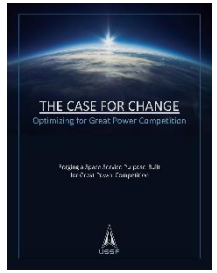
Department of the Air Force

DAF Cyber Strategy

Overall Classification of Briefing: Unclassified

Dr. Wanda T. Jones-Heath, SES
DAF Principal Cyber Advisor
24 September 2024

Strategic Thoughts



Secretary Kendall

The Department of the Air Force is working plans for reshaping, refocusing, and reoptimizing the Air Force and Space Force to ensure continued supremacy in those domains while also better posturing the services to deter and, if necessary, prevail in an era of Great Power Competition.

We are out of time!

Gen Allvin

Since the dawn of airpower, our proud heritage in history has been intertwined with key events in combat that have shaped … a notion in some cases, the world. Those are seminal events.

What's our next seminal event? I don't know, but I do know that right now we are in a time of consequence. What we do now matters.

We will not turn away. We will lean into it. The stakes are high, and the time is now.

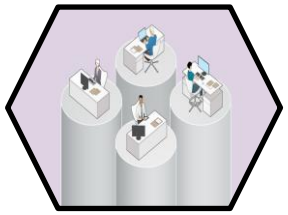
Gen Saltzman

We were created for this new space era; an era increasingly characterized by great power competition. This was the genesis of the Space Force, a military service focused on addressing the challenges and opportunities we face in the space domain.

As good as we are, as much as we've done, as far as we've come, it's not enough. We are not yet optimized for Great Power Competition.

Strategic Landscape

The fast-changing cyberspace landscape demands rapid action across the Department of the Air Force and DoD; however, the lack of synchronized, enterprise-level approach to address mission assurance and associated cyberspace vulnerabilities puts our people, processes, and technology at risk and hinders our ability to fully exploit the cyberspace domain to execute Air and Space Forces core missions.



Siloed Approaches

Visibility of Enterprise-level Cyber & IT

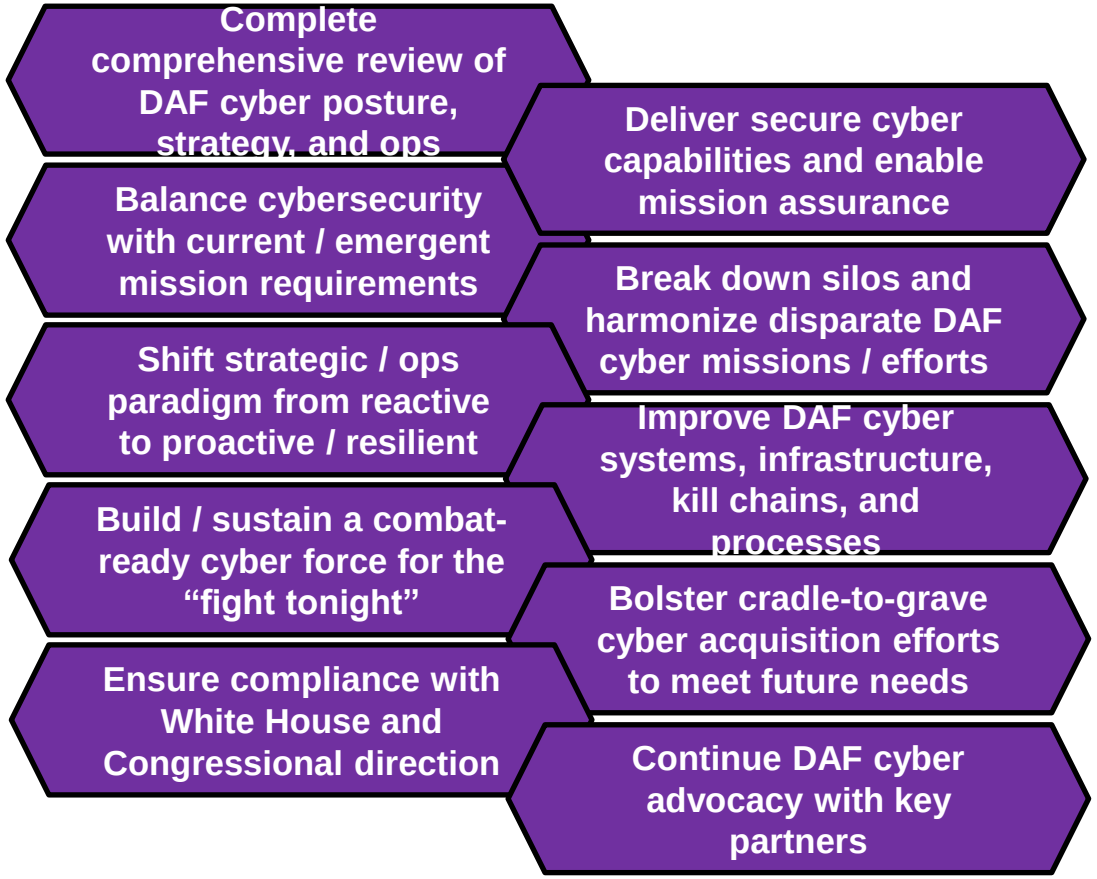
Cyber & IT investments

Unity of Efforts

Top Cyber Talent

Enterprise-level Governance

Outcome-Based Change for DAF Cyber & IT



Goal: Drive a Synchronized, Evolved, and Executable DAF Cyber & IT Portfolio

What Drives the Need?

Global Threat Landscape

PRC

- Cyber Espionage
- Cyber Attacks on Critical Infrastructure
- Support for Digital Authoritarianism
- Military Modernization
- Influence & Surveillance

Russia

- Cyber Espionage & Attacks
- Malign Influence Operations
- Cyber Support for Kinetic Warfare
- Destructive Cyber Attacks
- Collaboration with Cyber Criminals

N Korea

- Cyber Espionage & Criminal Activity
- State-Sponsored Cyber Crime
- Disruption of International Stability

Iran

- Cyber Espionage & Political Interference
- Cyber Attacks on Critical Infrastructure
- Targeting Critical Infrastructure
- Cyber Retaliation and Punishment

VEO

- Cyber Propaganda and Recruitment
- Command and Control
- Emerging Cyber Threats

Achieving and maintaining superiority in the cyberspace warfighting domain will be a critical factor in countering the aggregation of technologically advanced threats.

Cyberspace capabilities must be integrated with conventional military, space, and information warfare strategies to effectively address the full spectrum of security challenges these actors present.

Strategic Approach

DoD Cyber Strategy

- Disrupt and degrade malicious cyber actors
- Campaign in and through cyberspace to support joint force objectives
- Protect the cyber domain with allies and partners
- Build enduring advantages in cyberspace

DAF Cyber Principles

- Build a Robust, Resilient, & Ready DAF Cyber enterprise
- Enhance the DAF's Cybersecurity & Cyber Defense Posture
- Leverage DAF Cyber to enable DoD & National Goals
- Fully integrate & synchronize Information Warfare capabilities

Cyber LOEs

Reshape the DAF Cyber Workforce

Invest in the future of DAF Cyber

Secure the DAF Cyber enterprise

Evolve the DAF Cyber Industrial Base

Accountability

People | Process | Technology

Desired Outcome: Accelerate change within the cyber enterprise – One Team, One Fight!

Reshape the DAF Cyberspace Workforce

Recruit

College and University

- Senior Military Colleges
- Trade and Technical Colleges
- HBCU, HSI, and others
- Newly trained on recent research

Professional Organizations

- Cyber/IT professionals
- Depth of experience in the field
- Degree agnostic

Retain

U.S. AIR FORCE

UNITED STATES SPACE FORCE

AIR FORCE CIVILIAN SERVICE
Forces. Joined.

DAF Cyber & IT Personnel

- Cyber Excepted Service
- Technical Track
- Warrant Officers
- Direct commissions
- Awards/Incentives
- Increased training opportunities

Leverage

Reserve Component

- Civilian Experience
- Military training
- Connections outside DAF, DoD
- Guard maintains unique authorities to work with state agencies

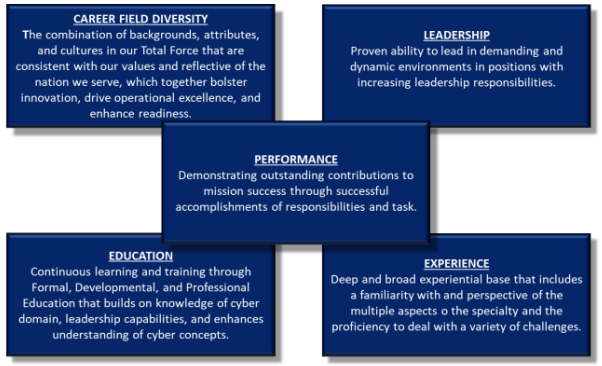
Industry/Academic Partners

- Contract services
- Think tanks
- FFRDC
- University partnerships

Invest in the Future of DAF Cyberspace

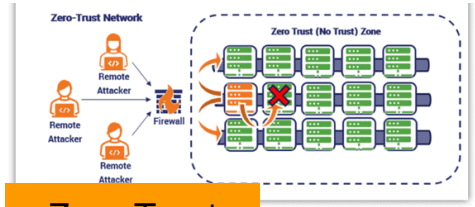
People

- Warrant Officers (Military, Street-to-Seat)
- Innovative cognitive assessment opportunities
- Promoting data workforce culture
  - Data & AI SEIs
- Upskilling workforce at their pace
  - Digital University, MIT accelerator, DAF e-Learning



Technology

- AI/ML – cyber tooling and automation
- NIPRgpt
- Zero Trust
- OT and ICS/SCADA solutions (investigating scalable solutions)
- Post-quantum cryptography
- Quantum Technologies (Computing, QAI/ML)

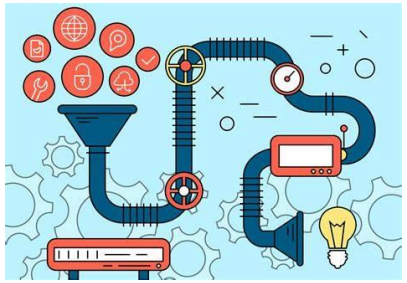


Zero Trust

Post Quantum Cryptography

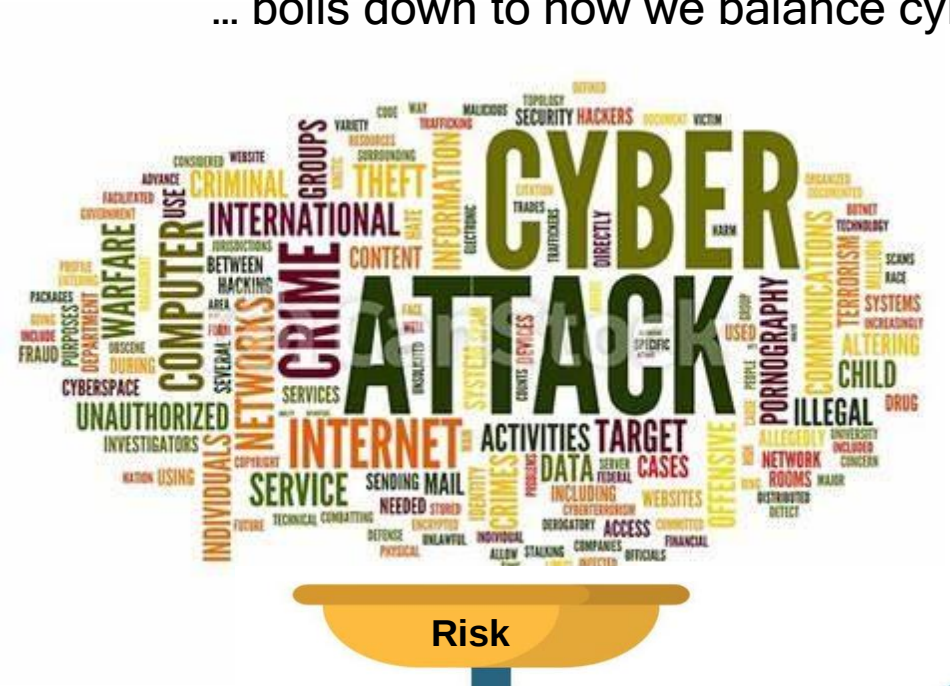
Processes

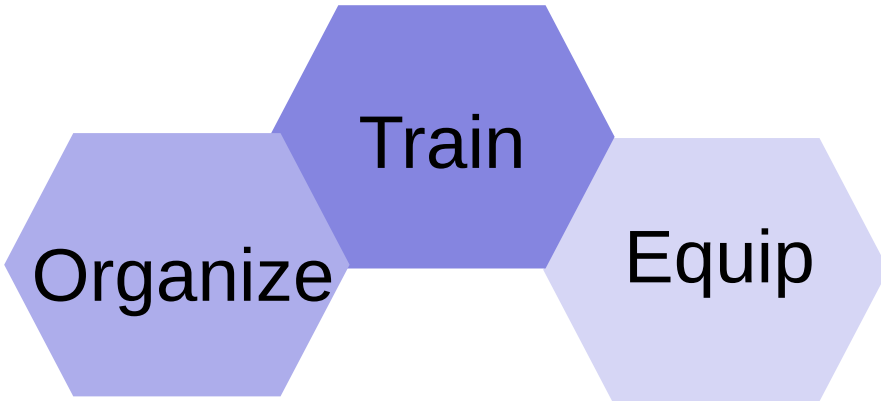
- Governance
  - Cyber Resiliency of Weapons Systems
  - Cyber Resiliency of Operational Control Systems
  - Strategic Cyber Security Program
  - Cyber Security & Cyber Defense (Senior leader DAF awareness)

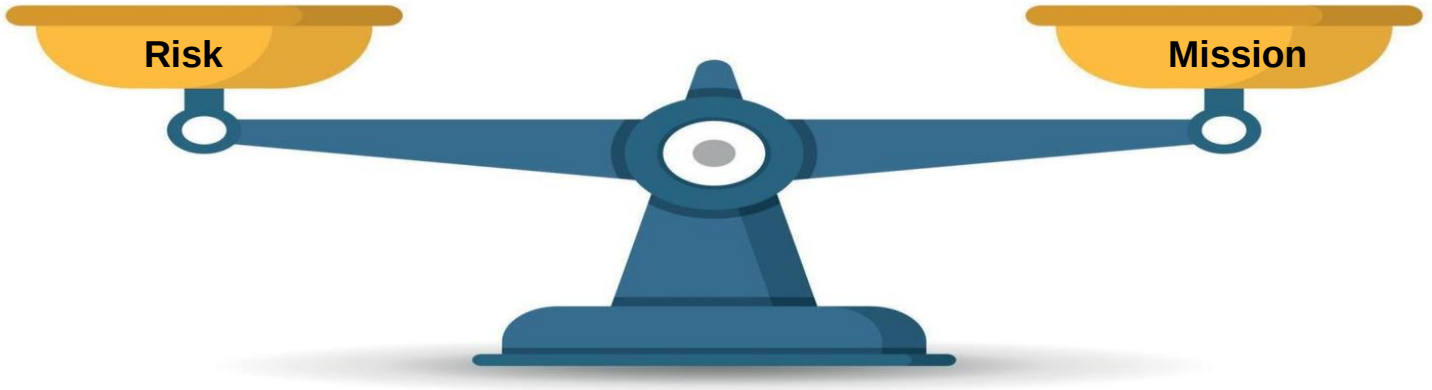


Secure the DAF Cyberspace Enterprise

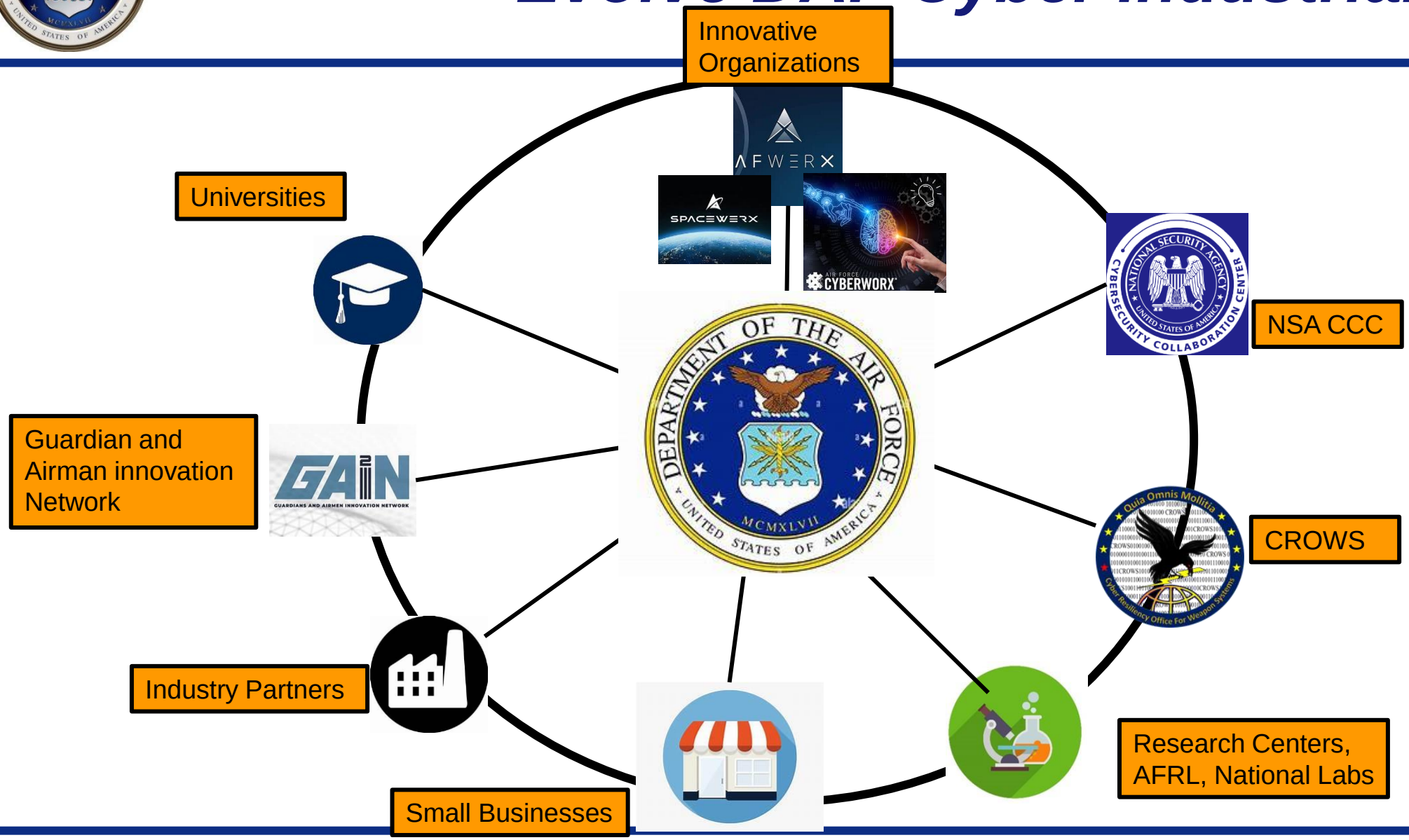
… boils down to how we balance cyber-security risk and operational mission risk







Evolve DAF Cyber Industrial Base



QUESTIONS