and greater flexibility in managing and routing network traffic. These gateways move beyond traditional functionalities by offering intelligent path selection, dynamic resource allocation, and sophisticated threat detection, ultimately improving network efficiency, scalability, and resilience for modern applications and distributed environments.

Enabling Capabilities

NGG

>SASE ARCHITECTURE

Provides a platform for secure access to applications and data by integrating next generation gateways with various security functions such as data loss prevention, DNS security, and cloud access security brokers

Zero Trust Security and Compliance

- Continuous authentication and authorization of users based on context to minimize lateral movement and prevent data breaches
- Must comply with NSA BOD to mandate specific encryption protocols and dictate configurations for network devices and applications

SDPs

- NGGs leverage SDP technology to dynamically provision and secure connections after verifying user and device identity
- Network resources are effectively cloaked from unauthorized users, reducing risk of attack
- Deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) within SDP-protected environments

Supporting Capabilities

ICAM

Robust Enterprise ICAM

- Robust and data-centric to enable centralized authentication and authorization
- Deliver data-centric fine-grained access control or ABAC

C2C

Safeguarded Endpoints

- Ensures that devices meet security policies prior to granting network access [B]
- Automatic device verification and continuous device monitoring

II.C.1. NGG

UX Driven

Zero Trust Security and Compliance

- Continuous authentication and authorization of users based on context to minimize lateral movement and prevent data breaches
- Must comply with NSA BOD to mandate specific encryption protocols and dictate configurations for network devices and applications

Software Defined Perimeters (SDPs)

- NGGs leverage SDP technology to dynamically provision and secure connections after verifying user and device identity
- Network resources are effectively cloaked from unauthorized users, reducing risk of attack
- Deploy IDS and IPS within SDP-protected environments

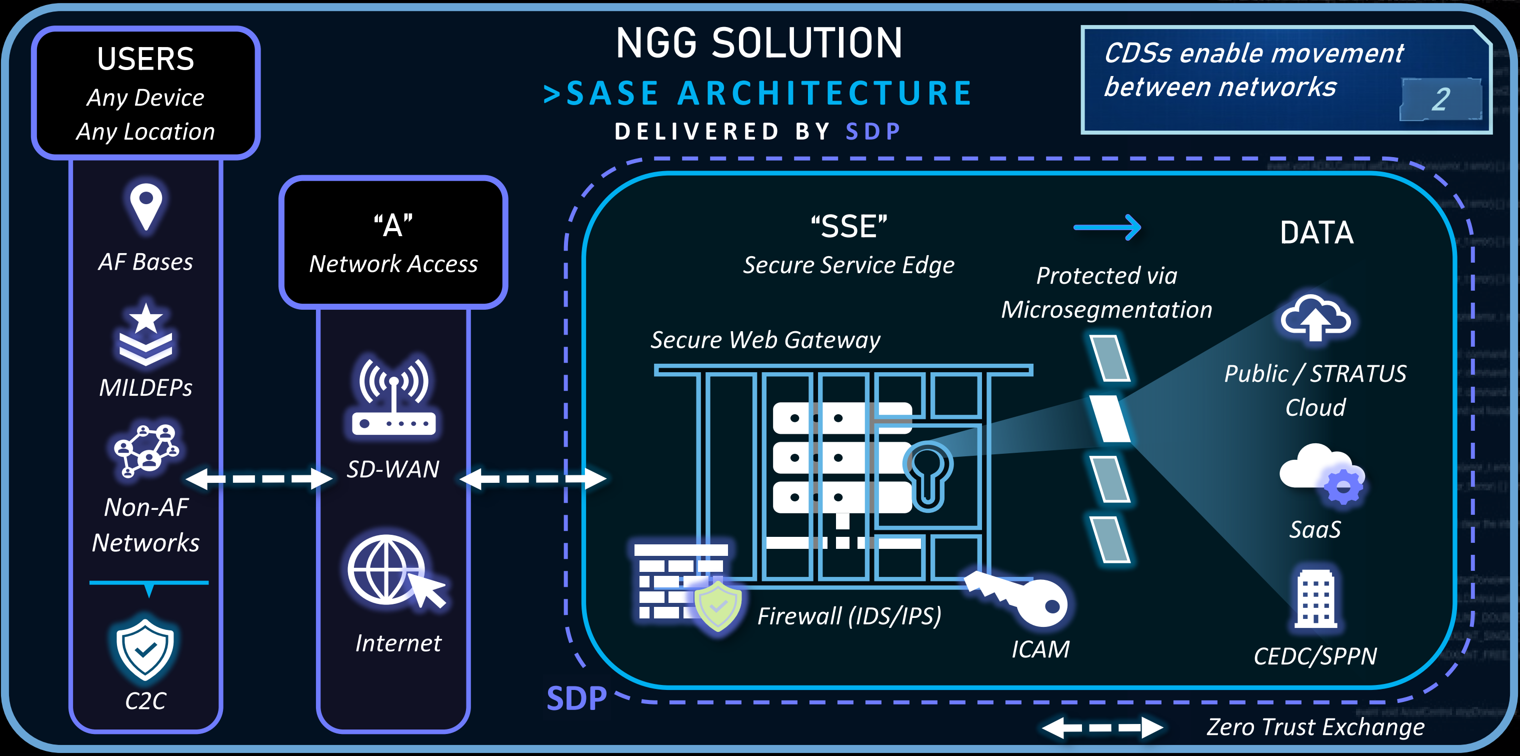


Figure II.C.1. NGG Operational Diagram

Impact to Warfighters

Next-Generation Gateways (NGGs) are crucial for warfighters by providing **secure** and reliable communication channels in dynamic and contested environments. NGGs go beyond traditional firewalls and basic web filtering by integrating capabilities like intrusion prevention, SDPs, PDPs/PEPs, and ABAC into a unified security solution offering granular control over network traffic. In addition to these capabilities, Microsegmentation protects data by limiting communication to only what is necessary for mission objectives and by ensuring every data access request is from an authenticated and authorized source. This enables the DAF to enforce security policies, protect sensitive data, improve overall network performance, and enhance **UX** for end users.

Achieving rapid response capabilities in a 'fight tonight' scenario requires a holistic approach to network planning, including redundancy, resilience, and real-time monitoring. These gateways enable seamless data transmission and access to critical information, facilitating enhanced situational awareness and decision-making on the battlefield. With advanced security features and optimized bandwidth management, NGGs empower warfighters with the connectivity they need to maintain operational effectiveness, mission success, and a consistently high-quality UX.

II.D. Objective 4: Streamline Network Management

Increase uniformity and availability to meet growing demand in a way that upholds security standards and enhances network agility.

Summary

In pursuit of streamlined network management, increased automation and centralization will help drive a reduction in regional configuration variations and snowflake policies. This includes transitioning to SD-WAN and transitioning to dual stack Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) baseline on all networks to establish commonality in rules for exchanging data over the internet. The integration of SD-WAN technology will enable content-aware routing and prioritization, aligning automated policy enforcement with mission needs. This technology represents a generational leap in the DAF network baseline and requires a future focused architecture that standardizes SD-WAN into a single implementation across the DAF. Interim implementation of this capability should be done with this end state in mind to take advantage of the economies of scale necessary to field this technology globally.

Enabling Capabilities

BIM Consistency & Enhancements

Transition to Enterprise As-a-Service Operations

- Modernize existing networks while deploying ‘As-a-Service’ Operations
- Leverage industry-leading commercial services
- Enhance operational capabilities of base personnel

Increased Availability & Economies of Scale

- Deliver modern network technologies to provide reliable performance
- Align network services to the mission, meeting operators where they are and where they are going
- Utilize COTS internet solutions to fulfill non-mission critical requirements

Centralized SIPR Domain

Shared Computing and Storage

- Remotely operate, manage and maintain the on-base hosting environment
- Consolidate and standardize core service stacks at the base level

Survivability in Disconnected Operations

- Provide the minimum functionality to an installation, should it become disconnected from the DoD Information Network (DoDIN)

IPv6 Availability

Ongoing Transition to Dual Stack Protocols

- Implement dual stack Internet Protocol Versions 4 and 6 (IPv4/6) baseline on AFNET WAN & LAN
- Expanding to IPv6 to allow for continued growth of connected users, services, and applications

Future-State Migration to IPv6

- Ensure cyber defensive tools can account for all terrain
- After AFNET WAN is up, begin moving bases to IPv6

II.D.1. BIM Consistency & Enhancements

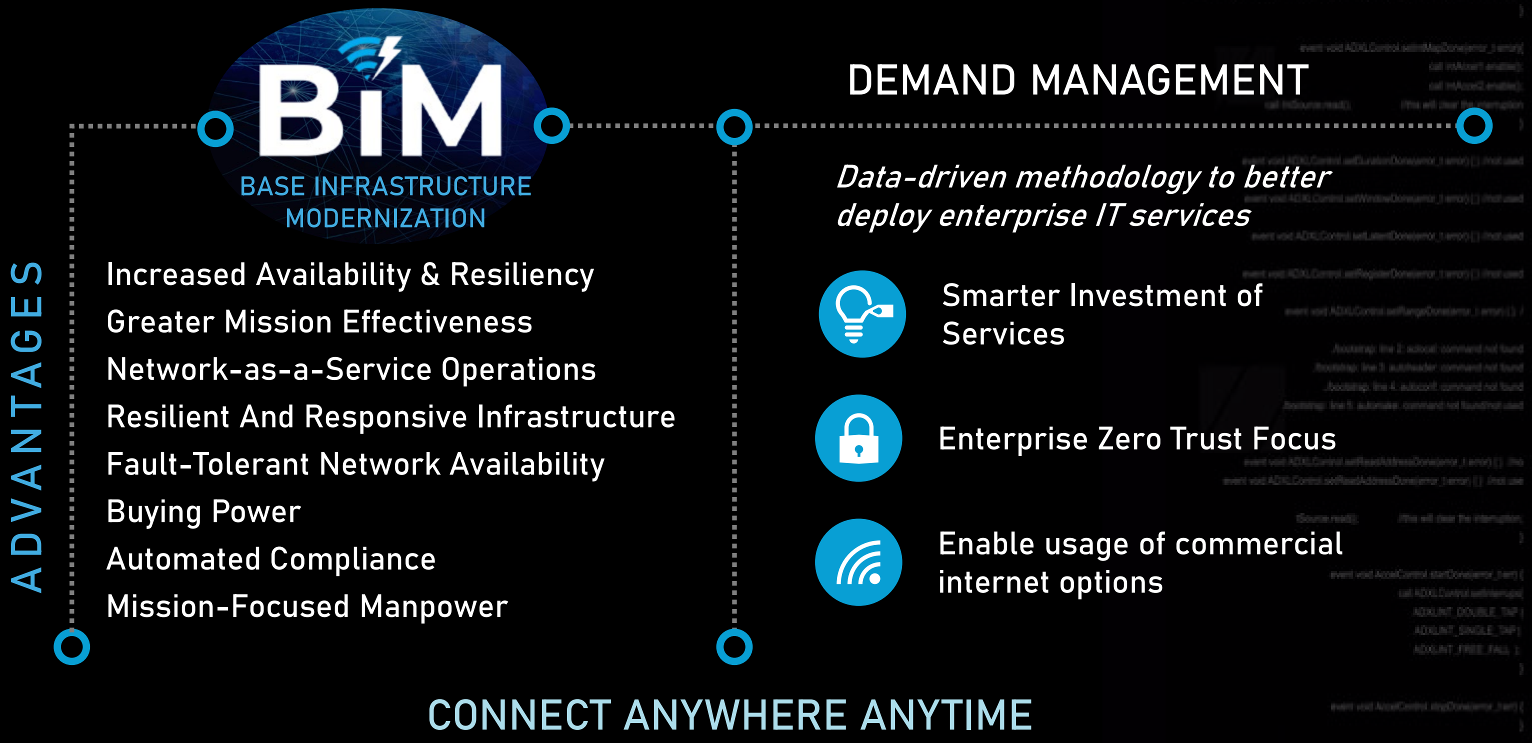
UX Driven

Transition to Enterprise As-a-Service Operations

- Modernize existing networks while deploying ‘As-a-Service’ Operations
- Leverage industry-leading commercial services
- Enhance operational capabilities of base personnel

Increased Availability & Economies of Scale

- Deliver modern network technologies to provide reliable performance
- Align network services to the mission, meeting operators where they are and where they are going
- Utilize COTS internet solutions to fulfill non -mission critical requirements



BiM

BASE INFRASTRUCTURE MODERNIZATION

ADVANTAGES

- Increased Availability & Resiliency
- Greater Mission Effectiveness
- Network-as-a-Service Operations
- Resilient And Responsive Infrastructure
- Fault-Tolerant Network Availability
- Buying Power
- Automated Compliance
- Mission-Focused Manpower

DEMAND MANAGEMENT

Data-driven methodology to better deploy enterprise IT services

- Smarter Investment of Services
- Enterprise Zero Trust Focus
- Enable usage of commercial internet options

CONNECT ANYWHERE ANYTIME

Figure II.D.1. Advantages to BIM and Demand Management

Impact to Warfighters

BIM will lay the foundation of DAF IT by modernizing DAF’s base area network (BAN) to increase availability, enable consistency, and incorporate emerging technologies as they become industry standards. Investing in BIM is key to creating base and network resiliency, which becomes increasingly important as we continue to posture ourselves for the newest geopolitical challenges our Nation faces.

Outdated IT systems impact operational effectiveness, as failure to upgrade these systems leads to increased maintenance costs and system downtime. BIM allows the DAF to buy down and manage technical debt by implementing a comprehensive process of upgrading, modernizing and optimizing base area networks that reside at every DAF Installation. This modernization will pave the way for increased **flexibility** for warfighters to perform their duties via new and adaptive technologies, transforming DAF Base Networks to highly performant architectures and ‘As-a-Service' operations.

II.D.1. BIM Consistency and Enhancements (Cont.)

Demand Management

- Reduce congestion on mission-critical networks to optimize utilization
- Align network resources to mission need based on operational effect

UX Driven

Demand Management

BIM and a formal Demand Management framework are central to the DAF's strategy to improve warfighter readiness. By shifting routine IT operations and supporting traffic away from mission networks, these initiatives enable Airmen and Guardians to concentrate on strategic tasks that directly affect operational success.

Optimizing Network Utilization

- BIM reduces congestion on mission-critical ("blue-wire") networks, preserving bandwidth and resiliency for combat operations, particularly in conflict with a near-peer adversary, missions with direct connection to the flightline, or other special missions
- Utilizes commercial networking technology where permissible to improve **UX** and maintain ubiquitous connectivity for Airmen and Guardians on base
    - Allows the DAF to adapt and adjust to hybrid working styles

Aligning Resources to Mission Priorities to Reduce Tech Debt

- Demand Management must align network services to validated mission needs
- Differentiates between mission-critical and non-critical users and systems ensuring resources are applied where they produce the greatest operational effect
    - Aims to standardize the enterprise service delivery approach to right-size costs of DAF network services and reduce tech debt
- Provides customized combinations of network services designed for distinct user groups/bases to support managing highly sensitive information (e.g., SCIFs, Crown Jewel Protection, Flightline Operations, and Special Access Programs) and enables direct connectivity from classified networks to the original secure location of the information

Impact to Warfighters

The net benefit to warfighters depends on the specific mix of technologies adopted and the rigor of their integration. Missions with stringent availability, latency, or security requirements will retain appropriately resilient connectivity. Conversely, operations that are not directly linked to mission criticality may transition to commercial alternatives. Demand Management must remain flexible, data-driven, and responsive to evolving operational risk.

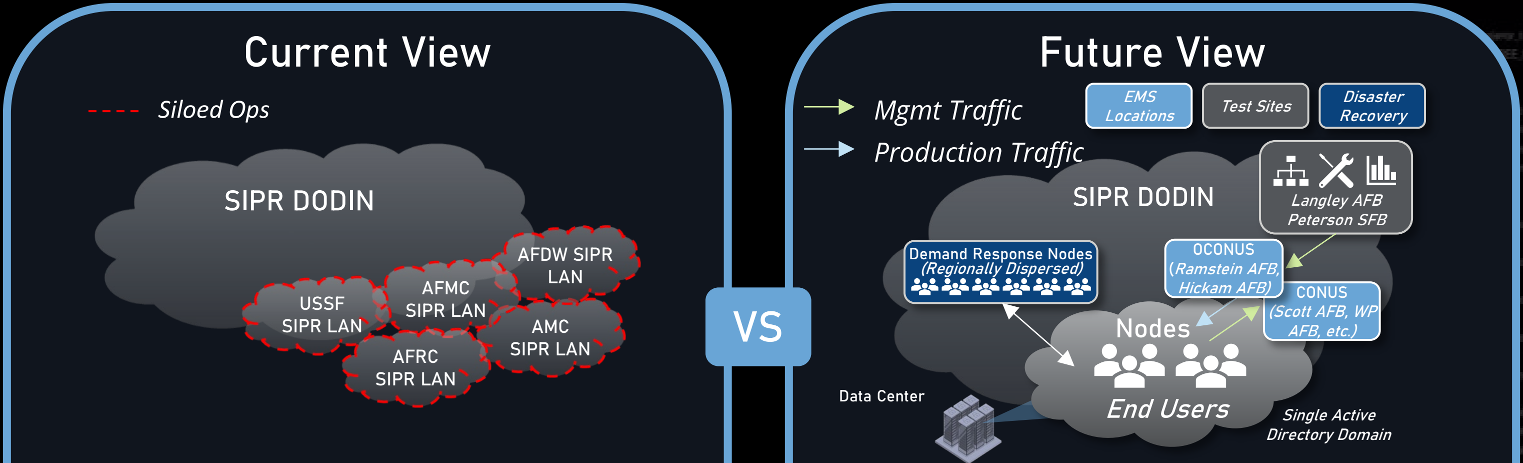
II.D.2. Centralized SIPR Domain

Shared Computing and Storage

- Remotely operate, manage and maintain the on -base hosting environment
- Consolidate and standardize core service stacks at the base level
- Create a federated domain

Survivability in Disconnected Operations

- Provide the minimum functionality to an installation, should it become disconnected from the DoD Information Network (DoDIN)



- Multiple legacy SIPRNet domains
- Not standardized, decentralized, with unique IDs per-domain per user

** Domains include ACC, AMC, AFMC, USSF, PACAF, USAFE, ANG, AFRC, AETC, AFDW

- Enterprise IT Service Management & standardization of SIPRNet
- Consolidation of core service operations
- Standardized AF SIPRNet configuration
- Hybrid GOCO/GOGO Construct

The DAF should collapse legacy SIPRNet domains under a unified management paradigm and establish a federated domain to simplify SIPR use and access

Figure II.D.2. Current and Future SIPR Configuration

Impact to Warfighters

Should a base or installation become disconnected from the DoDIN, there needs to be a way for the DAF to maintain **flexibility** to host core services. To do so, the DAF should establish an IPN infrastructure with the capacity to host capabilities beyond core services, including computing and storage for mission and other functional applications. These allow the DAF to provide basic functionality to an installation via disaster recovery sites, should it become disconnected from the DoDIN. The disaster recovery sites are configured to minimize latency while in CONUS and OCONUS locations.

With today's configuration, a new SIPR token must be requested for each domain, lengthening the process for those who need to work out of different bases. Additionally, should a base become disconnected from the WAN, there must be a way to validate a user's authentication certificate so that functionality is not lost. As such, the DAF should collapse legacy SIPRNet domains into a centralized paradigm. Online Certificate Status Protocol (OCSP) should be integrated to the solution to extend certificate validation capability, allowing longer periods of WAN disconnect before failure when operating at a fixed location.

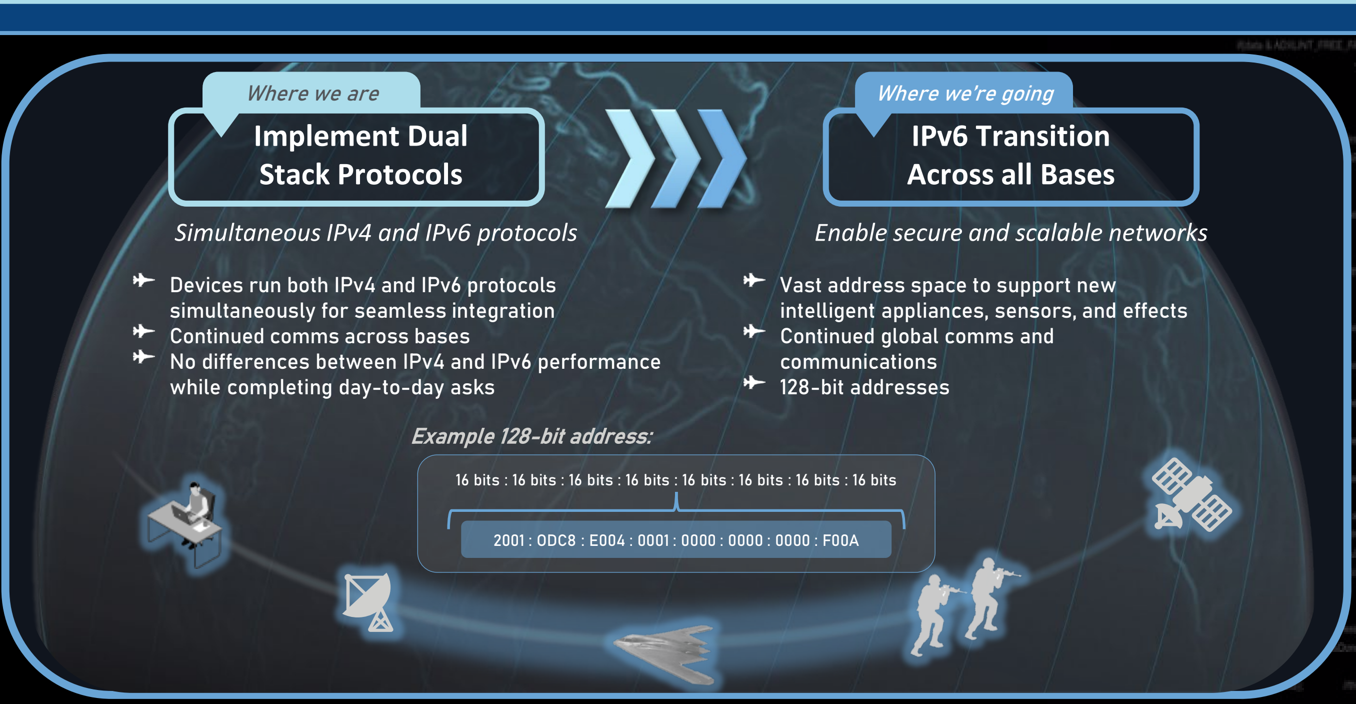
II.D.3. IPv6 Availability

Ongoing Transition to Dual Stack Protocols

- Implement dual stack Internet Protocol Versions 4 and 6 (IPv4/6) baseline on AFNET WAN & LAN
- Expanding to IPv6 to allow for more addresses

Future-State Migration to IPv6

- Ensure cyber defensive tools can account for all terrain
- After AFNET WAN is up, begin moving bases to IPv6



Where we are

Implement Dual Stack Protocols

Simultaneous IPv4 and IPv6 protocols

- Devices run both IPv4 and IPv6 protocols simultaneously for seamless integration
- Continued comms across bases
- No differences between IPv4 and IPv6 performance while completing day-to-day asks

Where we're going

IPv6 Transition Across all Bases

Enable secure and scalable networks

- Vast address space to support new intelligent appliances, sensors, and effects
- Continued global comms and communications
- 128-bit addresses

Example 128-bit address:

16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits : 16 bits

2001 : ODC8 : E004 : 0001 : 0000 : 0000 : 0000 : F00A

Figure II.D.3. Transition to Dual Stack and IPv6 [5]

Impact to Warfighters

Due to the rapidly growing number of network devices requiring routable IP addresses, the IPv4 address space is no longer sufficient to meet ongoing demand. Internet Protocol Version 6 (IPv6) has several advantages including address space expansion, enhanced security features, simplified network configuration, and improved mobility. IPv6 also simplifies network management with auto-configuration and eliminates NAT-related complexities, supporting efficient end-to-end connectivity and multicast services. As the DAF transitions to IPv6, they must ensure that all cyber defense posture tools function on both IPv4 and IPv6 via dual stack operation to minimize disruption during transition. To mitigate against the increased operational burden and increased attack surface of dual stack operations, the DAF should certify that IPv6 cybersecurity mechanisms implemented achieve a parity with their IPv4 mechanisms or better.

The DAF must ensure that their cyber defensive tools can account for terrain that includes IPv6 and clients using commercial Wi-Fi connecting through VPN or SDP. Expansion of IPv6 availability enables seamless integration with cloud environments, large-scale IoT networks, and mobile networking environments to increase **flexibility** for warfighters deployed in remote areas. Additionally, IPv6 allows for innovative security strategies, such as creating temporary networks that can be dismantled before adversaries can detect them.

II.E. Objective 5: Integrate the Network Environment

Enable interoperable networking and communications for all DAF Missions anytime, anywhere.

Summary

The DAF must ensure seamless network environment integration that enables communications for all missions. A key component of this success is the integration of Mission Partner Environments (MPE), which facilitates secure information sharing with trusted allies, significantly enhancing interoperability and overall situational awareness. Theater Deployable Communications (TDC) further extends agility, providing scalable communication capabilities to deployed forces at the tactical edge. By integrating MPE capabilities and TDC architecture, the DAF enables secure and reliable collaboration with mission partners, even in dynamic operational environments. This synergy between MPE and TDC will continue to be instrumental in the DAF's ability to support better-informed decisions and coordinated actions across the battlespace.

Enabling Capabilities

MPE

DoD Enterprise MPE

- U.S.-owned and operated under U.S. policy and regulations
- Globally integrated and operated day-to-day with our most-trusted partners and allies
- Primarily non -perishable data to be risk averse

DoD Expeditionary MPE

- CCMD/S/A governed, operated, and aligned with agreed-to standards
- Regionally and mission-focused operations shared with most trusted Allies and Partners
- Includes unanticipated mission partners, perishable data supports increased risk tolerance

TDC

Agile and Scalable Networks

- Wired and wireless connectivity provided by scalable deployable communications kit
- Point -to-point, point-to-multipoint, and mesh network connections that allow for wireless network extension
- Scalable for varying levels of user demand and changing mission requirements

Secure and Interoperable Communications

- Integrates with existing military communications systems
- Establishes secure information transmission

The DAF Battle Network

ABMS

C2ISR

Kessel Run

Airspace Mission Planning

II.E.1. MPE

DoD Enterprise MPE

- U.S.-owned and operated under U.S. policy and regulations
- Globally integrated and operated day-to-day with our most-trusted partners and allies
- Primarily non -perishable data to be risk averse

DoD Expeditionary MPE

- CCMD/S/A governed, operated, and aligned with agreed-to standards
- Regionally and mission-focused operations shared with most trusted Allies and Partners
- Includes unanticipated mission partners, perishable data supports increased risk tolerance

DAF MPE Execution

Connects Mission Areas and Mission Partners, including other MILDEPs, and enables information sharing capabilities at the strategic and operational level. By building a singular, agile MPE that integrates with external partners and mission specific infrastructure, and by leveraging robust ICAM, data tagging, and COP integration, the Air Force is positioned to lead in coalition operations—today and in the future

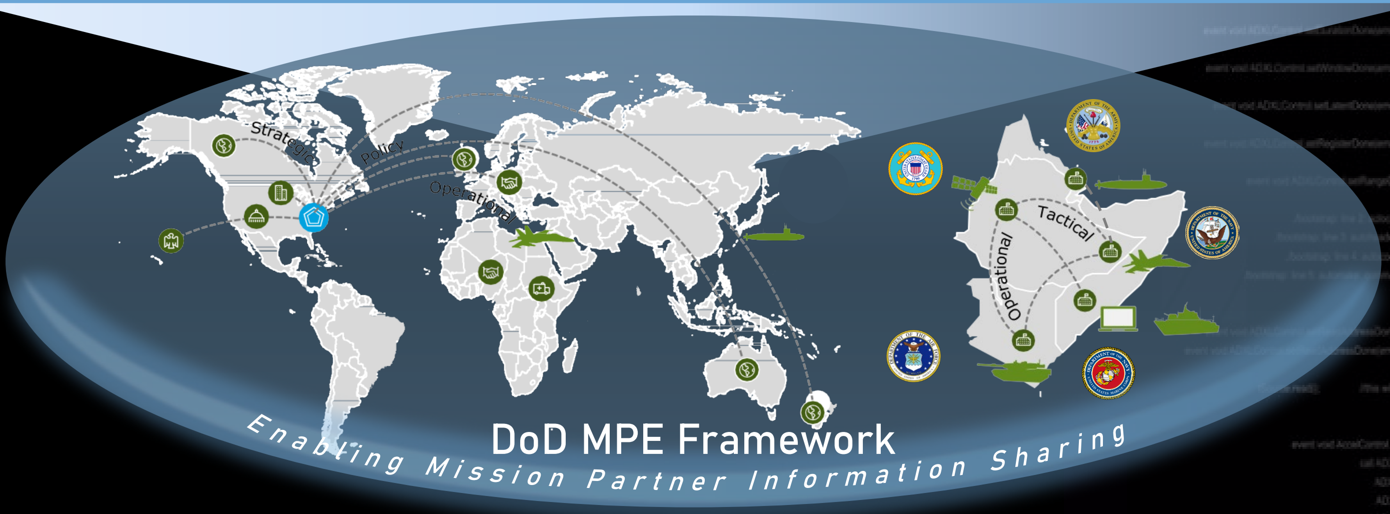


Figure II.E.1. DoD MPE Framework [6]

Impact to Warfighters

To establish a unified network, the DAF should develop and adopt a cloud-connected DAF MPE framework of common services, creating one cohesive enterprise network inclusive of existing allied networks. MPEs facilitate secure and efficient information sharing among joint US forces and trusted allies, guided by Zero Trust principles. Recognizing the diverse user base, a federated ICAM system is crucial to enable a decentralized approach to identity management while preserving each partner's control over their user base. Policy-based access control systems also rely on federated identities and data tagging for data security. This framework enhances **flexibility** for the warfighter by improving information exchange, enhancing shared situational awareness of the operational environment among the Joint Force and Mission Partners.

More collaboration is needed between MPE stakeholders to streamline identity integration. Current MPE implementations offer valuable insights into managing mission partner access. Ultimately, this approach will define architectural guardrails for managing sensitive data streams, such as moving data between Secret NOFORN and Secret REL TO, ensuring secure collaboration within weapons systems.

II.E.2. TDC

Agile and Scalable Networks

- Wired and wireless connectivity provided by scalable deployable communications kit
- Point -to-point, point-to-multipoint, and mesh network connections that allow for wireless network extension
- Scalable for varying levels of user demand and changing mission requirements

Secure and Interoperable Communications

- Integrates with existing military communications systems
- Establishes secure information transmission

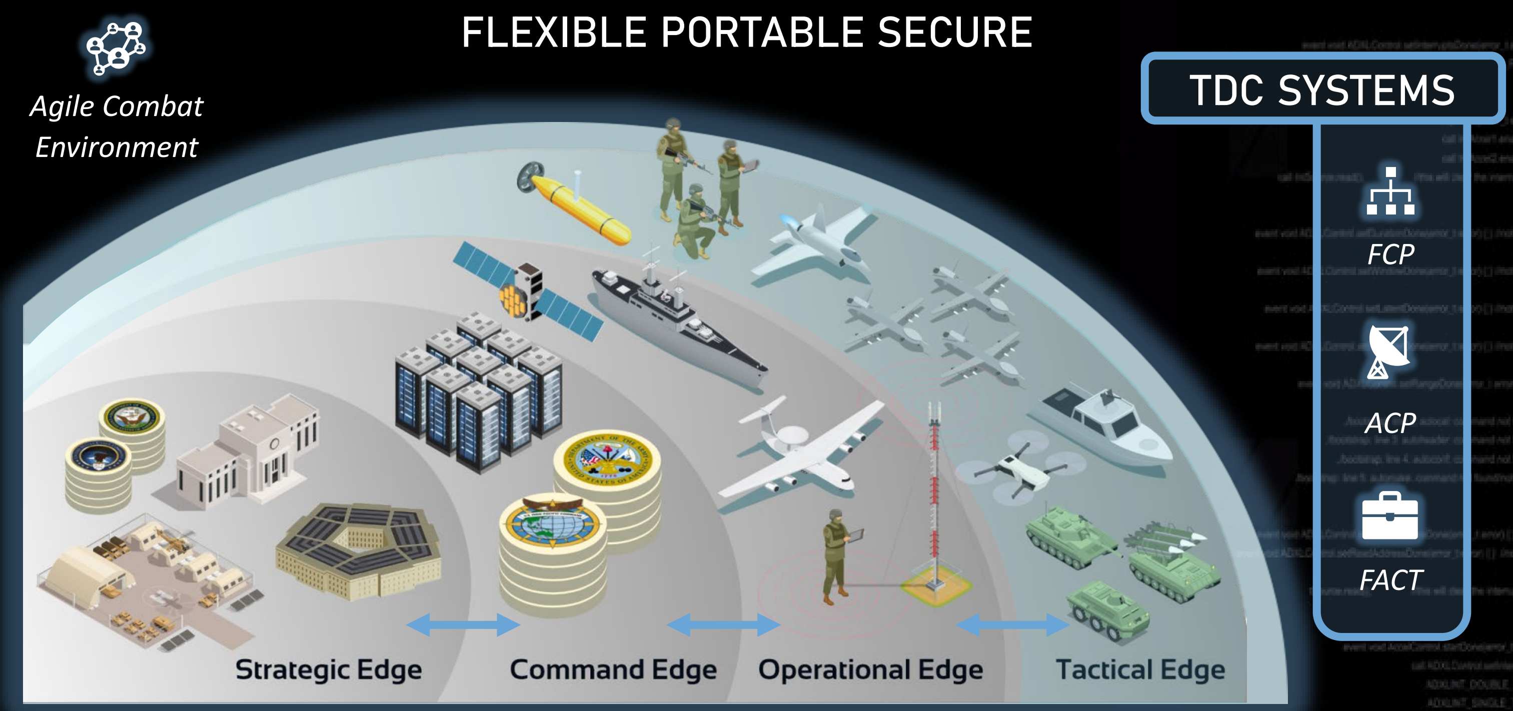


Figure II.E.2. Delivering TDC at all Edge Continuums [7]

Impact to Warfighters

To effectively serve warfighters at the tactical, or expeditionary edge, the DAF must enhance TDC and Flexible Communications Package (FCP) kits, ensuring a single, flexible architecture across the DAF that seamlessly connects to the enterprise and aligns with DISA standards. TDCs are portable communications systems that leverage COTS technology to send and receive secure messages, directly boosting warfighter **flexibility** by providing adaptable communication solutions in diverse operational environments.

To further enhance this flexibility and resilience, integrating mesh network capabilities into TDC communication kits creates self-forming, self-healing communication networks. This ensures resilient communication even when traditional infrastructure is damaged or unavailable, extending the reach of tactical communications and enabling more agile, distributed operations. Mesh networking capabilities also reinforce the need for an enterprise-wide CSfC implementation, extending classification mobility options. TDC kits enable warfighters to deploy in remote and emergency situations to establish secure communication at the edge, maintaining critical connectivity in rapidly changing situations. They are essential for enabling mobility, special operations missions, and disaster relief for secure communications across the force.

II.E.3. The DAF BATTLE NETWORK in Action

ABMS

- Fields aerial and terrestrial digital infrastructure, software and applications, and distributed nodes for C2 and battle management

C2ISR

- Provides acquisition and sustainment leadership supporting multiple operational weapons systems and mission critical capabilities

Kessel Run

- Delivers resilient C2 and targeting software capabilities that provide warfighters with decision advantage

Airspace Mission Planning

- Develops, delivers, and sustains world-class software solutions to enable full-spectrum mission planning and C2 for joint services warfighters

DAF BATTLE NETWORK Technical Architecture

DAF PEO C3BM Architecture & System Engineering (ASE)

ABMS

C2ISR

Kessel Run

Airspace Mission Planning

NETWORK IN ACTION

The DAF BATTLE NETWORK, and ABMS's efforts represent the **culmination of enabling capabilities** listed throughout this strategy.

Mission Optimization

Global Access

Streamlined Developer and User Accessibility

Globally Distributed C2NSOC Management

Impact to Warfighters

DAF PEO C3BM, along with BMC3I, C&N, ES, RCO, SDA, and MILSATCOM, delivers an integrated DAF BATTLE NETWORK, the systems-of-systems connecting sensor, effector, and logistics systems to enable better situational awareness, faster operational decisions, and decisive direction to the force. The DAF BATTLE NETWORK employs a "best of breed" approach to capability delivery by prioritizing risk management to optimize the delivery of mission thread closing solutions with **secure** and resilient infrastructure, empowering proactive actions within an adversary's decision cycle.

The DAF requires resilient, diverse, and secure connectivity with seamless cloud capabilities and a robust data fabric for a total approach solution. Targeted outcomes include Mission Optimization enabled by SD-WAN for optimized transport routing, Global Access via federated connectivity to SIPRNet and JWICS, Streamlined Developer And User Accessibility facilitated by a standardized interface for app development and rapid deployment to the Cloud, and Globally Distributed Command and Control Network Security Operations Center (C2NSOC) Management supported by automation, training, resilience, and reduction of resources needed to secure network across all DAF Command and Control (C2) Mission Sets [ii].

II.F. Objective 6: Enable the Workforce of the Future

Our competitive edge relies on both the Network of the Future and the readiness of our Airmen and Guardians.

UX Driven

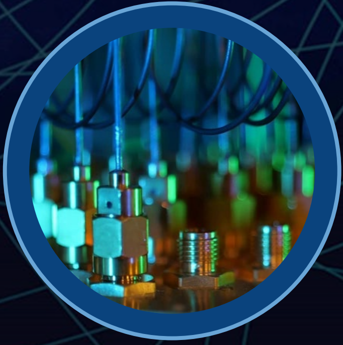
The future of DAF technology...

Communicate messages of all classification level to CONUS and OCONUS locations

Automate robots to bring supplies to the tarmac for maintainers

Identify parts and place orders for replacements while on the shop floor with AR

Access the network from any base, anytime



Encode information with single-direction photon polarization enabled by quantum networking

3D scan parts to rapidly and accurately reproduce or repair, reducing downtime

...is enabled by the Network of the Future...

The Network of the Future is a robust, agile backbone that will enable enterprise innovation and pave the way for ubiquitous connectivity, enabling emerging technologies to become industry standards.

...and bolstered by our Workforce.

It is equally important that the workforce is equipped with the skills and knowledge to operate and maintain these systems. Preparing our warfighters to understand, manage, and optimize next-generation networking technologies will be critical to ensuring mission success and delivering a high-quality UX. Here is how you can do your part to upskill and drive progress across the DAF.

Explore our Training Resources

Expeditionary Operations 🔗

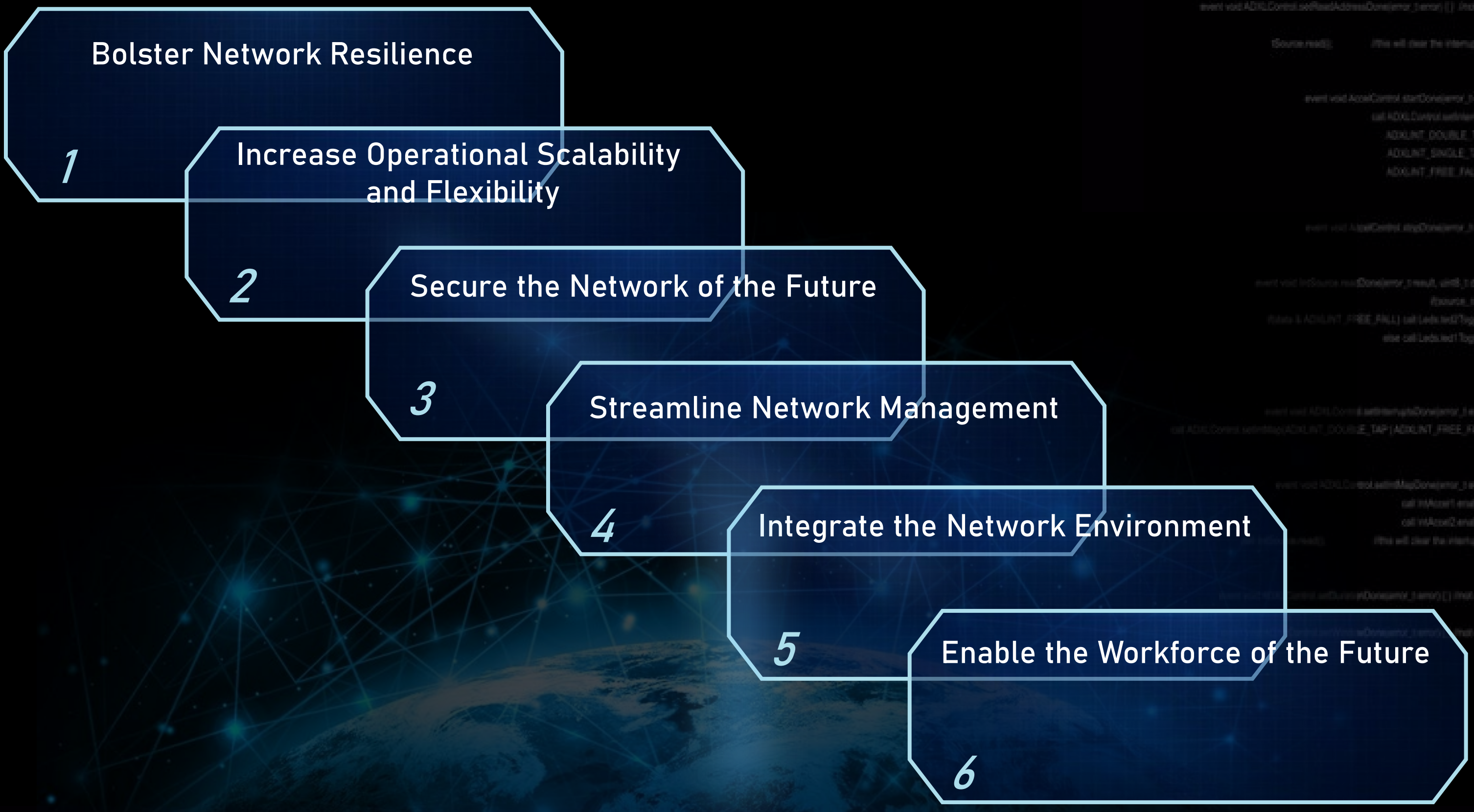
DAF e-Learning Services 🔗

myLearning 🔗

III. CONCLUSION

In summary, the DAF's Network of the Future must strike a deliberate balance between security and flexibility, ensuring both operate in tandem to empower the warfighter and continually improve UX. Achieving true decision advantage on the battlefield demands more than modernized technology, but also an unwavering commitment to strengthening network resilience, maximizing operational agility, fortifying security, simplifying management, continuous training and unifying the diverse network environments. By placing the warfighter at the center of every innovation, we transform technology progress into operational dominance and mission success where it counts most. Relentlessly pursuing these objectives ensures we outpace our adversaries and keep the DAF agile, adaptive, and fully prepared to meet any challenge, anytime, anywhere.

Our goal for this document is to drive a cohesive vision where we can bring next generation capabilities to our Airmen and Guardians worldwide. Together, we are responsible for shaping a resilient, secure, and agile network to provide ubiquitous connectivity that empowers our force, adapts to any threat, and enhances operational effectiveness. The future demands decisive action. Together let's champion innovation, integrate security with flexibility, and make every connection count. The next era of operational dominance starts now!



1 Bolster Network Resilience

2 Increase Operational Scalability and Flexibility

3 Secure the Network of the Future

4 Streamline Network Management

5 Integrate the Network Environment

6 Enable the Workforce of the Future

IV. APPENDIX

IV.A. Acronyms (1 of 2)

ACRONYM	EXPANSION
ABAC	Attribute-based Access Control
ABMS	Advanced Battle Management System
ACP	Agile Communications Packages
AFNET	Air Force Network
AI	Artificial Intelligence
AOR	Area of Responsibility
AR	Augmented Reality
BAN	Base Area Network
BIM	Base Infrastructure Modernization
BMA	Business Mission Area
C2	Command and Control
C2C	Comply to Connect
C2ISR	Command, Control, Intelligence, Surveillance, and Reconnaissance
C2NSOC	Command and Control Network Security Operations Center
CCMD/S/A	Combatant Command/Service/Agency
CDS	Cross Domain Solution
CEDC	Component Enterprise Data Center
CIO	Chief Information Officer
CJADC2	Combined Joint All-Domain Command and Control
CONUS	Continental United States
COP	Common Operational Picture
COTS	Commercial-Off-the-Shelf
CSfC	Commercial Solutions for Classified

ACRONYM	EXPANSION
CTO	Chief Technology Officer
DAF	Department of the Air Force
DDIL	Denied, Degraded, Intermittent, and Limited
DIMA	Defense Intelligence Mission Area
DISA	Defense Information System Agency
DNS	Domain Name System
DoD	Department of Defense
DODIN	Department of Defense Information Network
DR	Disaster Recovery
EDR	Endpoint Detection and Response
EIEMA	Enterprise Information Environment Mission Area
EITaaS	Enterprise Information Technology as a Service
EMS	Enterprise Management System
FACT	Fly-Away Communications Terminal
FCP	Flexible Communications Package
GOCO	Government-Owned, Contractor-Operated
GOGO	Government-Owned, Government-Operated
ICAM	Identity Credentials Access Management
ID	Identification
IDS	Intrusion Detection Systems
IL	Impact Level
IoT	Internet of Things
IP	Internet Protocol

IV. APPENDIX

IV.A. Acronyms (2 of 2)

ACRONYM	EXPANSION
IPN	Installation Processing Node
IPS	Intrusion Prevention Systems
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Information Technology
JADC2	Joint All-Domain Command and Control
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LEO	Low Earth Orbit
MFA	Multi-Factor Identification
MPE	Mission Partner Environment
NAT	Network Address Translation
NGG	Next Generation Gateway
NIPRNet	Non-secure Internet Protocol Routed Network
NOFORN	Not Releasable to Foreign Nationals
NPE	Non-Person Entity
NSA BOD	National Security Agency Binding Operational Directive
OCONUS	Outside the Continental United States
OCSP	Online Certificate Status Protocol
PAM	Privileged Access Management

ACRONYM	EXPANSION
PDP	Policy Decision Point
PEP	Policy Enforcement Point
REL TO	Releasable To
RFK	Radio Frequency Kits
SaaS	Software as-a-Service
SASE	Secure Access Service Edge
SATCOM	Satellite Communications
SCIF	Sensitive Compartmented Information Facility
SDP	Software Defined Perimeter
SD-WAN	Software-Defined Wide Area Network
SIPRNet	Secure Internet Protocol Routed Network
SSE	Secure Service Edge
TDC	Theater Deployable Communication
TS	Top Secret
USSF	United States Space Force
UX	User Experience
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network
WAN	Wide Area Network
WMA	Warfighting Mission Area
XDR	Extended Detection and Response

IV. APPENDIX

IV.B. Figure Table

IV. APPENDIX

IV.C. Reference Table

Diagrams included in the Network of the Future Strategy were abstracted from public resources and are not meant to be prescriptive of DAF specific technologies, programs, specifications, etc.

ID	FIGURE RESOURCES	PAGE
[1]	SD-WAN: Digital Transformation with SDN	8
[2]	Learn About Cross Domain Solutions	11
[3]	NSA COMMERCIAL SOLUTIONS for CLASSIFIED	12
[4]	Disruption Tolerant Mobile Wireless Networks for Defense and Homeland Security	13
[5]	DoD Instruction 8440.02	20
[6]	Zero Trust: Enabling Partnerships for a Warfighter Decision Advantage	22
[7]	Employing artificial intelligence and the edge continuum for joint operations	23
ID	**TEXT RESOURCES**	**PAGE**
[i]	The Emerging Potential for Quantum Computing in Irregular Warfare	4
[ii]	DAF BATTLE NETWORK	24
ID	**FOOTNOTES**	**PAGE**
[A]	Figure II.A.2 Transport Methods offers a generalized overview and does not reflect all nuances of evolving technologies (e.g., advanced PLEO satellites, hyperscalers, etc). As these technologies progress, ongoing analysis should supplement this network strategy to maintain accuracy and relevance.	9
[B]	References to C2C throughout this document are intended solely for the purposes of outlining DAF strategy and initiatives. These references are not intended to address, interpret, or fulfill any Congressional mandates related to the C2C program. For matters pertaining to Congressional requirements or compliance, please refer to official policy documentation and guidance.	14