LINE OF EFFORT #1: ACCELERATE CLOUD ADOPTION
CHAMPION: Mr. Bonci

- Update DAF Cloud Strategy to include OCONUS, hybrid-edge integration including disconnected operations, multi-vendor and multi-level security elements ensuring the seamless movement of data from anywhere to anywhere.

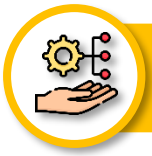
LINE OF EFFORT #2: THE FUTURE OF CYBERSECURITY
CHAMPION: Mr. Bishop

- Baseline the DAF cyber posture measurement framework to understand and articulate cybersecurity risk to include visibility of readiness, assessments, and compliance. This cyber posture will feed operational risk reviews across the DAF.
- Streamline and clarify Cyber roles and responsibilities aligned with statutes and DAF, USAF, and USSF agreed-upon direction.
- Coordinate with AF/A30 Mission Assurance Teams, and related OCRs, to establish Cybersecurity MARPA processes. Upon DCA, TCA, and DCI identification, advocate for resourcing to complete MRT-C mapping of assets and infrastructure. Leveraging existing assessments, and new mapping efforts, perform cybersecurity posture analysis. Leverage results to create risk informed messaging and advocate for resourcing to enhance critical infrastructure resiliency.
- Publish an Enterprise Software Bill of Materials (SBOM) service strategy and policy framework to support the security of our critical software supply chain, in line with existing DoD efforts.

LINE OF EFFORT #3: WORKFORCE
CHAMPION: Dr. Hardiman

- Implement and maintain DoD 8140 Qualification Program to enhance overall readiness of the workforce; publish and implement DAFMAN 17-1305 (DoD Cyber Workforce Strategy Implementation Plan Initiative 2.3.1).
- In collaboration with ACC, AETC, and AF/A1, define enterprise approach to capture specialized experience identifiers (SEI) in order to track cyberspace and IT talent and skills inventory in order to meet missions needs (utilizing manpower and personnel systems and training tools, i.e. MyVector, DCPDS, MyLearning, Digital University, ETC.).
- The Department must champion compensation flexibilities to expand opportunities across the cyber workforce. This is possible by enhancing authorities, pay flexibilities and incentives for civilian cyber professionals, to include the Cyber Excepted Service (CES), beyond existing levels to make DAF competitive and address talent gaps. The goal is to evaluate the effectiveness of recruiting and retention efforts through compensation (DoD Cyber Workforce Strategy Initiatives: 1.1.1; 2.2.2; 2.2.3; 3.6.1).

- Many enterprise talent management programs are not tracked through authoritative systems, creating challenges in understanding existing talent. The goal is to enhance the ability in identifying and tracking cyber requirements (e.g. training, qualifications, resources and compliance) utilizing cyber work roles and proficiency levels. Executing system change requirements will allow MPES cyber data to feed into DCPDS as the authoritative source. Additionally, create a unique identifier in MPES to delineate CES from all other cyberspace positions (DoD Cyber Workforce Strategy Initiatives: 1.1.1; 1.2.1; 1.2.2; 1.2.3; 1.3.2; 1.3.3).
- In collaboration with ACC, identify available cyber workforce training sources, core competencies, and gaps; develop training repository; and create training governance framework to manage training across the cyber workforce.
- Establish processes and procedures for using specialized experience, training, and experiential assignments to offer bonuses/incentives, affect promotions, and identify key position placements.
- The Department must review workforce capabilities and requirements on a regular basis (e.g., bi-annually, annually) to support workforce planning efforts and data-driven decision making. The goal is to enhance advanced analytic capabilities to increase the speed, accuracy and efficiency of cyber requirement reviews. This is possible by automating cyber workforce reports and assessing metrics through readily accessible dashboards (DoD Cyber Workforce Strategy Initiatives: 1.1.1; 1.2.3; 1.3.2; 1.3.3).
- As the cyber workforce continues to evolve and new communities are reflected in the DoD Cyber Workforce Framework (DCWF), the Department requires standard tools to aid in the understanding and application of work roles for coding and other human capital initiatives. Additionally, all civilian cyber positions must be coded IAW DoD 8140 to enable workforce planning and talent management activities. The goal is to accurately code all civilian recognized cyberspace and CES positions in MPES and DCPDS (DoD Cyber Workforce Strategy Initiatives: 1.1.1; 1.2.1; 1.2.3; 1.3.2; 1.3.3).



LINE OF EFFORT #4: IT PORTFOLIO MANAGEMENT (PfM)
CHAMPION: Mr. Beauchamp

- Enforce CPIC to provide IT Portfolio transparency across the DAF by: (a) Provide CPIC Proof of Concept for system level IT Portfolio Transparency , and (b) continue ITIPS modernization efforts to include CPIC components.
- Implement TBM as a foundational capability for the DAF, establishing cost transparency and aligning cost to mission and value.
- Fully Operationalize Digital Experience Monitoring: Assess capabilities/limitations of Microsoft Enterprise Monitoring Tools and provide "total cost of ownership" analysis to inform paths to integrate/transition to these tools where appropriate.
- Develop IT Modernization Planning and Implementation Guide to ensure all Mission Areas can maximize use of Enterprise IT Capabilities and Resource Support.
- Streamline Enterprise IT services through strategic sourcing and category management. This process will involve collaborating with the DoD ESI Team, DAF IT Category Management Council, AFICC [w/ 771st ESS], and others to choose the best execution site. Create a roadmap for promptly preparing EAs for Hardware, Software, and any related IT Services while discontinuing

redundant procurement channels. For FY24, codify a DAF strategic position for acquisition and sustainment for at least three (3) products (e.g., Gartner, ServiceNow, and Salesforce). With the option to exceed—by adding even more products.

- Policy Management Alignment: Assess existing policies and establish a Policy Plan of Action and Milestones to track the identification, development, and coordination of IT policies to address known gaps of IT management, to include cancelling or editing existing policies and regulations or guidance, incorporating authorities of HAF MD 1-26, assigning roles and responsibilities, and incorporating enforcement mechanisms (i.e. internal controls (Preventative and Detective)). Develop new AFI/AFMANs where policies and/or governance are lacking.

LINE OF EFFORT #5: EXCELLENCE IN CORE IT & MISSION-ENABLING SERVICES
CHAMPION: Mr. Bonci

- Publish a network strategy including SIPR 2.0, Battle Network integration, and Network of the Future.
- Publish an end user device strategy including alternate platforms/BYOAD with the goal provide for the future of work and increase accessibility to required digital resources (may become a subset of the Device as a Service Strategy).
- Publish DevSecOps Enterprise Support Strategy: Identify Enterprise services necessary to deliver to the DevSecOps enterprise and provide a clear path to production and full API integration.

LINE OF EFFORT #6: DATA & AI
CHAMPION: Ms. Donelson

- Publish the initial DAF enterprise metadata standards for data sources and data sets and an enterprise data catalog.
- Deploy a business model for the DAF data platform ecosystem.
- Deploy data services operations and interoperability plan to enable, ensure, and empower business enterprise efficiency, mission operations capability, and warfighting capacity.
- Stand-up and execute DAF Data and Artificial Intelligence Governance to assure compliance with statutory guidance, Federal regulation, DoD and DAF policies.
- Establish enterprise DAF Data and Artificial Intelligence Strategy.
- Draft, coordinate, and release a development and acquisition handbook for data and AI technical solutions or services.