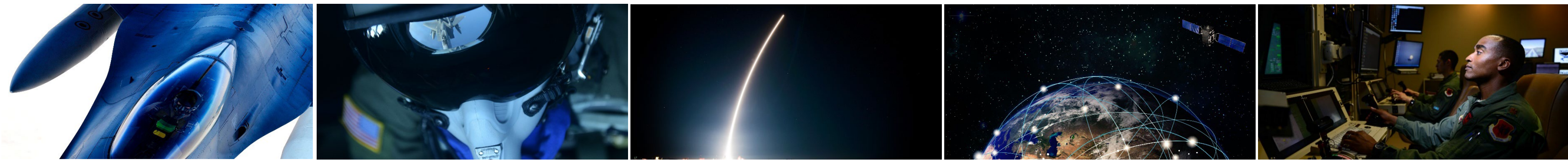




CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS



Education & Training for Resiliency in Cyber Contested Environments

Mr. Steven A. Stolly

Team Lead, Education & Training (Manpower), Cyber Resiliency Office for Weapon Systems

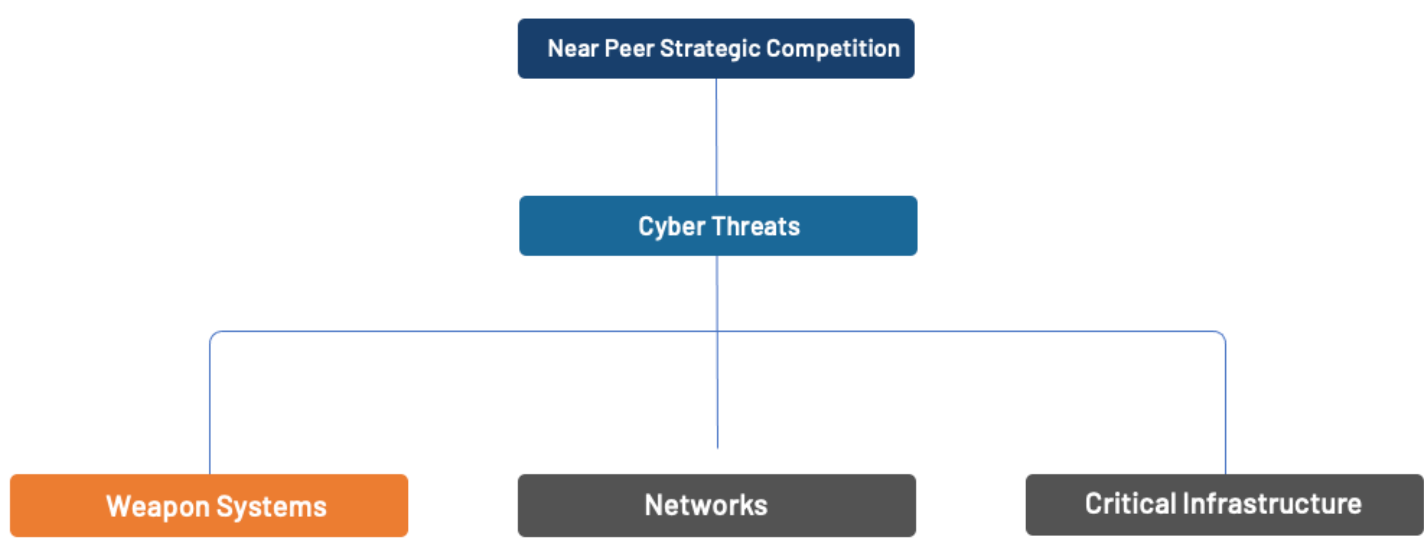
AFLCMC.CROWS.EDU@US.AF.MIL



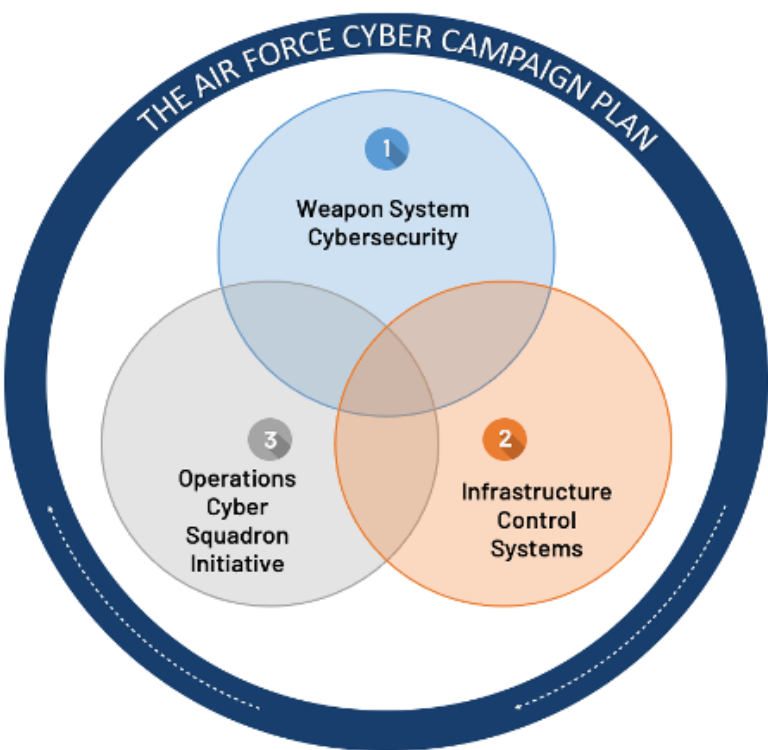


CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

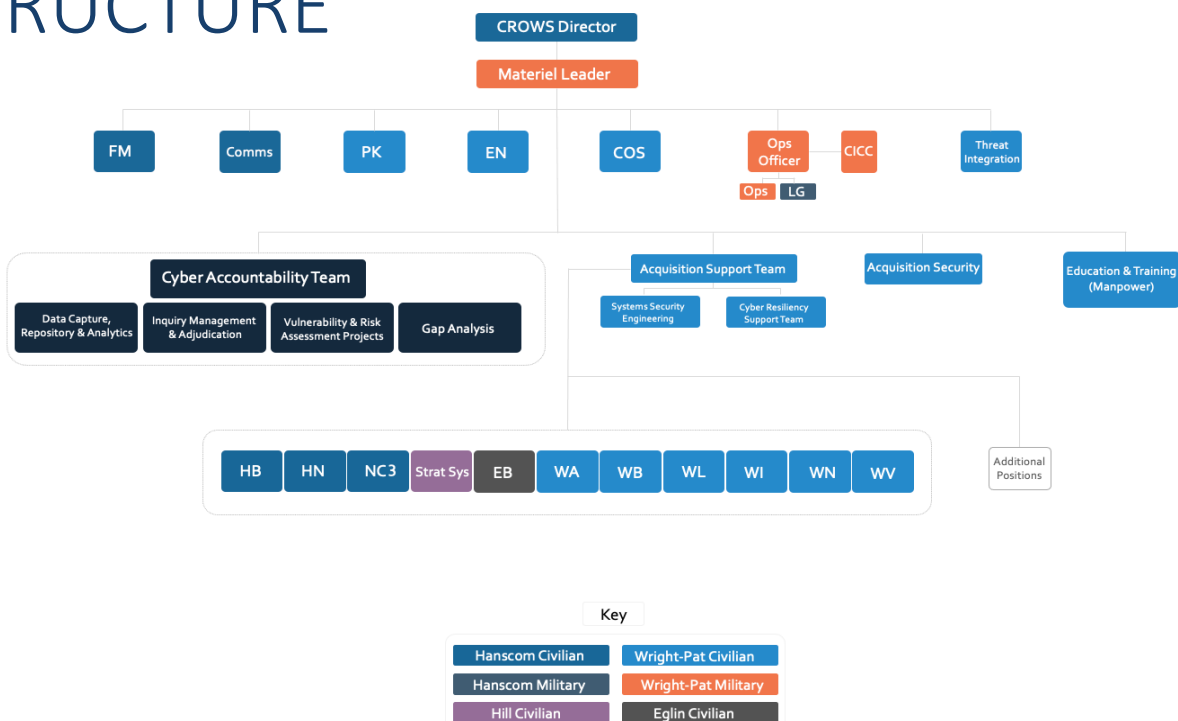
● National Defense Strategy



HISTORY



STRUCTURE



Acquisition Support Team

● Acquisition Support Team

How the Acquisition Support Team Impacts the CROWS Cyber Resiliency Mission

Train and deploy Cyber Focus Teams capable of integrating cybersecurity and cyber resiliency measures into all phases of the acquisition process

Integrate Systems Security Engineering into Systems Engineering

Provide advice and consultation to the weapon system cyber workforce in applying emerging cyber resiliency requirements, tools, techniques, and guidance

Integrate best practices and lessons learned across the acquisition enterprise

Institutionalize Acquisition Security and establish a common security operating environment to ensure Cyber Resiliency in Department of the Air Force Weapon Systems

Education, Training, & Manpower

● Education, Training, & Manpower

Education, Training, & Manpower's goal is to **change the Air Force acquisition culture** from within through hiring, education, and training, thus providing the right people at the right place with the right systems and tool knowledge

MANPOWER

- 855 NEW positions across 5 Acquisition and Testing Centers (FY18-24)
- Multi-disciplinary: Engineers, IT, Computer Scientists, Information Security, Intel, Logistics, Program Management

EDUCATION

- Cyber Education Consortium: CROWS, DAU, AFIT, AF Cyber College, NAVAIR, ACE
- Leveraging existing courses and building from scratch
- Implementing "Learning Paths" to take basic engineer or IT professionals and get them cross-certified (i.e., engineers that know IT and IT personnel that know engineering)



CROWS Education & Training

● CROWS Education & Training

The 2014-2024 Air Force Engineering Enterprise Executive Council (EEEC) identified competency management as its #4 priority

- This task leveraged competency management efforts within AFLCMC/EN to support workforce development.
- Early efforts of the Education and Training Team focused on providing inputs to support AFLCMC/EN's initiative to develop cybersecurity/resiliency competencies to understand what combination of academic background, experience, education and training are necessary to build and sustain a cyber-capable acquisition workforce.
- This effort concluded with the incorporation of the following competencies to the AFLCMC/EN competency database:

Cybersecurity and Resiliency Implementation
Cybersecurity Assessment and Analysis
Anti-Tamper
Cryptography



CROWS Education & Training

● CROWS Education & Training

So what do we do with it all?

CROWS developed, and is growing, its Cyber Resiliency Learning Paths.

Incorporating a building block approach, these paths are targeted at different experience levels and incorporate internal, external and industry standard material to walk personnel through the myriad of material available to broader and deeper Cyber Resiliency Knowledge, Skills, and Abilities.

- Incorporates DoD's "Back-to-Basics" framework
- Incorporates DoD 8570.01 Certification requirements
- Incorporates career field and DAU Certifications
- CROWS AWARE Learning Path Fielded 2021
- CROWS SMART Learning Path to be released FY22

CROWS Education & Training

Path Description

This learning path is for PAQs, PCIPS, and new CROWS employees. The path includes courses in engineering, program protection, cyber resiliency, and acquisition. The objectives of this path are: Obtain Foundational ACQ Engineering and Technical Management (ETM) Certification. Obtain Program Protection Credential upon passing written exam. Establish a well-rounded foundational knowledge base of cyber resiliency, system security engineering, and program protection. Prepare CROWS members for Sec+ boot-camp and certification. NOTE: Professionals actively proceeding through this AWARE Learning Path should be cognizant that some courses are only conducted at certain

Learning Path Steps

Select a step to navigate to content

- 1. Intro to CROWS & SSE
- 2. Foundational ACQ Engineering and Technical Management Certification
- 3. Focus Week
- 4. Air Force Cyber, Engineering, & Technical Data Management



crows@us.af.mil

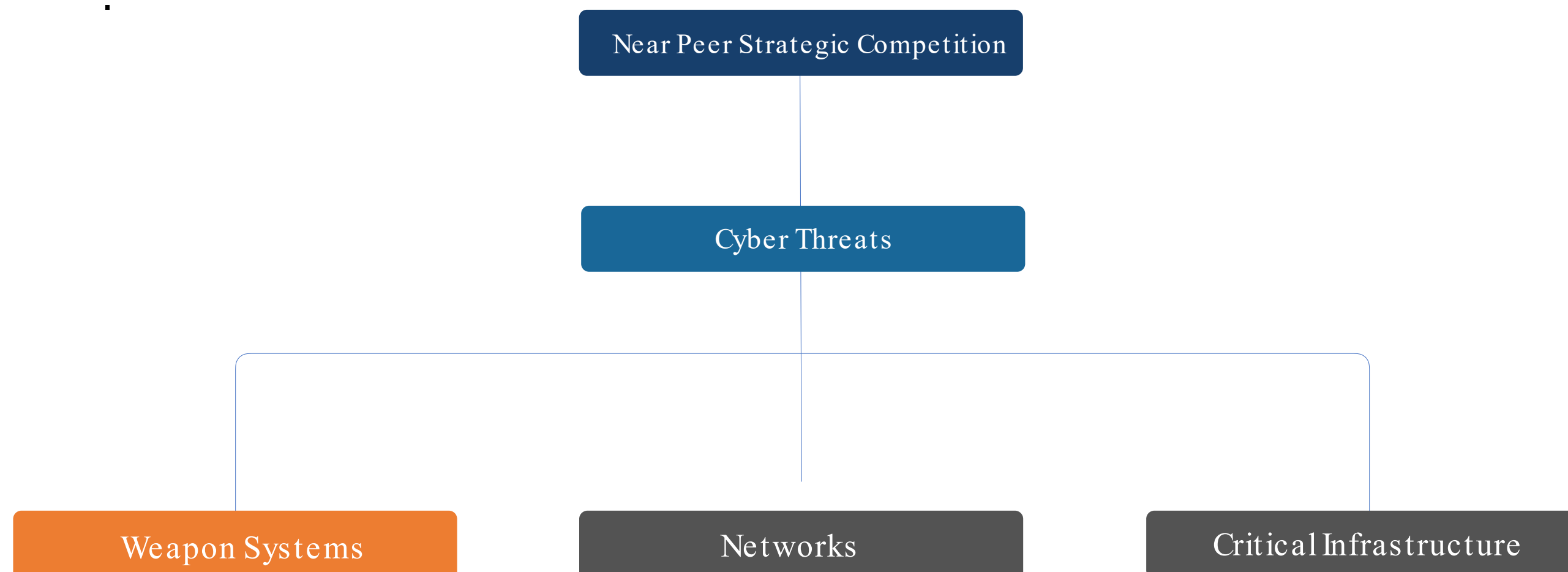
● National Defense Strategy

“The Department **will prioritize investments in cyber defense, resilience,** and the continued integration of cyber capabilities into the full spectrum of military operations.”

The National Security Strategy highlighted the re-emergence of long-term strategic competition as the central challenge to U.S. prosperity and security.

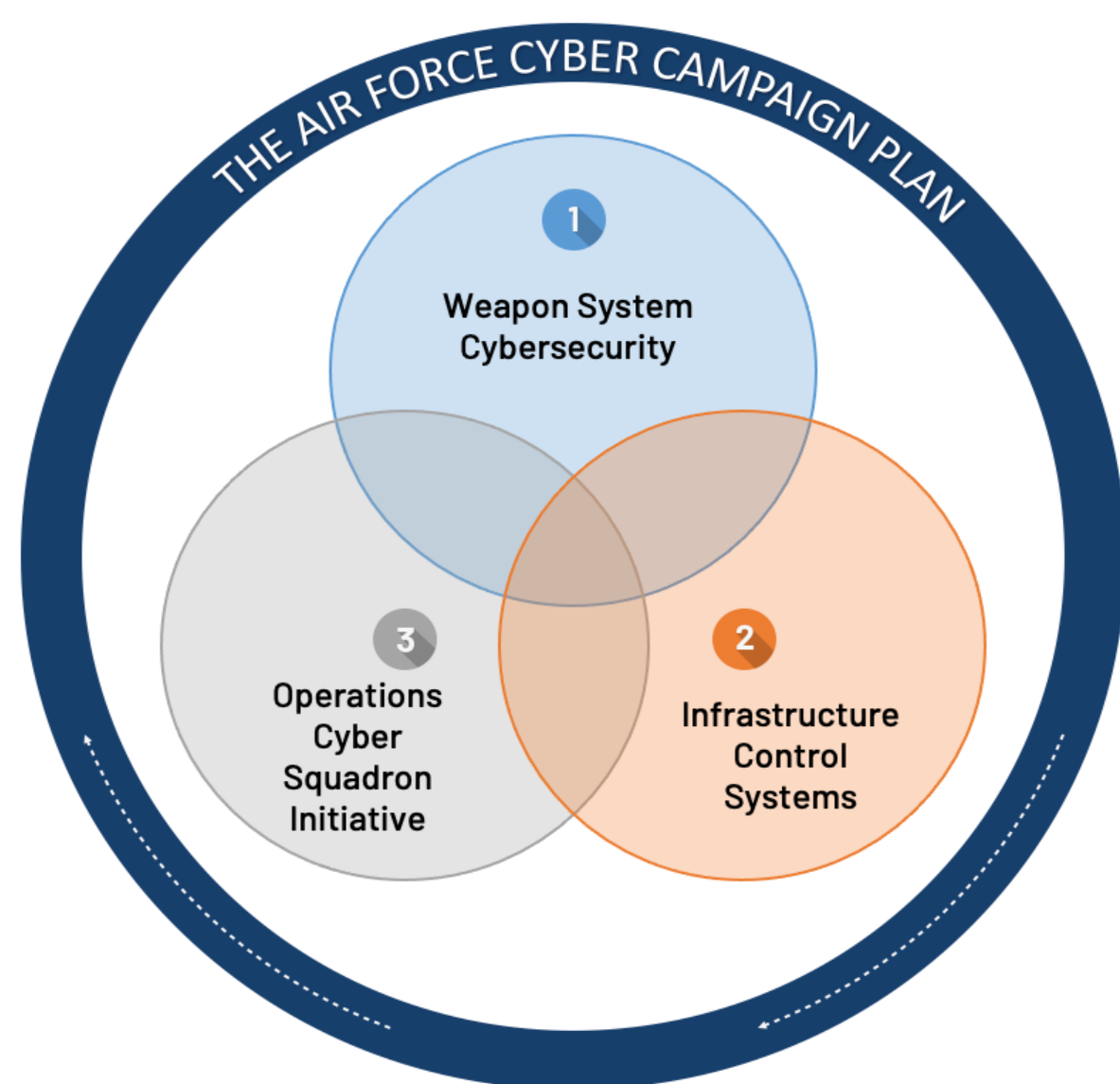
Near peer adversaries continue to seek ways to exploit cyber vulnerabilities to gain strategic and political advantage

The need to protect critical infrastructure, networks, and weapon systems from cyber threats is crucial in order to achieve resiliency in cyber contested environments.



● A Brief History of CROWS

“The task force will diagnose the extent of the cyber threat and the vulnerabilities that currently impact our core missions, will plan to develop a risk management plan that will allow the Air Force to fly, fight and win in a cyber-contested environment, and will recommend investment priorities to the SECAF and CSAF for how best to address the cybersecurity challenges. - **Lt Gen Bill Bender, USAF CIO, 2015**”

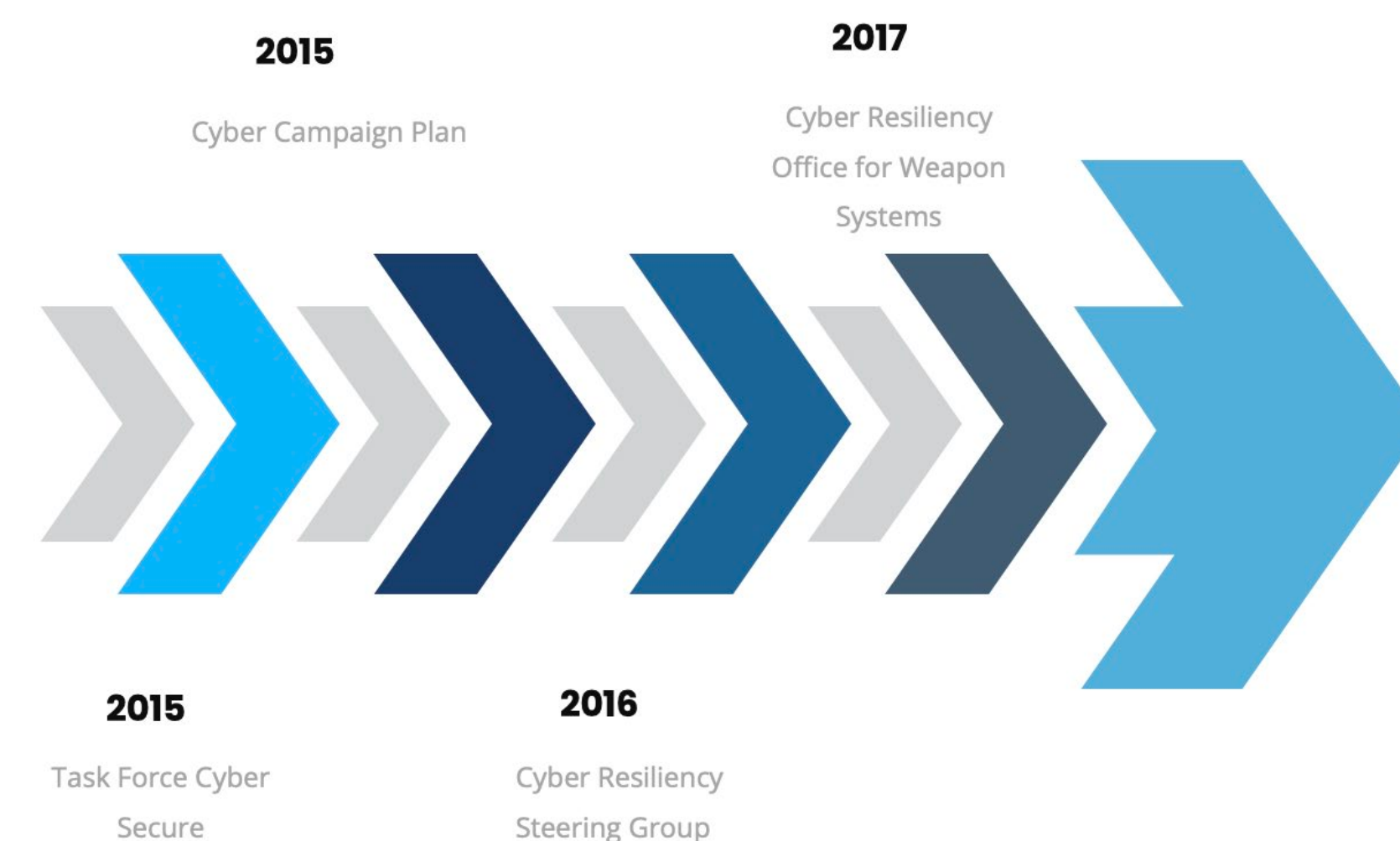


Cyber Campaign Plan

Forged out of 2015's Task Force Cyber Secure, an initiative enacted by then Air Force Chief of Staff Gen. Mark A. Welsh, the Cyber Campaign Plan was developed to synchronize cyber security efforts across the Air Force enterprise to improve the security of information and warfighting systems.

- Acquisition – Weapon System Cyber Resiliency led by the Secretary of the Air Force for Acquisition, Technology, and Logistics (SAF/AQ)
- Infrastructure – Industrial Control Systems and Supervisory Control and Data Acquisition (ICS/SCADA)
- Operations – Communication Squadron Initiative led by the SAF/Chief Information Officer

CROWS TIMELINE



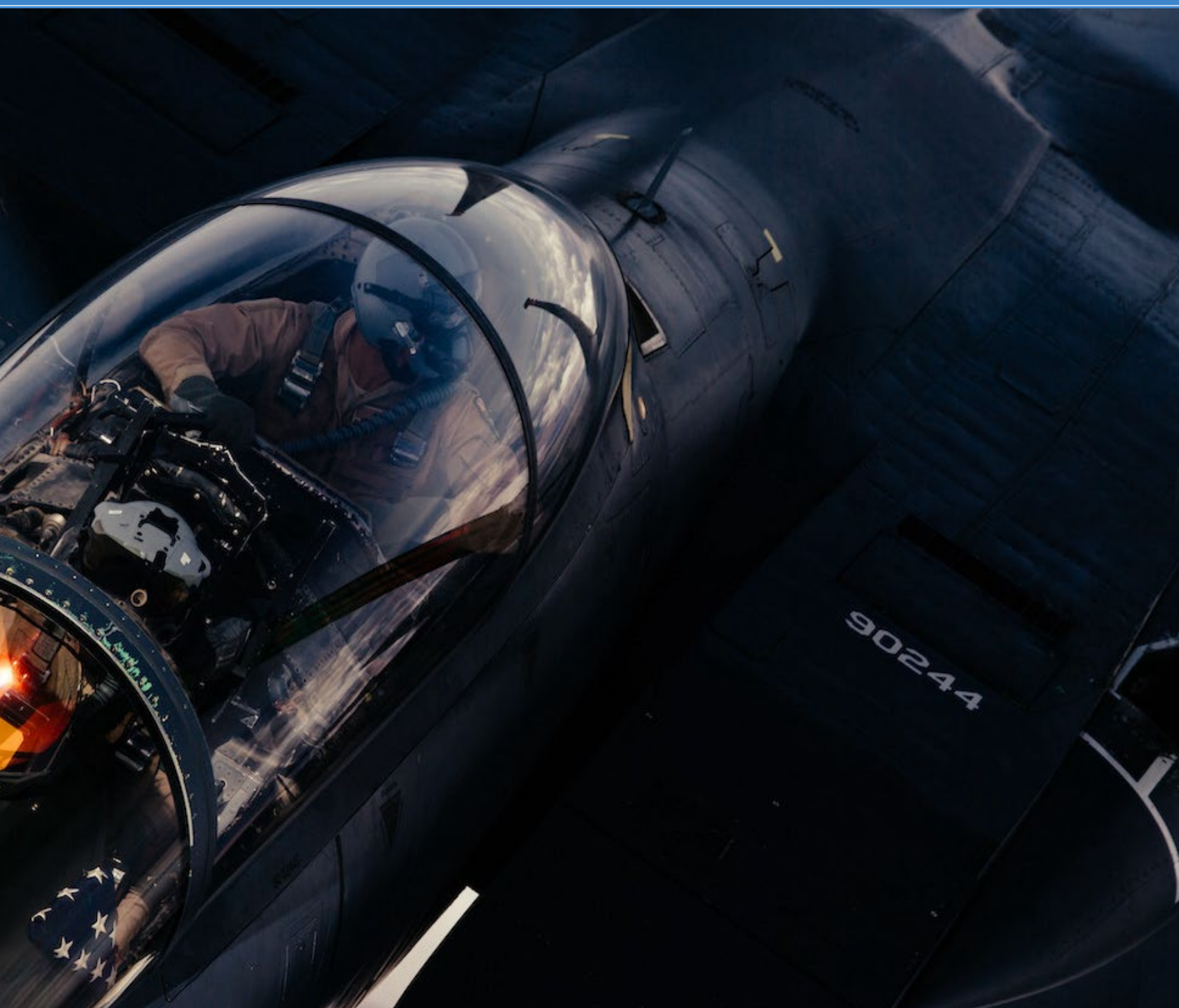
MISSION

INCREASE THE CYBER RESILIENCY OF AIR AND SPACE FORCE WEAPON SYSTEMS TO MAINTAIN MISSION EFFECTIVE CAPABILITY UNDER ADVERSE CONDITIONS



GOALS

BAKE CYBER RESILIENCY INTO NEW WEAPON SYSTEMS AND MITIGATE CRITICAL VULNERABILITIES IN FIELDDED WEAPON SYSTEMS

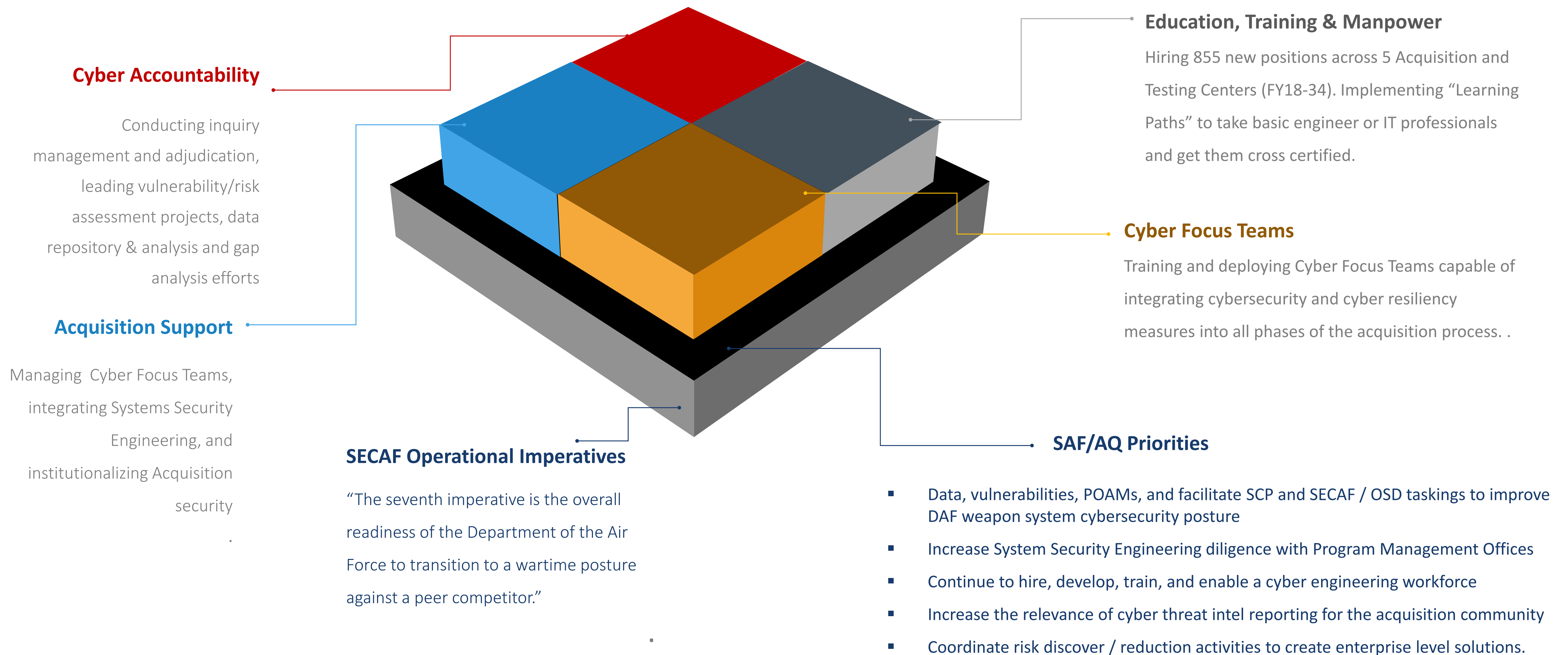


VISION

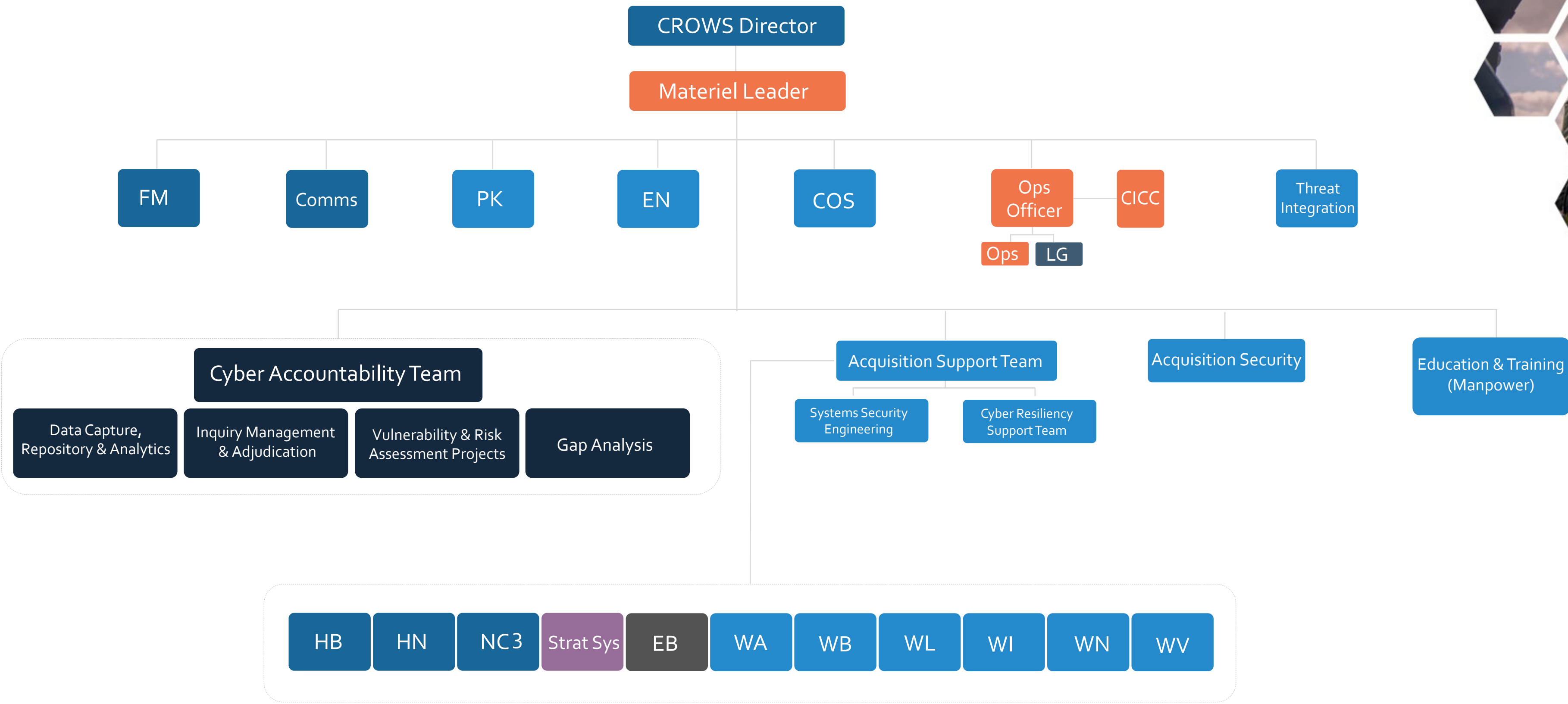
CYBER RESILIENCY EMBEDDED INTO AIR AND SPACE FORCE WEAPON SYSTEMS AND INGRAINED IN DEPARTMENT OF THE AIR FORCE CULTURE



CROWS at a glance



CROWS STRUCTURE



Key

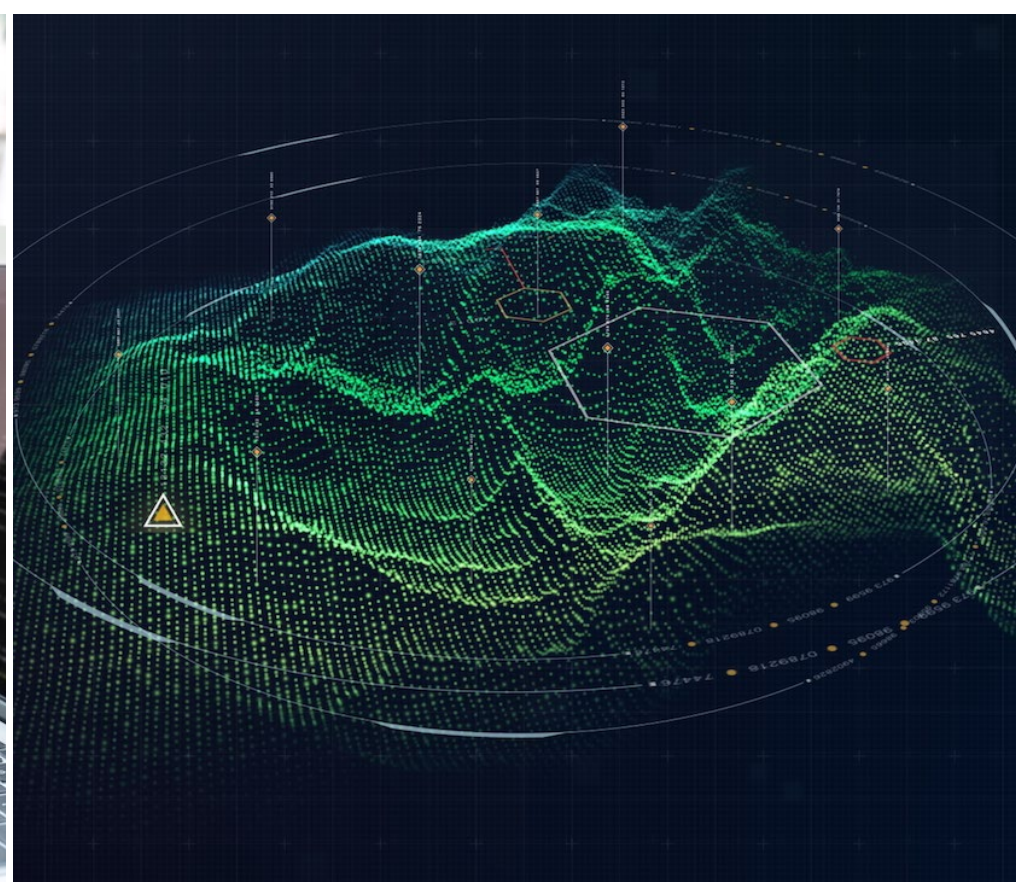
Hanscom Civilian	Wright-Pat Civilian
Hanscom Military	Wright-Pat Military
Hill Civilian	Eglin Civilian

● Acquisition Support Team

How the **Acquisition Support Team** Impacts the CROWS Cyber Resiliency Mission



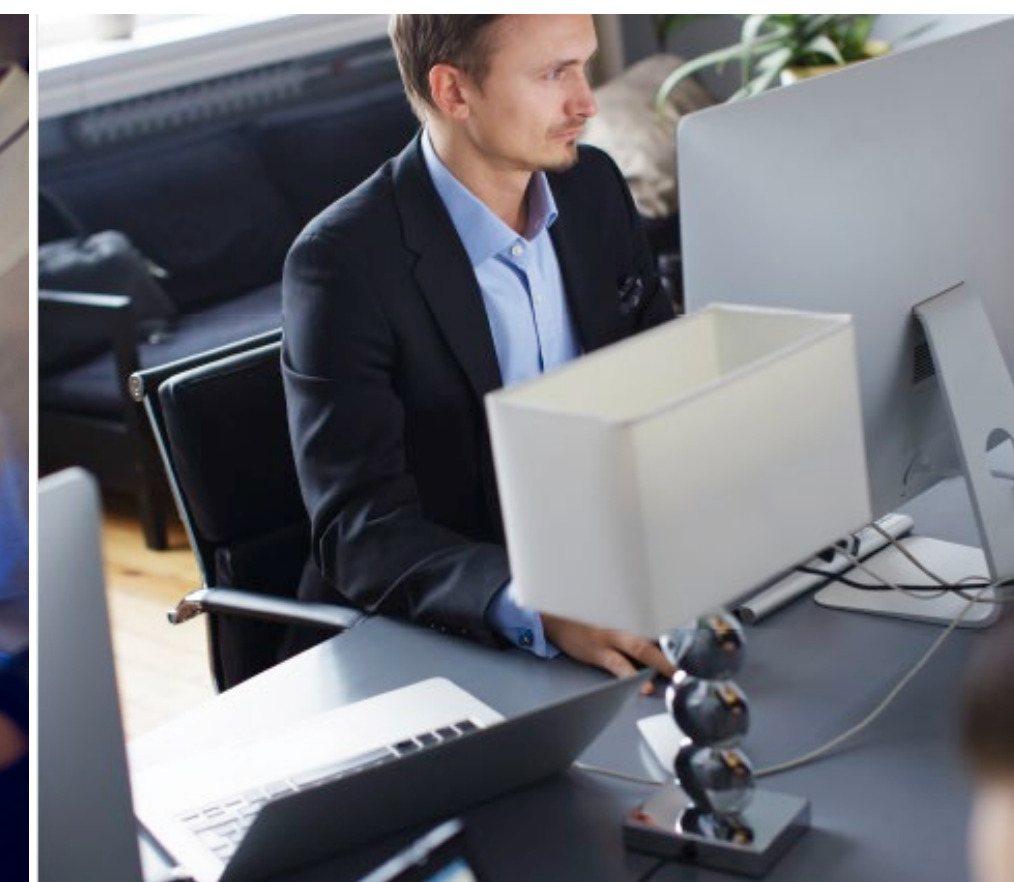
Train and deploy Cyber Focus Teams capable of integrating cybersecurity and cyber resiliency measures into all phases of the acquisition process



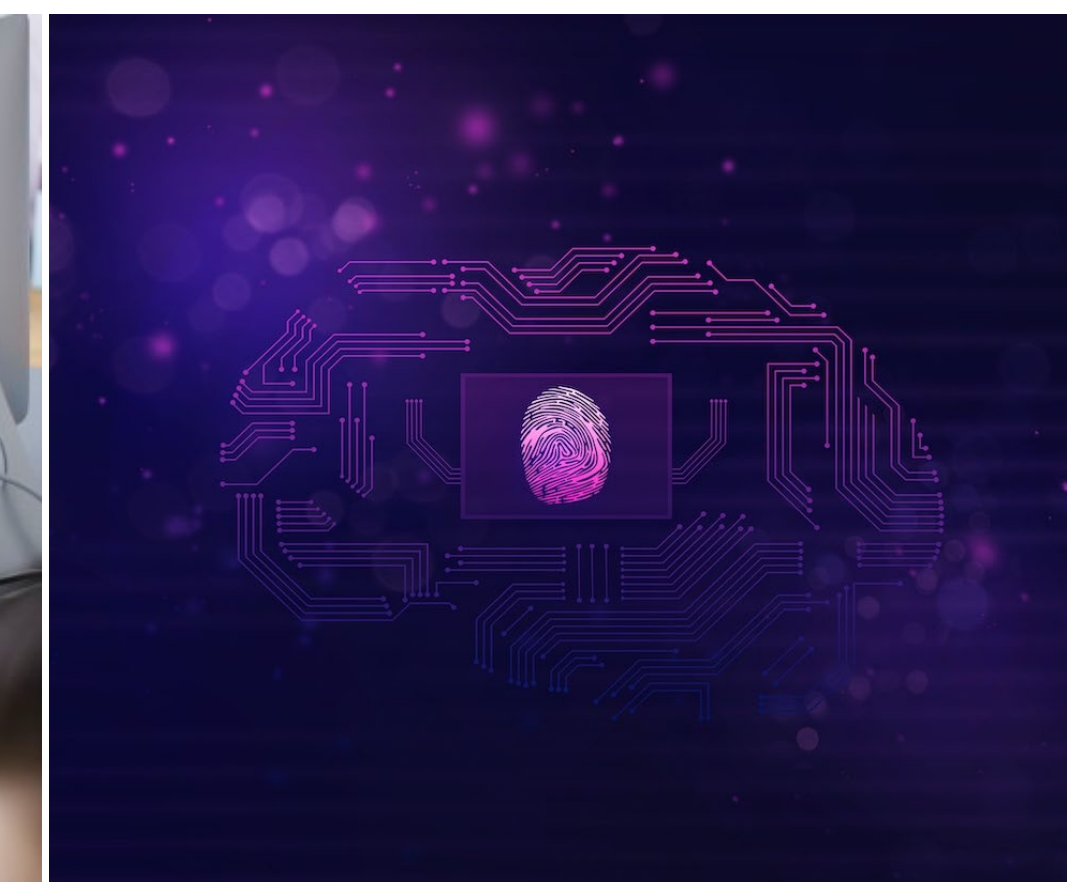
Integrate Systems Security Engineering into Systems Engineering



Provide advice and consultation to the weapon system cyber workforce in applying emerging cyber resiliency requirements, tools, techniques, and guidance

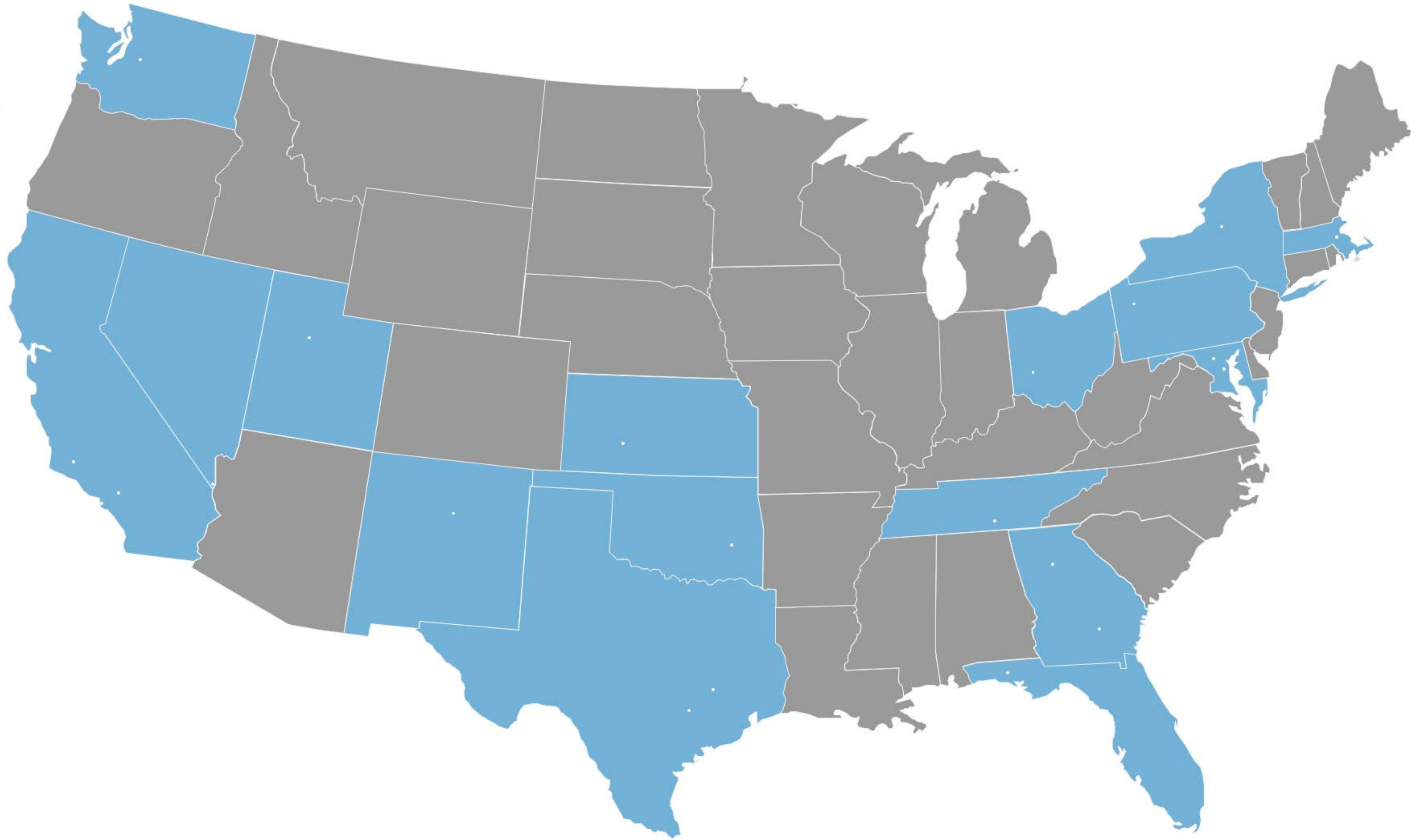


Integrate best practices and lessons learned across the acquisition enterprise



Institutionalize Acquisition Security and establish a common security operating environment to ensure Cyber Resiliency in Department of the Air Force Weapon Systems

CROWS FOOTPRINT



• Education, Training, & Manpower

Education, Training, & Manpower's goal is to **change the Air Force acquisition culture** from within through hiring, education, and training, thus providing the right people at the right place with the right systems and tool knowledge

MANPOWER

- 855 NEW positions across 5 Acquisition and Testing Centers (FY18-34)
- Multi-disciplinary : Engineers, IT, Computer Scientists, Information Security, Intel, Logistics, Program Management

EDUCATION

- Cyber Education Consortium: CROWS, DAU, AFIT, AF Cyber College, NAVAIR
- Leveraging existing courses and building from scratch
- Implementing "Learning Paths" to take basic engineer or IT professionals and get them cross-certified (i.e., engineers that know IT and IT personnel that know engineering)



• Education, Training, & Manpower

SAF/AQR PRIORITY 2: Ensure Program Protection & System Security Engineering are an integral aspect of program management & systems engineering requirements through and increased SSE diligence with program offices and is measured and monitored thru Program Protection Plans, Independent Technical Risk Assessments, contract actions, and Cyber Focus Teams oversight

SAF/AQR PRIORITY 3: Hire, develop, train and enable all 855 Cyber Campaign Plan billets thru FY34

SAF/AQR PRIORITY 4: Strengthen CROWS' Intelligence integration activities in order to prioritize its in-house threat intelligence integration efforts whose throughput will help program offices prioritize their mitigation activities

Key Stakeholders

- Acq Community, Program Offices, Cyber Focus Teams
- SAF/AQR, AFLCMC, AFNWC, AFOTEC, AFTC, SSC
- CROWS, DAU, AFIT, AF Cyb College, NAVAIR



• CROWS Education & Training

- The 2014-2024 Air Force Engineering Enterprise Executive Council (EEEEC) identified competency management as its #4 priority
 - This task leveraged competency management efforts within AFLCMC/EN to support workforce development
 - Early efforts of the Education and Training Team focused on providing inputs to support AFLCMC/EN's initiative to develop cybersecurity/resiliency competencies to understand what combination of academic background, experience, education and training are necessary to build and sustain a cyber-capable acquisition workforce
 - This effort concluded with the incorporation of the following competencies to the AFLCMC/EN competency database:

Cybersecurity and Resiliency Implementation
Cybersecurity Assessment and Analysis
Anti-Tamper
Cryptography



• CROWS Education & Training

Through education and training of the acquisition workforce, the CROWS hopes to ingrain cyber resiliency concepts into weapon systems and the Air Force culture

The initial Education and Training efforts was to find the *best of breed, existing, relevant courseware*

- Re-use rather than build
- Modify existing when possible
- Initial sources: NAVAIR, DAU, AFIT
- Lastly, develop new cyber security and cyber resiliency courses to meet acquisition workforce training requirements

2018 CROWS established Cyber Resiliency Education Consortium

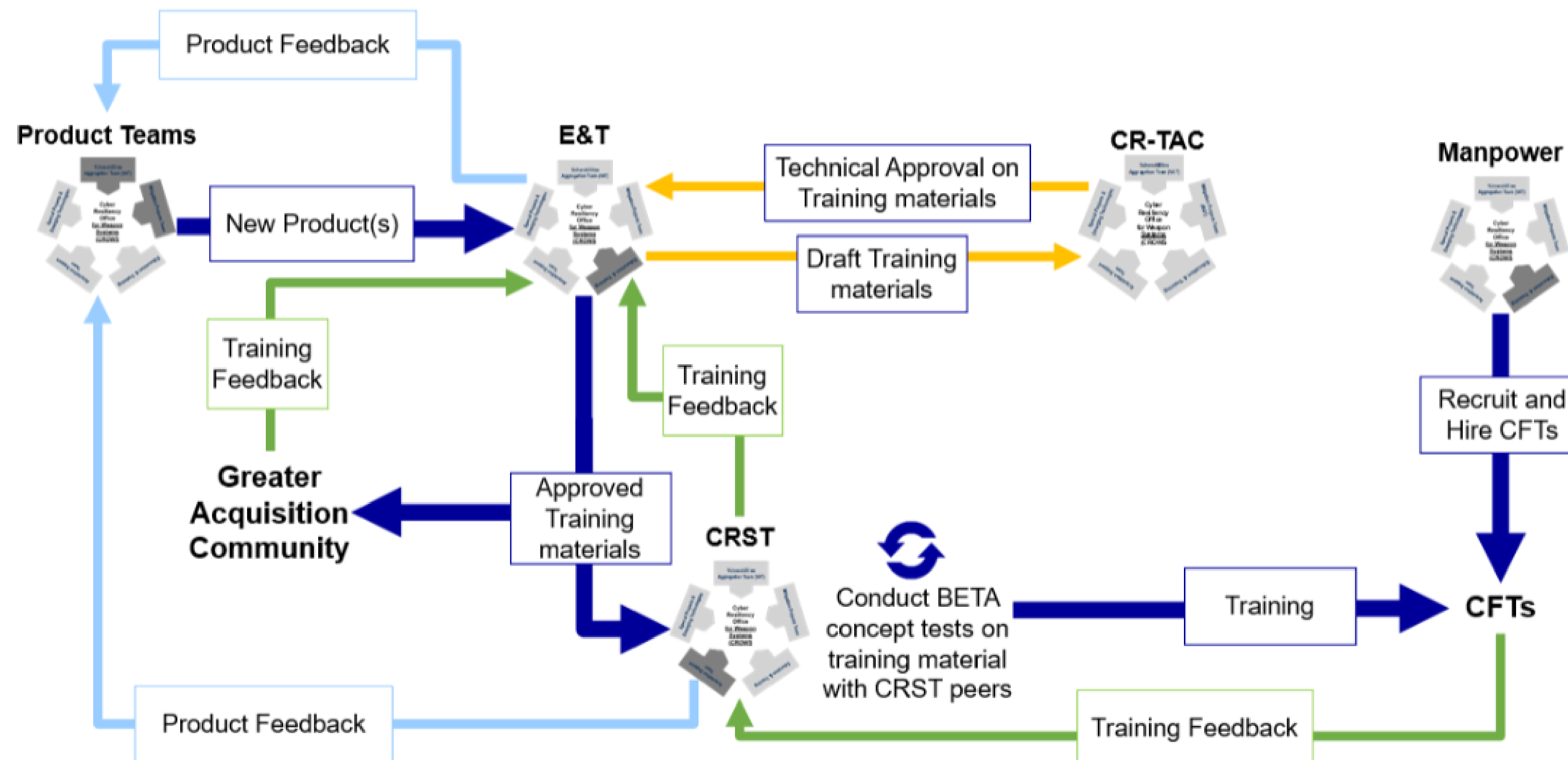
- Supports identification/coordination of cyber course material, build and improve an AF level, weapon system specific, acquisition focused cyber course curriculum
- Sustained effort to review, evaluate and endorse existing cyber training for relevance and identify gaps for development or further investigation

- **CROWS Education and Training** - Consortium Chair; leads projects; manages whole of workforce efforts
- **AFIT AF Cyberspace Technical Center of Excellence** - Rapid Development Team (RDT), Instructional design, SME support
- **DAU** - coordination & standardization (SSE Cyber Guidebook usage)
- **Air University Cyber College** - provides Mission Defense Team (MDT) training; coordination & standardization (Functional Mission Analysis-Cyber (FMAC) course, seminars, ACI)
- **NAVAIR** - cross-service educational collaboration

• CROWS Education & Training

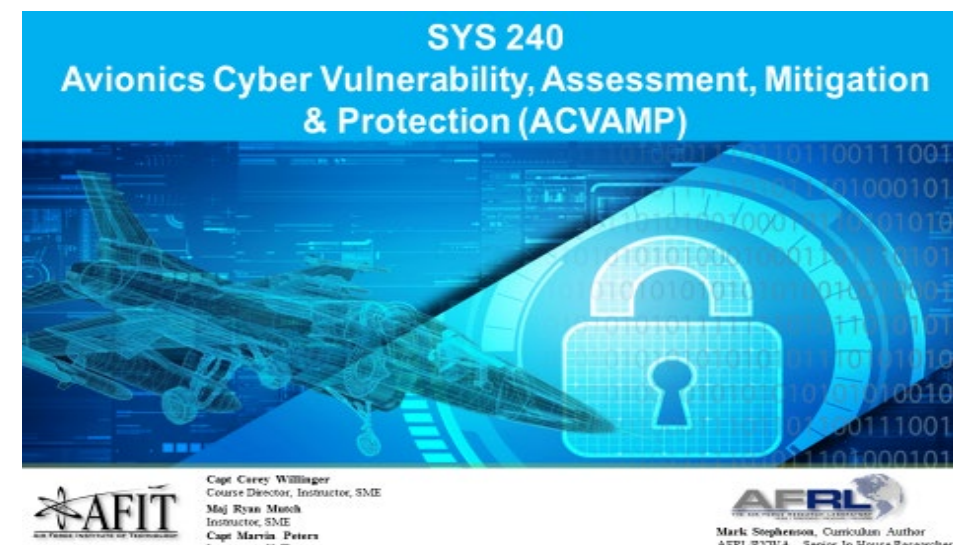
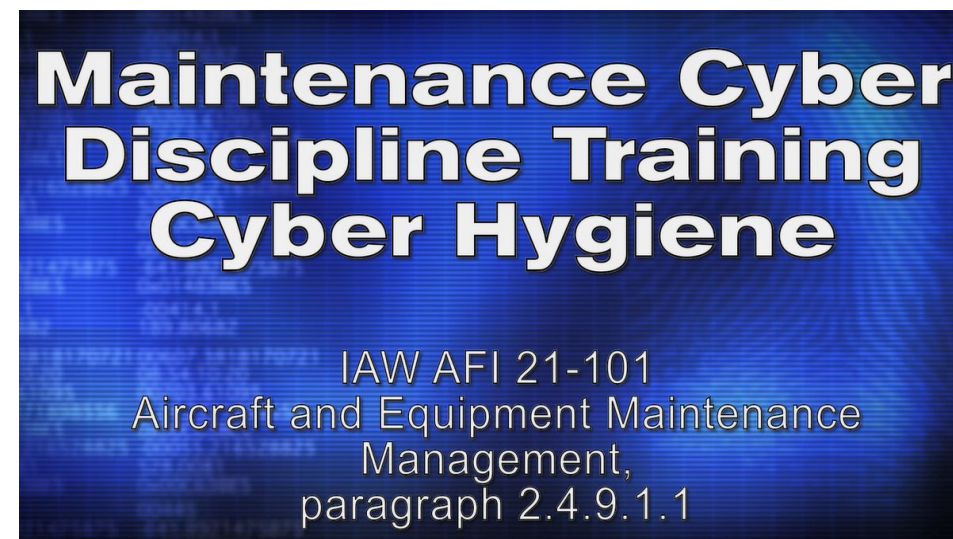
The Team considers external training products (AFIT, DAU, Federal, DoD, vendor, etc.) when the course content aligns with the CROWS competency goals

1. Internal training (limited) – CROWS specific training; organizational in nature
2. Acquisition Workforce training (wide-availability) – designed for delivery to the greater Acquisition Workforce



• CROWS Education & Training

Fielded Classes, Training or Workshops



- **Maintenance Cyber Discipline Training (myLearning)**
 - Fielded and mandated by AF/A4 for ~130k Active Duty, Guard and Reserve maintenance personnel (IAW 21-101)
- **Avionics Cyber Vulnerability, Assessment, Mitigation & Protection (ACVAMP) (AFIT)**
 - Over 2,000 students trained across multiple acquisition bases; cybersecurity related to aircraft avionic systems beyond traditional IT. A five step vulnerability assessment and mitigation process, teaching how to discover, analyze, and consider mitigation of vulnerabilities in an avionic systems
- **CROWS Lexicon Video**
 - Developed in conjunction with CROWS Engineering and DAU; SSE Cyber Guidebook definitions of Cybersecurity, Cyber Resiliency, and Cyber Survivability and how they intertwine; for new CROWS, 35K acquisition professionals, and MDTs
- **Introduction of Cyber Resiliency for Acquisition Video**
 - For all career fields, 3 modules; game based learning 100-level cyber security/cyber resiliency video for new CROWS and optional for acquisition professionals and MDTs
- **OPREP 3B R6C Training**
 - Weapon system Cyber Incident Coordination process; all current and future Mission Defense Team (MDT) members; used by AF Cyber College during their Functional Mission Analysis – Cyber (FMAC) course; all CROWS CFTs

• CROWS Education & Training



Fielded Classes, Training or Workshops

■ **SYS 253 Early Test and Evaluation Influence in Acquisition Course**

- Addition of Cyber Resiliency module; preps Air Force personnel engaged in T&E execution or management to be effective members of the acquisition team with emphasis on early influence in an acquisition program

■ **Fortiphyd Simulation Training**

- A virtual environment based on a notional UAS/ground station; learn how to exploit common vulnerabilities and mitigate common vulnerabilities; initially all new CFTs, eventually open to all acquisition professionals and MDTs; 40 attendees per year

■ **SSE Cyber Guidebook Overview Course**

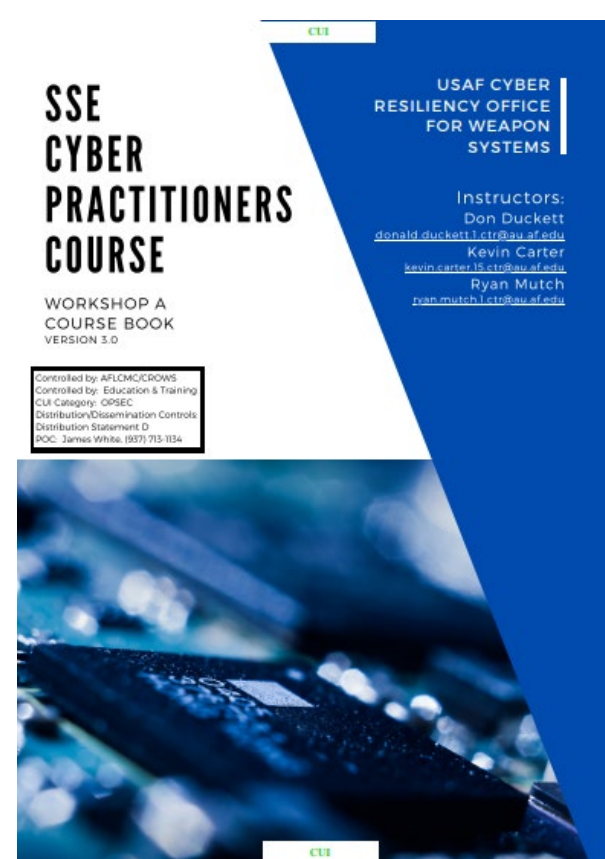
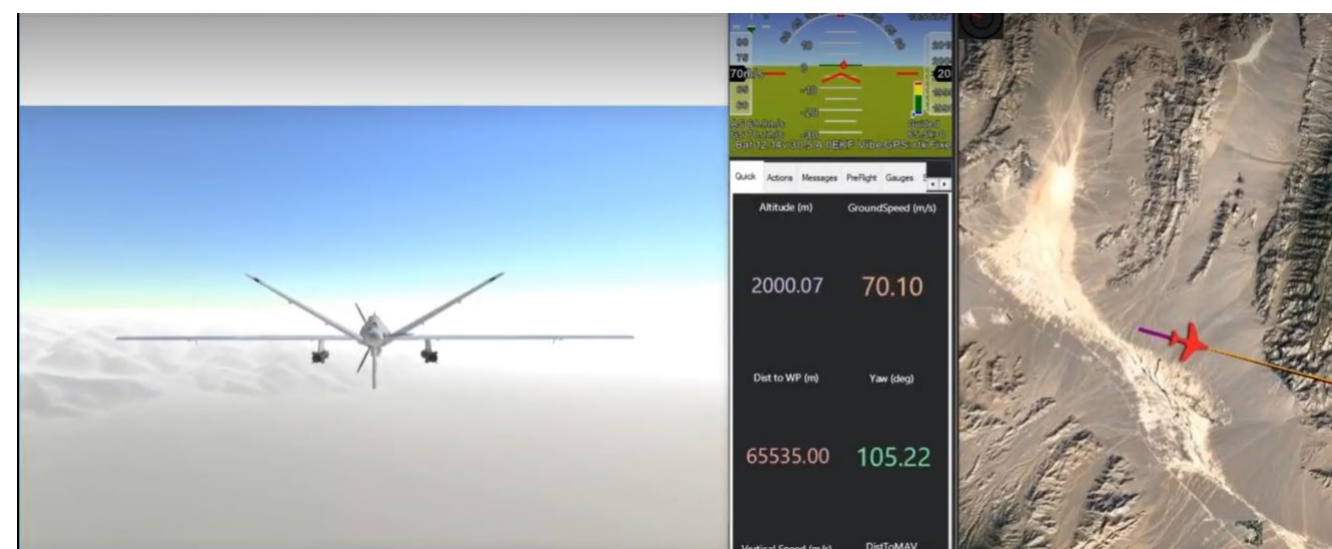
- Cornerstone of “baking-in” cyber resiliency; designed to explain the “Why” behind the SSE Processes, mandatory for all CROWS Cyber Focus Team (CFT) members; 1,000+ students

■ **USAF SSE Cyber Practitioner’s Course (300-level)**

- Course composed of two-workshops with hands-on exercises/scenarios to learn how to apply the SSE Cyber Guidebook work breakdown structure; audience CROWS CFTs and 35K acquisition professionals

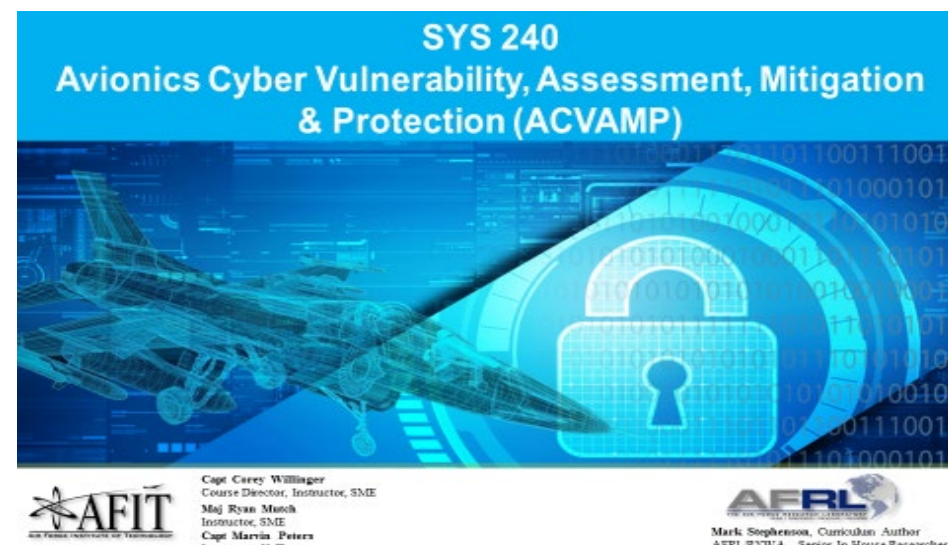
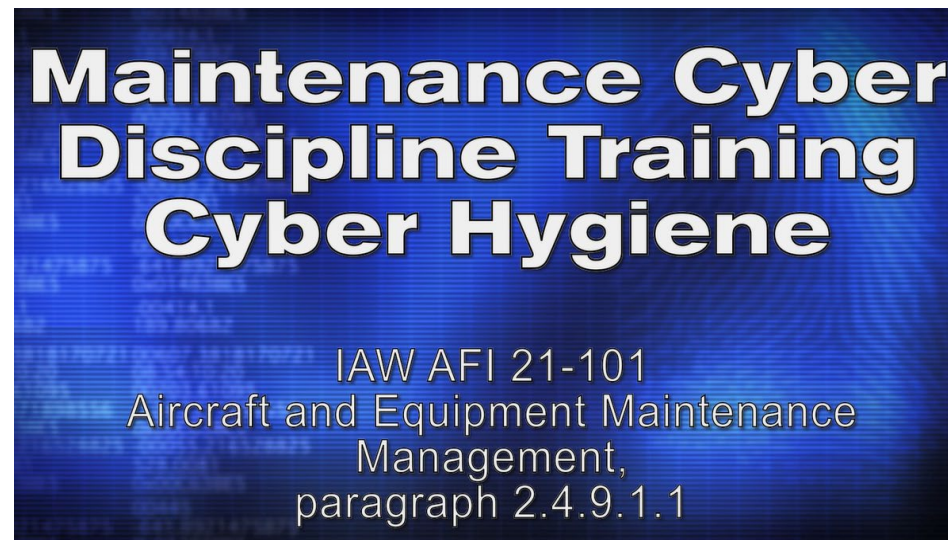
■ **CROWS Orientation**

- Designed for new CFTs and CROWS members; consists of two-days of Team presentations and SSE Cyber Guidebook Overview; also open to program office personnel



• CROWS Education & Training

Classes, Training or Workshops in Development



- **SSE Cyber Video Series**
 - Multiple 10-minute videos on particular SSE Cyber Guidebook topics for Just-in-Time training
- **Smart Level Learning Path**
 - This is the Aware Learning Path follow-on; currently in development
- **Digital Engineering in the SSE Cyber Process**
 - An introductory course to look at how Digital Engineering, MBSE, DEVSECOPS, and Agile Software Development impacts the SSE Cyber processes
- **Acquisition Intel Training**
 - In data collection phase, in conjunction w/ DAU efforts
- **CROWS Acquisition Information Protection Security Training**
 - Initial and recurring training designed for cyber acquisition professionals
- **Cyber Analysis, Cyber Risk, etc. Tools**
 - Consolidated list of available tools and their uses, standardized information sheets and mapping to SSE Cyber Guide Book work breakdown structure

● CROWS Education & Training

Education & Training Support to Other Efforts

- Assisting development of **AFLCMC Information Protection community's Program Protection Practitioner's course** based on the SSE Cyber Guidebook Practitioner's Course methodology
- Review of **Air Force Research Lab Cyber Security Analysis Tool** computer-based training (12)
- Including elements of the SSE Cyber Guidebook into **DAU Secure Cyber Resiliency Engineering material; Cyber Resiliency Certifications**
- Providing CICC and Threat integration **briefs to AFIT's CYB 300 Joint Advanced Cyberspace Operations**
- Review of concepts, material, and **sharing of our efforts with Aviation Cyber Initiative**
- **Support to AFLCMC Focus Week by providing CROWS 101 & SSE Cyber Guidebook Overview to program office personnel**

Funded (or Partially) through CROWS

- **BANSHEE Innovation Training Program** a partnership between Hanscom Air Force Base, MassChallenge and the Air Force Research Lab designed to help participants incorporate innovative ideas
- **Advanced Course in Engineering Cyber Security Boot Camp (ACE)**, a graduate level curriculum covers leadership during crisis situations, the science of mission assurance, the art of cyber warfare, and written/verbal communication skills; 10-week cyber internship; 50 students per class
- **57th Information Aggressor Squadron instructor course** curriculum development

• CROWS Education & Training

So what do we do with it all?

CROWS developed, and is growing, its Cyber Resiliency Learning Paths.

Incorporating a building block approach, these paths are targeted at different experience levels and incorporate internal, external and industry standard material to walk personnel through the myriad of material available to broader and deeper Cyber Resiliency Knowledge, Skills, and Abilities.

- Incorporates DoD's "Back-to-Basics" framework
- Incorporates DoD 8570.01 Certification requirements
- Incorporates career field and DAU Certifications
- CROWS AWARE Learning Path Fielded 2021
- CROWS SMART Learning Path to be released FY22

● CROWS Education & Training



Search...

ADD CONTENT



Path Description

This learning path is for PAQs, PCIPS, and new CROWS employees. The path includes courses in engineering, program protection, cyber resiliency, and acquisition. The objectives of this path are: Obtain Foundational ACQ Engineering and Technical Management (ETM) Certification. Obtain Program Protection Credential upon passing written exam. Establish a well-rounded foundational knowledge base of cyber resiliency, system security engineering, and program protection. Prepare CROWS members for Sec+ boot-camp and certification. NOTE: Professionals actively proceeding through this AWARE Learning Path should be cognizant that some courses are only conducted at certain

Learning Path Steps

Select a step to navigate to content



1. Intro to CROWS & SSE

SHOW DETAILS



2. Foundational ACQ Engineering and Technical Management Certification

SHOW DETAILS



3. Focus Week

SHOW DETAILS



4. Air Force Cyber, Engineering, & Technical Data Management

SHOW DETAILS

AWARE Learning Path

Upon Completion of the AWARE Learning Path professionals will:

1. Obtain Engineering and Technical Management Foundational Certification
2. Obtain Program Protection Credential upon passing a written exam
3. Obtain Cybersecurity Engineering Resiliency (CSER) Credential Lvl 1 (In Dev)
4. Prepared for a Sec+ boot camp & certification

Unclassified

20

• CROWS Education & Training

1. Intro to CROWS

- Intro to Resiliency for Acquisition 100
- DAU ACQ 101
- CROWS Orientation
- SSE Cyber Guidebook Workshop

2. Foundational ACQ Engineering & Tech Management Certification

- ETM 1010 Leading Change
- ETM 1020 Mission & Systems Thinking
- ETM 1030 Requirements Definition & Analysis
- ETM 1040 Tech Management
- ETM 1050 Design Consideration
- ETM 1060 Product Realization
- ETM 1070 Digital Literacy
- ETM 1080 Software Literacy
- ETM 1090 Tech Perspectives on Defense Contracting

3. FOCUS Week

- AFIT Workshop 0665 Current Topics in Cyber for AF Weapons Systems
- EZA 110 Intro to Weapons System Cybersecurity and Resiliency

4. AF Cyber, Engineering, & Tech Data Management

- PPR 150 Intro to TSN
- SYS 182 Intro to SE
- CLE 003 Tech Reviews
- CLE 022 PM Intro to Anti-Tamper
- CLE 068 Intellectual Property/Data Rights
- CLE 074 Cybersecurity Throughout DoD Acq
- CLE 080 SCRM for Info & Comm Tech
- CLE 081 Software Assurance Awareness
- PMT 0170 Risk Management
- ENG 101 Fundamentals of Systems Engineering

5. Program Protection Credential

- ACQ 160 Program protection Planning Awareness
- ENG 260 Program Protection for Practitioners

6. Management of Systems Engineering & Cyber Risk Assessment for Weapon Systems

- SYS 240 Avionics Cyber Vulnerability Assessment, Mitigation and Protection (ACVAMP)
- SYS 282 Management of the Systems Engineering Process
- SYS 341 Cyber Risk Assessment for Weapons Systems (PIT)
- BANSHEE Innovation Training Program
- Fortyphid Simulation Training
- CompTIA Security+ Boot Camp & Certification

• CROWS Education & Training

AVOLVE Search...

Learning Paths
Guided Educational Resources

GETTING STARTED **BROWSE PATHS**

Learning Path Content

5 steps 5 hours	9 steps	11 steps 2 hours 15 minutes	6 steps 6-12 Months
Avolve Users Guide	Introduction to Risk Management	Configuration Management for Beginners	CROWS Aware Learning Path
Mark McDonald 2 years ago	Kara Allison 2 years ago	Steven Glazewski 2 months ago	CROWS Ed&T a year ago
Last Updated 2 years ago	Last Updated a year ago	Last Updated 2 months ago	Last Updated 4 months ago

SMART Learning Path (Draft)

Upon Completion of the SMART Learning Path professionals will:

1. Obtain Engineering and Technical Management Practitioner Certification
2. Obtain Cybersecurity for Program Managers Credential
3. Complete CROWS SSE Practitioners course
4. Obtain Cybersecurity Engineering Resiliency (CSER) Credential Lvl 2 (In Dev)
5. Additional courses/credentials still under review for CFT relevancy

• CROWS Education & Training

Education & Training SSE Training Roadmap Only

- **SSE Cyber Guidebook Overview Course** (2 Hours) AFIT taught during CROWS Orientation or AFLCMC FOCUS Week
- **SSE Cyber Guidebook Workshop** (2 Hours) AFIT taught two weeks after CROWS Orientation
- **SSE Cyber Guidebook In-depth Course** (2 Hours) taught during AFLCMC quarterly PPP Course
- **CPI/CC Course** (1 hour) taught by AFIT during AFLCMC quarterly PPP course
- **Digital Engineering in the SSE Cyber Process** – Short topical videos
- **SSE Cyber Video Series (FY23)** will consist of multiple 10-minute videos on particular SSE Cyber Guidebook topics for Just-in-Time training
- **SSE Cyber Practitioners Course (4 Days)** consisting of two-workshops

YIN & YANG

A FULL LIFE CYCLE SUPPORT ACTIVITY

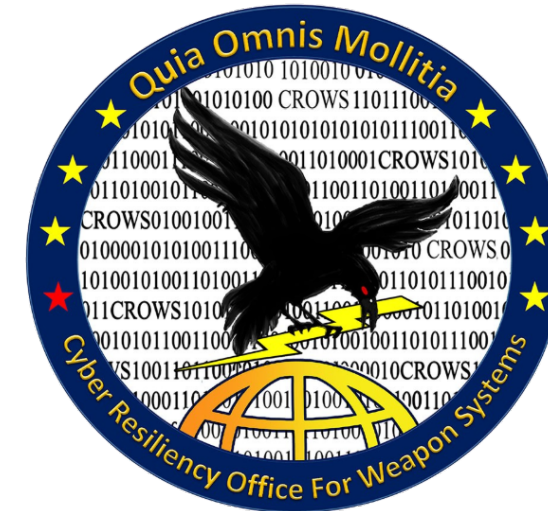


The CROWS mission consists of two primary facets which can be viewed as the Yin and Yang of weapon system cybersecurity. Both represent a series of activities that are each complimentary, interconnected, and/or interdependent of one another; and represent our holistic outlook on attacking the challenge of advancing the cyber resiliency of weapon systems.

Collectively, the Ying and the Yang represent a full life cycle of engagement, oversight, and enforcement activities designed to meet the Department of the Air Force’s cyber demand signal.



CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS



crows@us.af.mil