CROWS

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

PROTECT • DETECT • RESPOND • RECOVER

WHAT

CROWS is an Air Force level, interdisciplinary organization established under the Assistant Secretary of the Air Force (Acquisition, Technology & Logistics) to ensure Air Force weapon systems can perform their missions in a cyber-contested environment.

HOW

We partner with acquisition, operational and test communities to assess the fielded fleet and with Program Executive Offices to prototype mitigation solutions. We also deliver tools, cyber-focused intelligence, a common security environment, education, training, and a cyber-savvy workforce to program offices—providing them the capability to do for their systems what CROWS does for the Acquisition Enterprise.

WHEN

We operate at every stage of the acquisition life cycle — from development planning through sustainment.

MISSION

Increase cyber resiliency of Air Force weapon systems to maintain mission effective capability under adverse conditions.

GOALS

Bake cyber resiliency into new weapon systems. Mitigate critical vulnerabilities in fielded weapon systems.

VISION

Cyber resiliency embedded into Air Force weapon systems and ingrained in Air Force culture.

CUSTOMERS AND MISSION PARTNERS

CROWS SUCCESS STORIES

Assessments

Completed Cyber Mission Thread Analysis (CMTA) on Aerial Refueling, Global Positioning System, Nuclear Strike, and Suppression of Enemy Air Defense missions.

Completed Cyber Vulnerability Assessments on 27 of 48 major weapon systems under NDAA 1647.

Mitigations

Developed virtual systems integration lab and prototyped Resilient Embedded GPS/INS (R-EGI) to provide open systems government reference architecture for Position, Navigation, and Timing (PNT) — transitioning to new program in PNT PMO under PEO Agile Combat Support.

Partnering with programs for prototyping efforts:

- C-17: MILSTD-1553B firewall miniaturization
- Jt Mission Planning System: software integrity
- PEO Fighter/Bomber: OFP digital signatures
- AF Research Lab: software attestation

Intel

Provided cyber-focused intelligence support to the acquisition community.

Published CYBERFLASH, the AF Journal of Cyber Resiliency, for Acquisition Senior Leaders.

Matured the Cybersecurity & Intelligence Working Group to share information across AF, DoD, Missile Defense Agency, and intel communities.

Operations

Activated Cyber Incident Coordination Cell with CONOPS signed by AFLCMC/CC and 24 AF/CC.

Led Cyber Incident Response Teams (CIRT) in world-wide cyber events on AF weapon systems.

Acquisition Support

Released major update to AF Systems Security Engineering (SSE) Acquisition Guidebook.

Stood up initial Cyber Resiliency Support Team (CRST) and provided system analysis and acquisition document support to programs across four PEOs.

Advanced Common Security Environment:

- Published enterprise-wide Weapon System Cyber Security Classification Guide (SCG).
- Initiated 13 facility projects across seven bases to provide AFLCMC, AFNWC, SMC, and AFSC programs secure environment for cyber analysis.

Education & Training

Launched Cyber Hygiene for Maintainers course — adopted by HAF/A4 as mandatory for 147,000 maintenance Airmen in the Total Force.

Fielded Intro to Cyber for Acquisition course and delivered to 300+ professionals across six bases.

Developed AFIT Avionics Cyber Vulnerability, Assessment, Mitigation & Protection course (ACVAMP, SYS 240) and updated SYS 253 with Test & Evaluation Concepts & Policy for Cyber —educated 1500+ students.

CONTACT US AT CROWS@US.AF.MIL

PROTECT • DETECT • RESPOND • RECOVER