Cyber Resiliency Office for Weapon Systems (CROWS)

Integrity - Service - Excellence

Air Force Cyber Campaign Plan

Mr. Joseph F. Bradley, SES
Director

Lt Col Bai Zhu, USAF
Materiel Leader

Mr. Daniel C. Holtzman, HQE
Technical Director

October 2019

CROWS@us.af.mil

Cyber Resiliency – A War Winning Capability

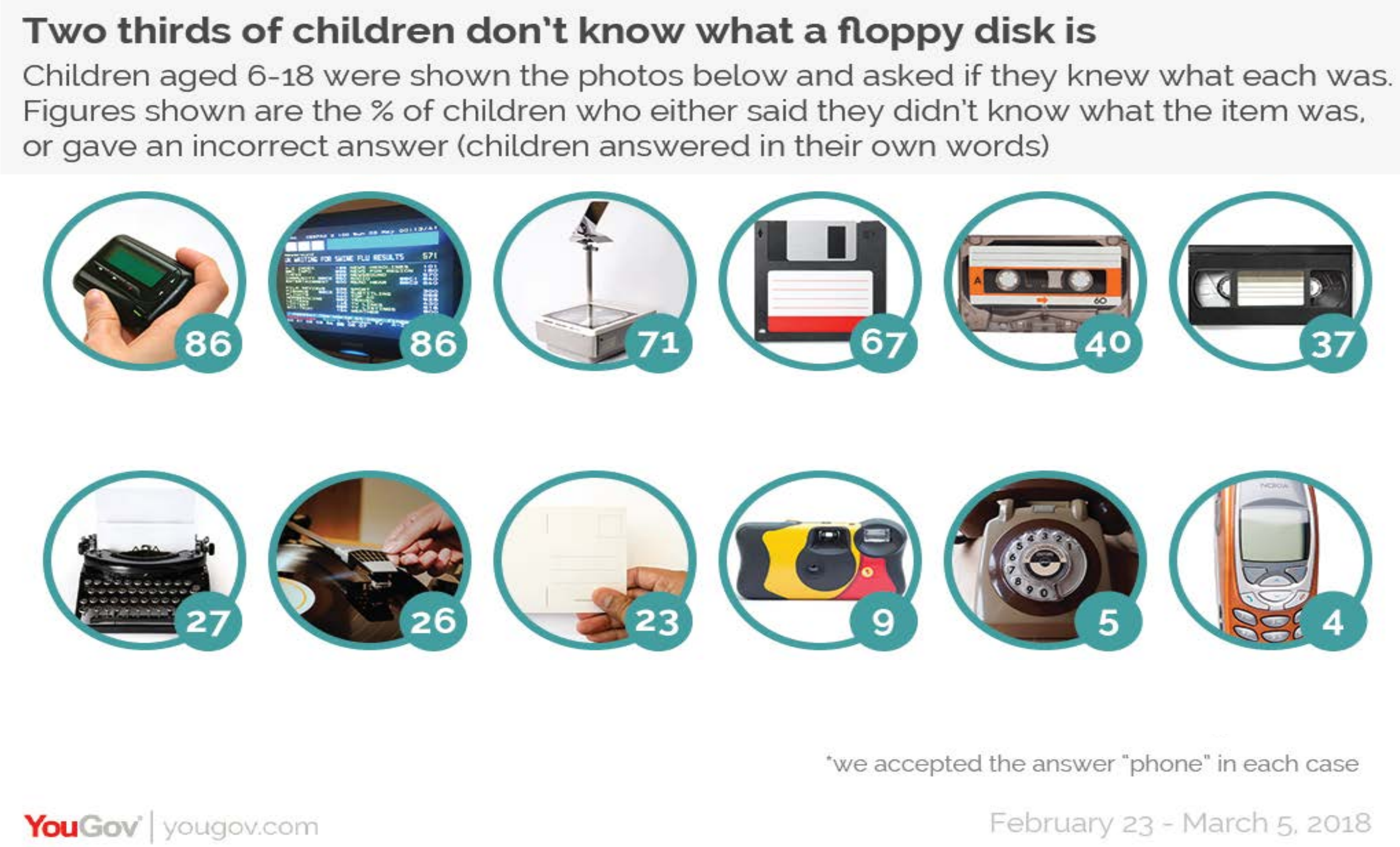
Approved for Public Release; Distribution Unlimited. Case 2019-0702

Overview

- AF Cyber Campaign Plan & CROWS
- CROWS Structure and Priorities
- Major Efforts and Activities
- Summary

Cyber Culture Conundrum

- **"Cool, you 3D-printed the save icon!"**



Two thirds of children don't know what a floppy disk is

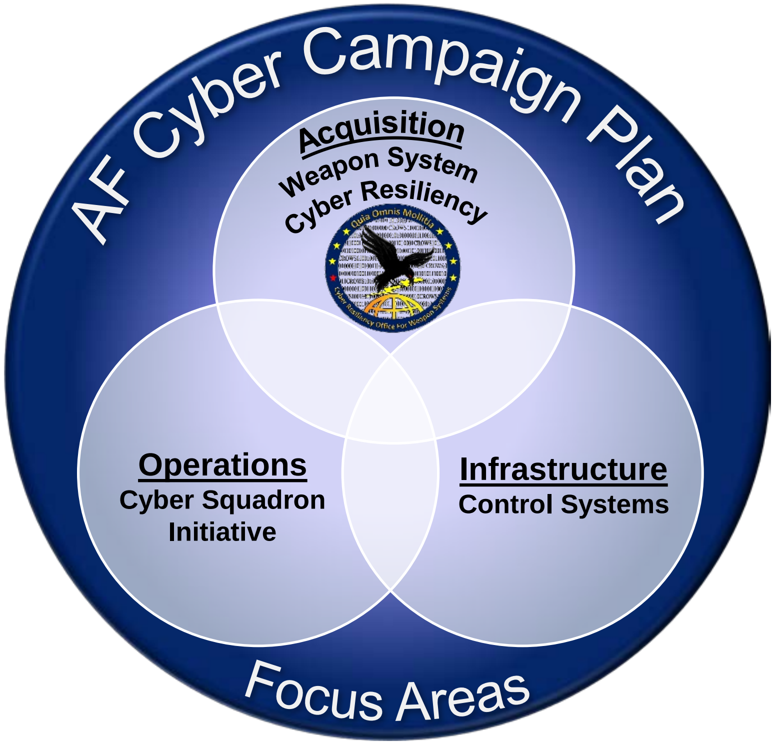
Children aged 6-18 were shown the photos below and asked if they knew what each was. Figures shown are the % of children who either said they didn't know what the item was, or gave an incorrect answer (children answered in their own words)

*we accepted the answer "phone" in each case

YouGov | yougov.com

February 23 - March 5, 2018

AF Cyber Campaign Plan



CUSTOMERS AND MISSION PARTNERS

AIR FORCE LCMC
AIR FORCE NUCLEAR WEAPONS CENTER
SPACE & MISSILE SYSTEMS CENTER
AF SUSTAINMENT CENTER
AIR FORCE RESEARCH LABORATORY
AD INEXPLORATA
OPERATIONAL TEST & EVALUATION CENTER

MISSION

Increase cyber resiliency of AF weapon systems to maintain mission effective capability under adverse conditions

GOALS

Bake cyber resiliency into new weapon systems

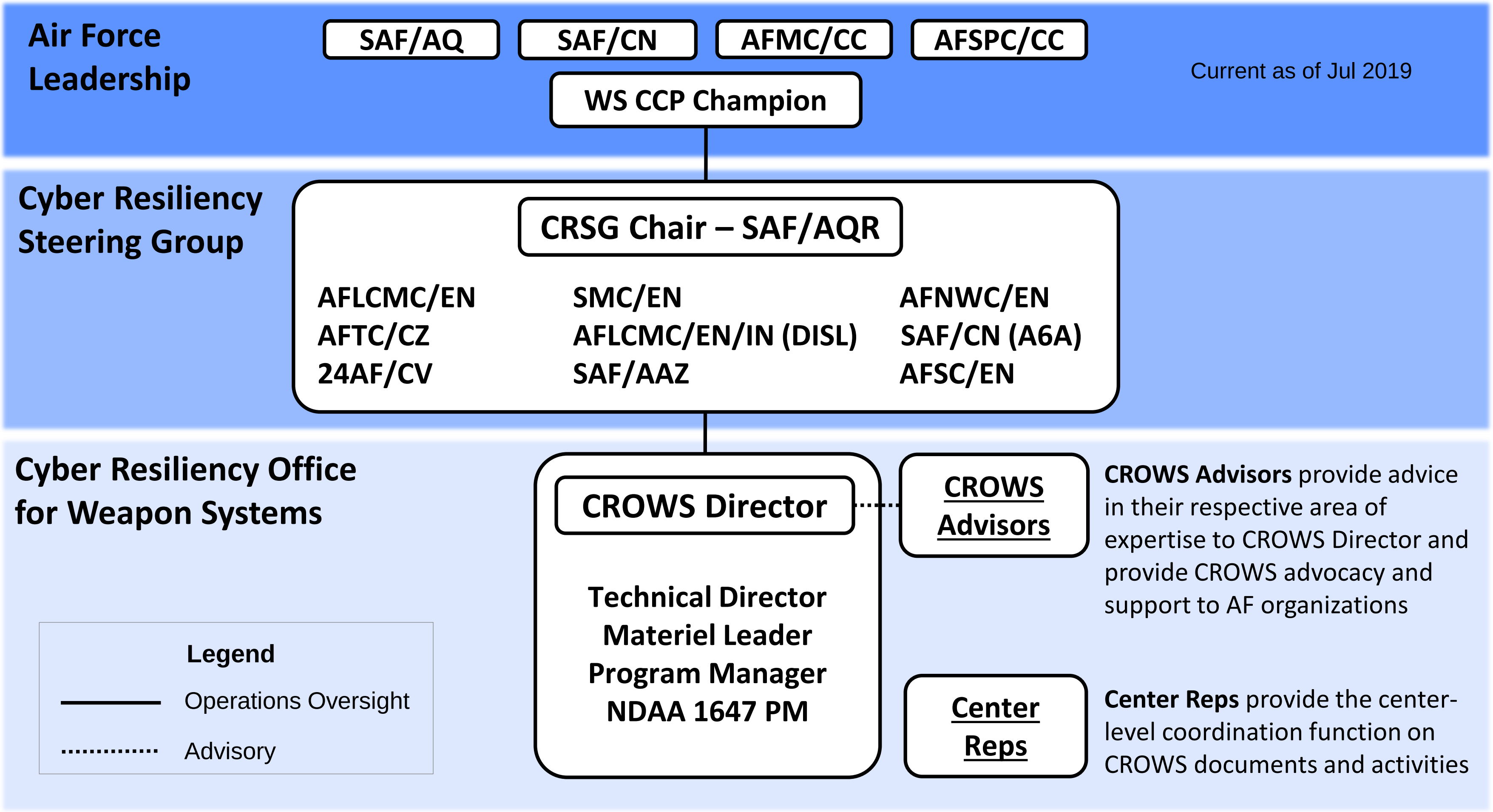
Mitigate critical vulnerabilities in fielded weapon systems

VISION

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

Approved for Public Release;
Distribution Unlimited. Case 2019-0702

CROWS Structure



Air Force Leadership

SAF/AQ

SAF/CN

AFMC/CC

AFSPC/CC

WS CCP Champion

Current as of Jul 2019

Cyber Resiliency Steering Group

CRSG Chair – SAF/AQR

AFLCMC/EN
AFTC/CZ
24AF/CV

SMC/EN
AFLCMC/EN/IN (DISL)
SAF/AAZ

AFNWC/EN
SAF/CN (A6A)
AFSC/EN

Cyber Resiliency Office for Weapon Systems

CROWS Director

Technical Director
Materiel Leader
Program Manager
NDAA 1647 PM

CROWS Advisors

CROWS Advisors provide advice in their respective area of expertise to CROWS Director and provide CROWS advocacy and support to AF organizations

Center Reps

Center Reps provide the center-level coordination function on CROWS documents and activities

Legend

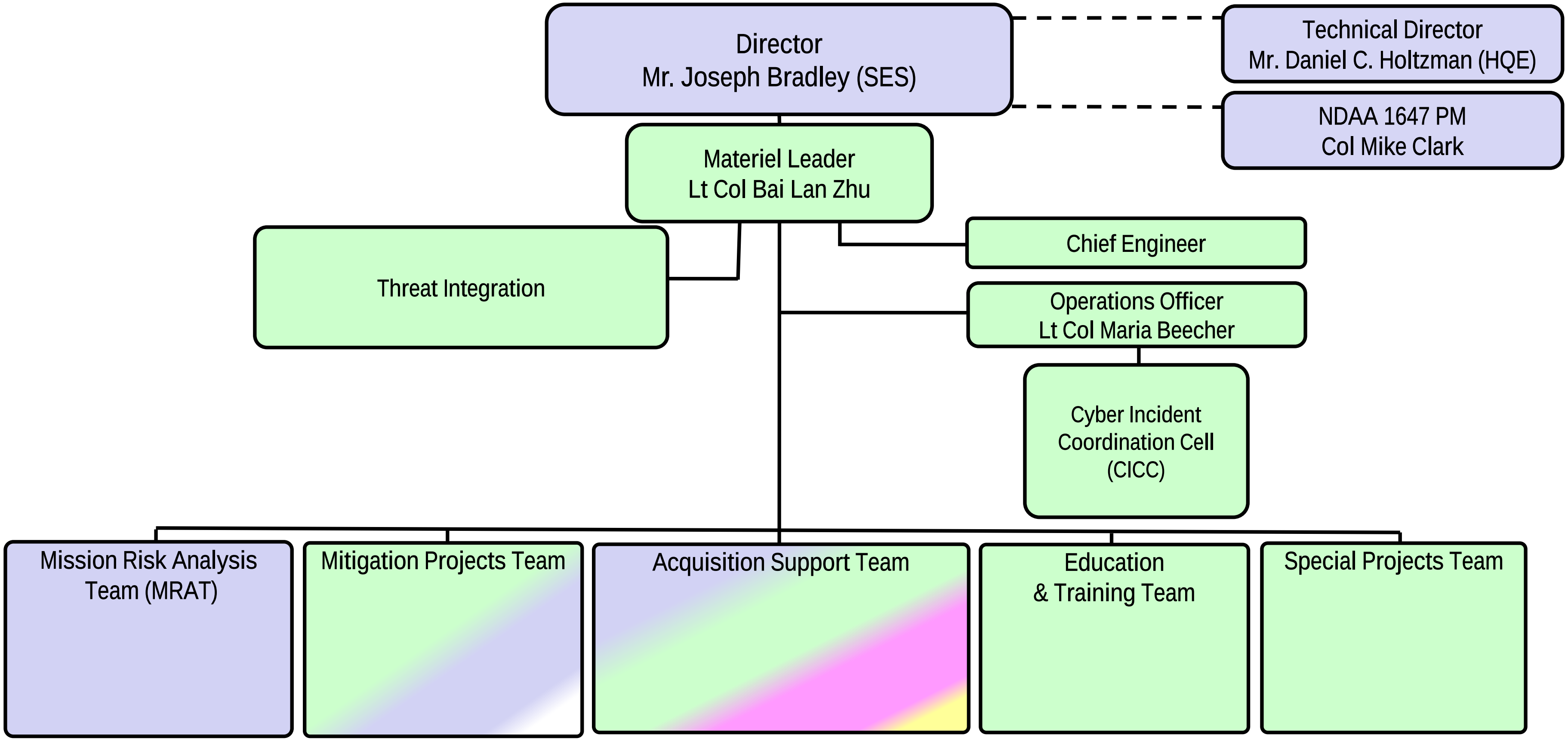
───── Operations Oversight

┈┈┈┈┈ Advisory

CROWS is an Air Force-level organization that reports to the SAF/AQR-chaired CRSG

Approved for Public Release;
Distribution Unlimited. Case 2019-0702

CROWS Organization



Director
Mr. Joseph Bradley (SES)

Technical Director
Mr. Daniel C. Holtzman (HQE)

NDAA 1647 PM
Col Mike Clark

Materiel Leader
Lt Col Bai Lan Zhu

Threat Integration

Chief Engineer

Operations Officer
Lt Col Maria Beecher

Cyber Incident Coordination Cell (CICC)

Mission Risk Analysis Team (MRAT)

Mitigation Projects Team

Acquisition Support Team

Education & Training Team

Special Projects Team

Hanscom | Wright-Patt | Hill
Eglin | Los Angeles

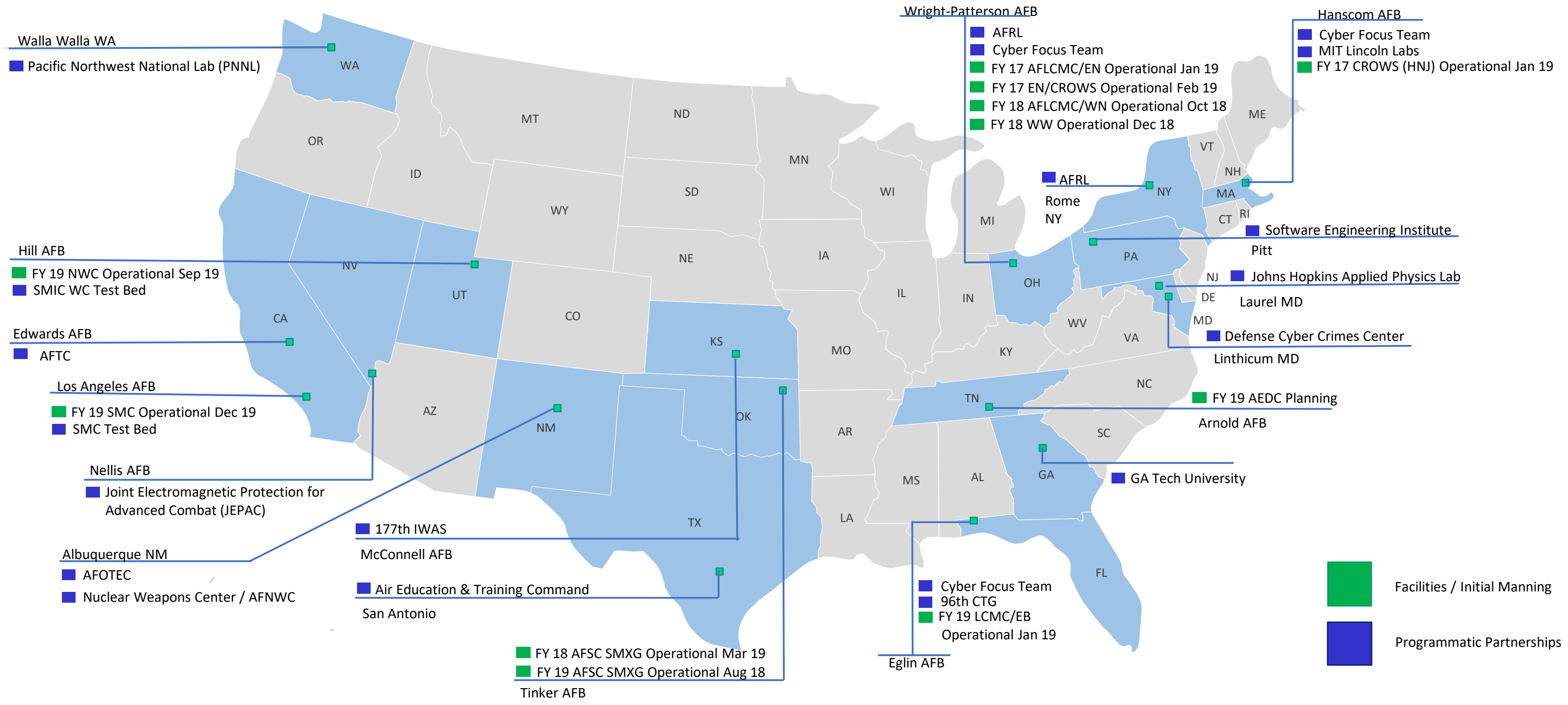
*Current as of 18 Aug 2019

U.S. AIR FORCE

CROWS Footprint

Facilities, Initial Manning, and Programmatic Partnerships

CROWS@US.AF.MIL



Walla Walla WA
🟦 Pacific Northwest National Lab (PNNL)

Hill AFB
🟩 FY 19 NWC Operational Sep 19
🟦 SMIC WC Test Bed

Edwards AFB
🟦 AFTC

Los Angeles AFB
🟩 FY 19 SMC Operational Dec 19
🟦 SMC Test Bed

Nellis AFB
🟦 Joint Electromagnetic Protection for Advanced Combat (JEPAC)

Albuquerque NM
🟦 AFOTEC
🟦 Nuclear Weapons Center / AFNWC

🟦 177th IWAS
McConnell AFB

🟦 Air Education & Training Command
San Antonio

🟩 FY 18 AFSC SMXG Operational Mar 19
🟩 FY 19 AFSC SMXG Operational Aug 18
Tinker AFB

🟦 Cyber Focus Team
🟦 96th CTG
🟩 FY 19 LCMC/EB Operational Jan 19
Eglin AFB

Wright-Patterson AFB
🟦 AFRL
🟦 Cyber Focus Team
🟩 FY 17 AFLCMC/EN Operational Jan 19
🟩 FY 17 EN/CROWS Operational Feb 19
🟩 FY 18 AFLCMC/WN Operational Oct 18
🟩 FY 18 WW Operational Dec 18

🟦 AFRL
Rome
NY

Hanscom AFB
🟦 Cyber Focus Team
🟦 MIT Lincoln Labs
🟩 FY 17 CROWS (HNJ) Operational Jan 19

🟦 Software Engineering Institute
Pitt

🟦 Johns Hopkins Applied Physics Lab
Laurel MD

🟦 Defense Cyber Crimes Center
Linthicum MD

🟩 FY 19 AEDC Planning
Arnold AFB

🟦 GA Tech University

🟩 Facilities / Initial Manning

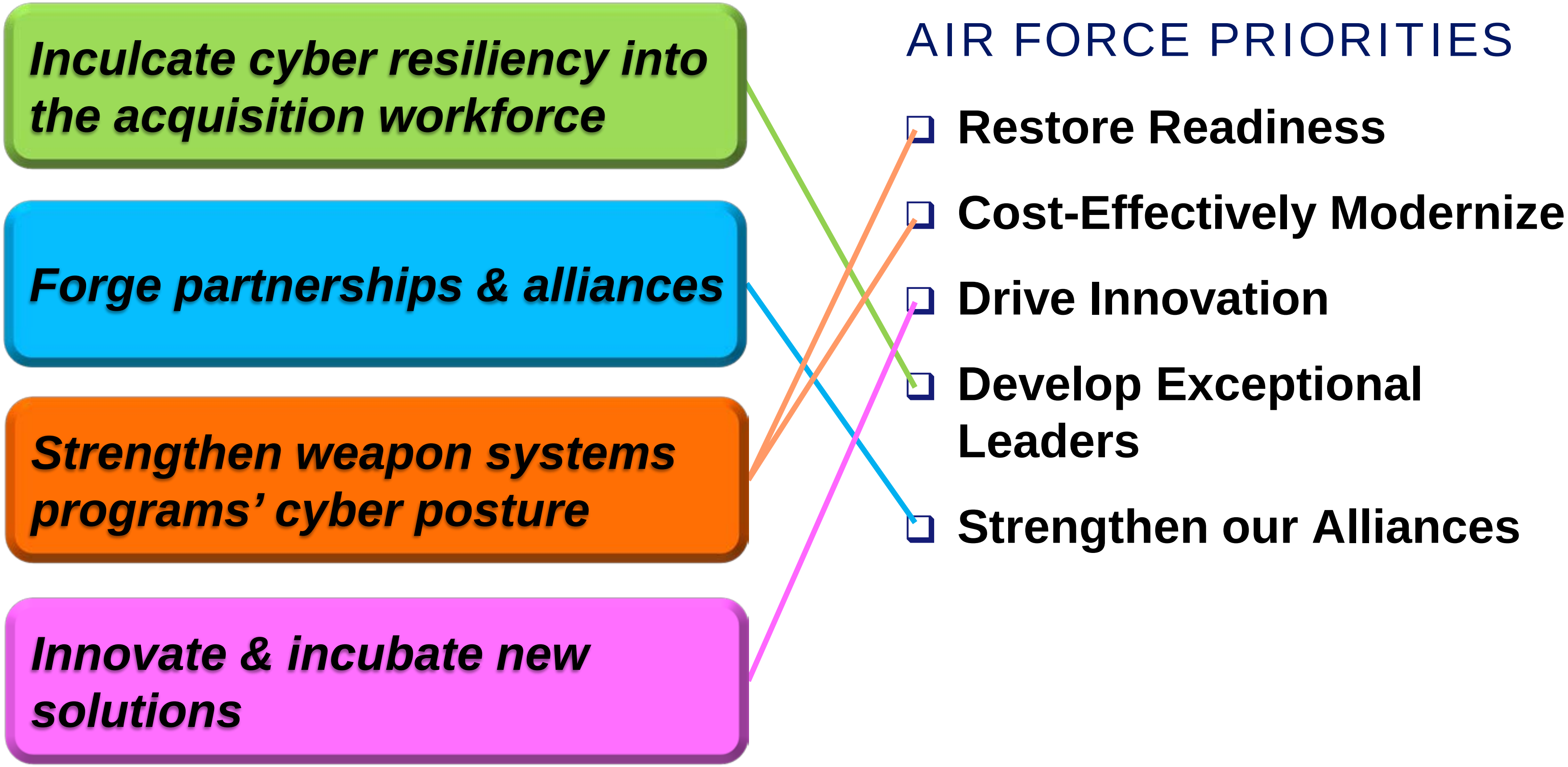
🟦 Programmatic Partnerships

As of: 01 Feb 2019 : POC Raoul Fischer

**Approved for Public Release;
Distribution Unlimited. Case** 2019-0702

Integrity – Service – Excellence

CROWS Prorities



Inculcate cyber resiliency into the acquisition workforce

Forge partnerships & alliances

Strengthen weapon systems programs' cyber posture

Innovate & incubate new solutions

AIR FORCE PRIORITIES

- ❑ **Restore Readiness**
- ❑ **Cost-Effectively Modernize**
- ❑ **Drive Innovation**
- ❑ **Develop Exceptional Leaders**
- ❑ **Strengthen our Alliances**

CROWS philosophy is to <u>help programs be successful</u> in addressing cyber resiliency

CROWS Major Efforts

Conduct NDAA 1647 Assessments

Analyze data to prioritize vulnerabilities

Lead cyber incident response

Partner with PMOs & Industry to develop mitigation solutions

Incubate emerging technologies

Develop products, tools, guides, & training to help PMOs bake cyber resiliency into weapon systems

Hiring, train, & deploy CRST & CFTs

Develop common security environment

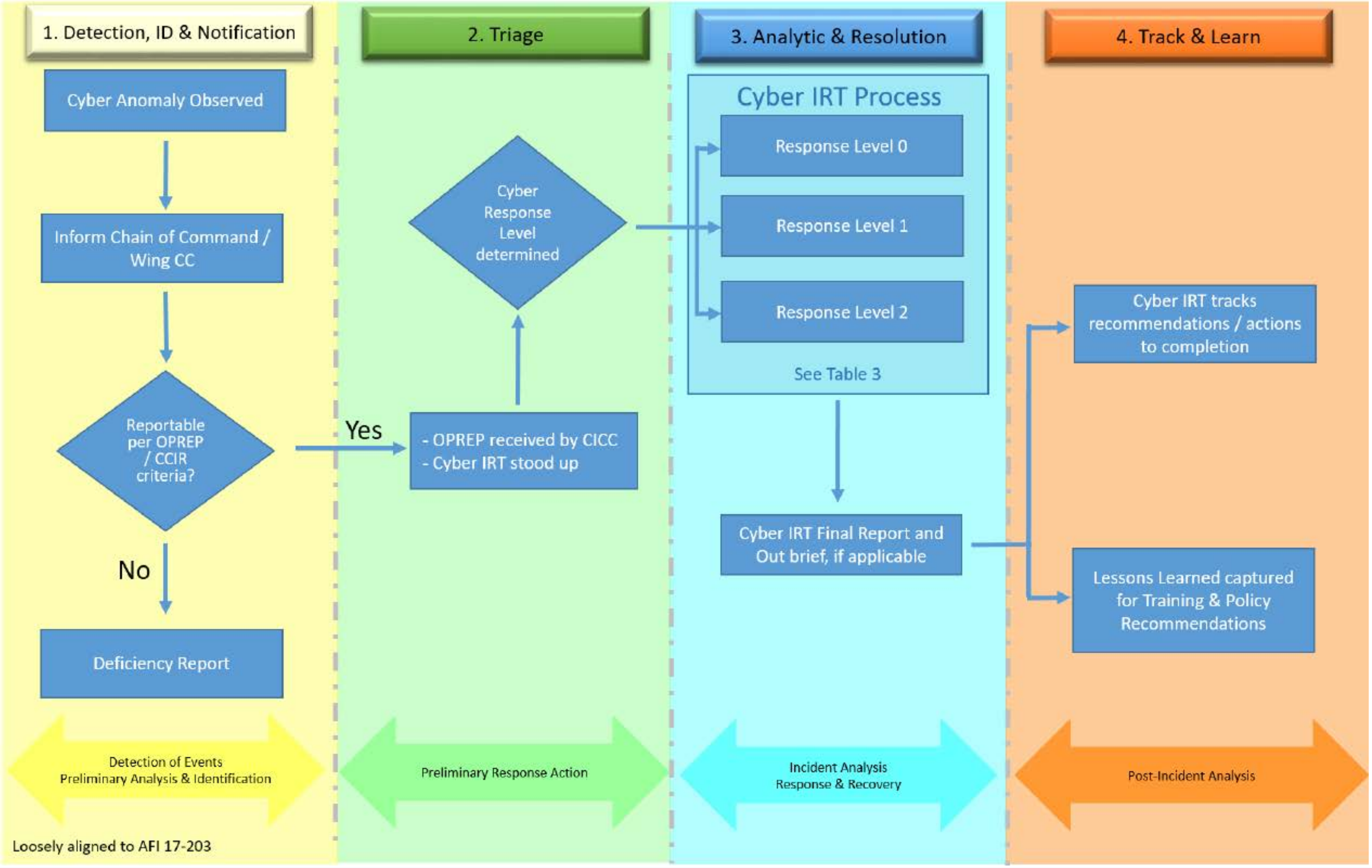
Collect, analyze, and apply cyber relevant threat information

Approved for Public Release;
Distribution Unlimited. Case 2019-0702

Cyber Resiliency

- Definition (What does it mean?)
  - Cyber Resiliency = ***<u>The ability to provide required capability despite adversity</u>***, that impacts the Cyber aspects of the Systems
  - "Cyber Aspects" = Software, Firmware and data in electronic form and the associated hardware
- Cyber Resilience, like system security, is an end goal:
  - And just like security having protection mechanisms (aka controls) that do not necessary combine to make one "adequately secure",
  - Having a set of resilience techniques and a framework for their application does not necessary combine to make one "resilient".

Cyber Incident Collaboration Center (CICC) Process Flow

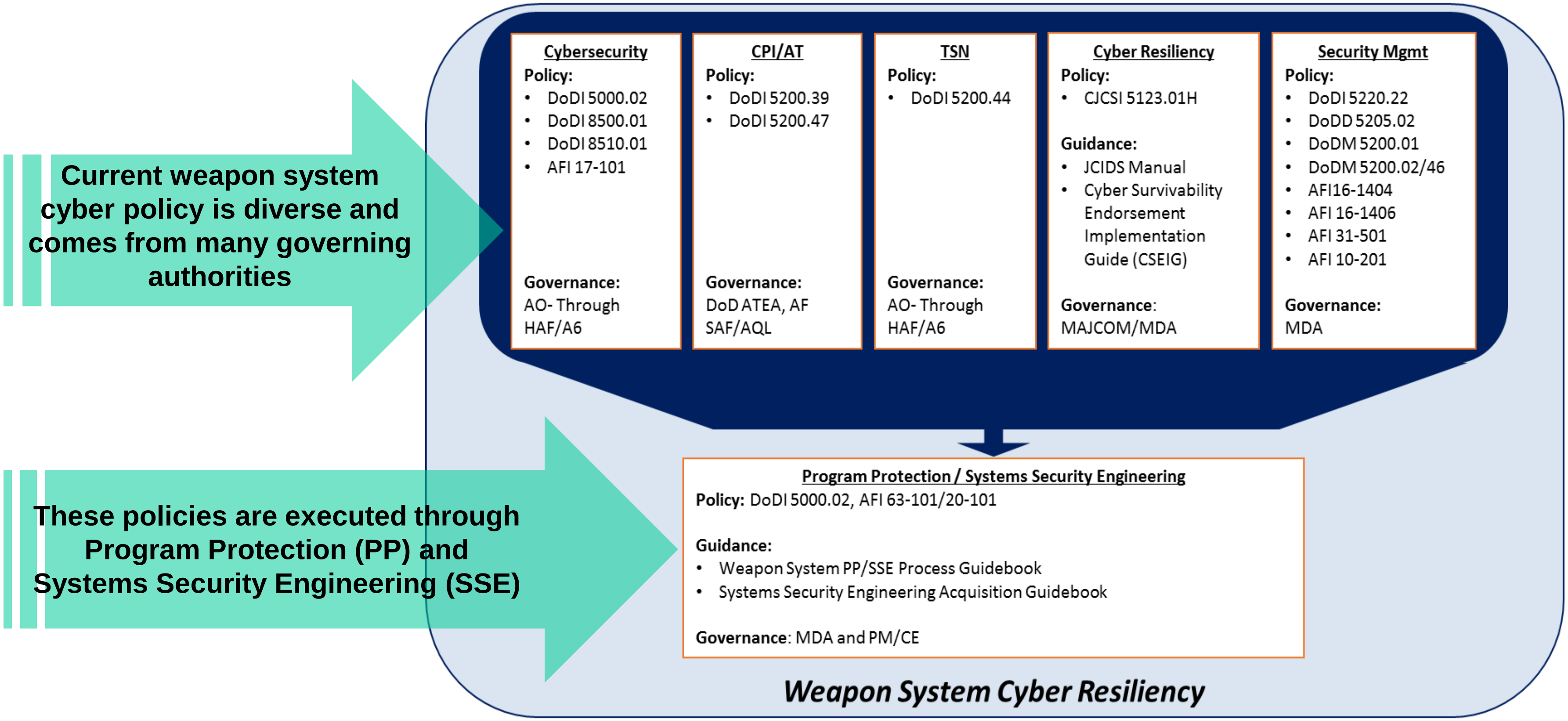


1. Detection, ID & Notification
2. Triage
3. Analytic & Resolution
4. Track & Learn
Cyber Anomaly Observed
Inform Chain of Command / Wing CC
Reportable per OPREP / CCIR criteria?
Yes
No
Deficiency Report
- OPREP received by CICC
- Cyber IRT stood up
Cyber Response Level determined
Cyber IRT Process
Response Level 0
Response Level 1
Response Level 2
See Table 3
Cyber IRT Final Report and Out brief, if applicable
Cyber IRT tracks recommendations / actions to completion
Lessons Learned captured for Training & Policy Recommendations
Detection of Events
Preliminary Analysis & Identification
Preliminary Response Action
Incident Analysis
Response & Recovery
Post-Incident Analysis
Loosely aligned to AFI 17-203

Approved for Public Release;
Distribution Unlimited. Case 2019-0702

Integrity – Service – Excellence

Weapon System Cyber Resiliency Policy



Current weapon system cyber policy is diverse and comes from many governing authorities

Cybersecurity

Policy:
- DoDI 5000.02
- DoDI 8500.01
- DoDI 8510.01
- AFI 17-101

Governance: AO- Through HAF/A6

CPI/AT

Policy:
- DoDI 5200.39
- DoDI 5200.47

Governance: DoD ATEA, AF SAF/AQL

TSN

Policy:
- DoDI 5200.44

Governance: AO- Through HAF/A6

Cyber Resiliency

Policy:
- CJCSI 5123.01H

Guidance:
- JCIDS Manual
- Cyber Survivability Endorsement Implementation Guide (CSEIG)

Governance: MAJCOM/MDA

Security Mgmt

Policy:
- DoDI 5220.22
- DoDD 5205.02
- DoDM 5200.01
- DoDM 5200.02/46
- AFI16-1404
- AFI 16-1406
- AFI 31-501
- AFI 10-201

Governance: MDA

These policies are executed through Program Protection (PP) and Systems Security Engineering (SSE)

Program Protection / Systems Security Engineering

Policy: DoDI 5000.02, AFI 63-101/20-101

Guidance:
- Weapon System PP/SSE Process Guidebook
- Systems Security Engineering Acquisition Guidebook

Governance: MDA and PM/CE

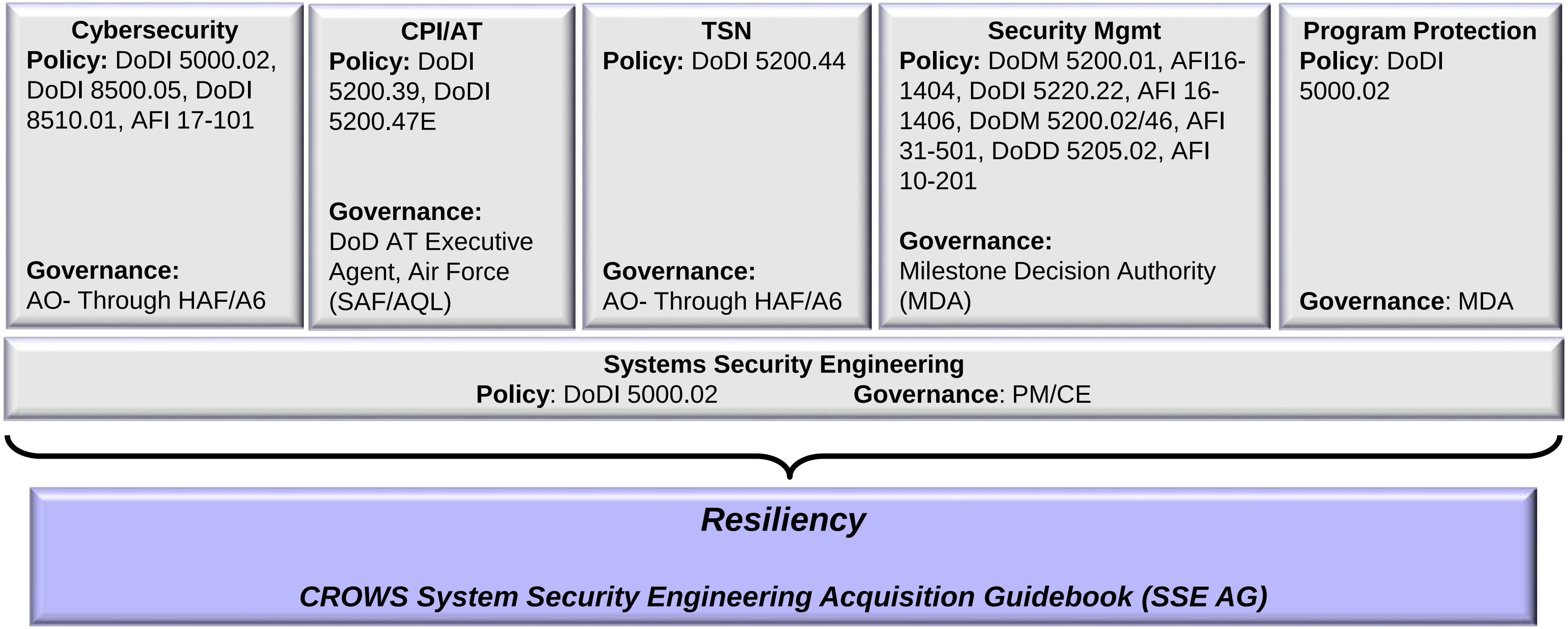
Weapon System Cyber Resiliency

CPI - Critical Program Information
AT - Anti-Tamper
TSN - Trusted Systems and Networks

CROWS delivered consolidated practitioner's guide for PP/SSE execution

SSE Acquisition Guidebook

What is it? A guidebook of best practices of how to integrate Systems Security Engineering and cyber considerations into acquisition documents in order to bake cyber resiliency into USAF weapon systems



Cybersecurity
Policy: DoDI 5000.02, DoDI 8500.05, DoDI 8510.01, AFI 17-101
Governance: AO- Through HAF/A6

CPI/AT
Policy: DoDI 5200.39, DoDI 5200.47E
Governance: DoD AT Executive Agent, Air Force (SAF/AQL)

TSN
Policy: DoDI 5200.44
Governance: AO- Through HAF/A6

Security Mgmt
Policy: DoDM 5200.01, AFI16-1404, DoDI 5220.22, AFI 16-1406, DoDM 5200.02/46, AFI 31-501, DoDD 5205.02, AFI 10-201
Governance: Milestone Decision Authority (MDA)

Program Protection
Policy: DoDI 5000.02
Governance: MDA

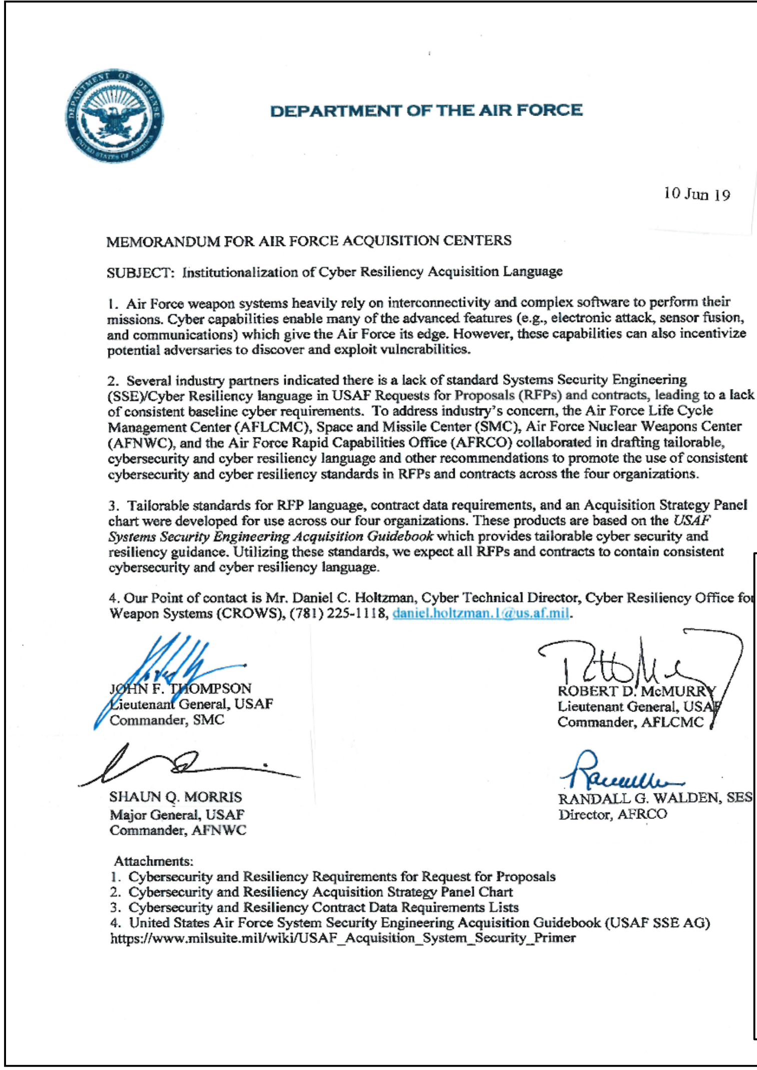
Systems Security Engineering
Policy: DoDI 5000.02 **Governance**: PM/CE

Resiliency

CROWS System Security Engineering Acquisition Guidebook (SSE AG)

Contractual language and requirements to execute SSE policies captured in SSE AG

Institutionalizing Cyber Resiliency



DEPARTMENT OF THE AIR FORCE

10 Jun 19

MEMORANDUM FOR AIR FORCE ACQUISITION CENTERS

SUBJECT: Institutionalization of Cyber Resiliency Acquisition Language

1. Air Force weapon systems heavily rely on interconnectivity and complex software to perform their missions. Cyber capabilities enable many of the advanced features (e.g., electronic attack, sensor fusion, and communications) which give the Air Force its edge. However, these capabilities can also incentivize potential adversaries to discover and exploit vulnerabilities.

2. Several industry partners indicated there is a lack of standard Systems Security Engineering (SSE)/Cyber Resiliency language in USAF Requests for Proposals (RFPs) and contracts, leading to a lack of consistent baseline cyber requirements. To address industry's concern, the Air Force Life Cycle Management Center (AFLCMC), Space and Missile Center (SMC), Air Force Nuclear Weapons Center (AFNWC), and the Air Force Rapid Capabilities Office (AFRCO) collaborated in drafting tailorable, cybersecurity and cyber resiliency language and other recommendations to promote the use of consistent cybersecurity and cyber resiliency standards in RFPs and contracts across the four organizations.

3. Tailorable standards for RFP language, contract data requirements, and an Acquisition Strategy Panel chart were developed for use across our four organizations. These products are based on the *USAF Systems Security Engineering Acquisition Guidebook* which provides tailorable cyber security and resiliency guidance. Utilizing these standards, we expect all RFPs and contracts to contain consistent cybersecurity and cyber resiliency language.

4. Our Point of contact is Mr. Daniel C. Holtzman, Cyber Technical Director, Cyber Resiliency Office for Weapon Systems (CROWS), (781) 225-1118, daniel.holtzman.1@us.af.mil.

JOHN F. THOMPSON
Lieutenant General, USAF
Commander, SMC

ROBERT D. McMURRY
Lieutenant General, USAF
Commander, AFLCMC

SHAUN Q. MORRIS
Major General, USAF
Commander, AFNWC

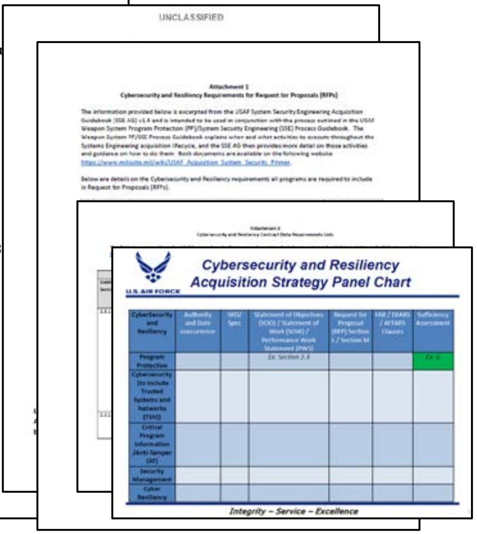
RANDALL G. WALDEN, SES
Director, AFRCO

Attachments:
1. Cybersecurity and Resiliency Requirements for Request for Proposals
2. Cybersecurity and Resiliency Acquisition Strategy Panel Chart
3. Cybersecurity and Resiliency Contract Data Requirements Lists
4. United States Air Force System Security Engineering Acquisition Guidebook (USAF SSE AG)
https://www.milsuite.mil/wiki/USAF_Acquisition_System_Security_Primer

AFLCMC, SMC, AFNWC, AFRCO Collaboration

- Provide consistent messaging to Industry
- Cyber Resiliency is important and expected

Tailorable standard language for RFPs, CDRLs, and ASP chart



UNCLASSIFIED

Attachment 1
Cybersecurity and Resiliency Requirements for Request for Proposals (RFPs)

The information provided below is excerpted from the USAF System Security Engineering Acquisition Guidebook (SSE AG) v1.4 and is intended to be used in conjunction with the process outlined in the USAF Weapon System Program Protection (PP)/System Security Engineering (SSE) Process Guidebook. The Weapon System PP/SSE Process Guidebook explains when and what activities to execute throughout the Systems Engineering acquisition lifecycle, and the SSE AG then provides more detail on those activities and guidance on how to do them. Both documents are available on the following website https://www.milsuite.mil/wiki/USAF_Acquisition_System_Security_Primer.

Below are details on the Cybersecurity and Resiliency requirements all programs are required to include in Request for Proposals (RFPs).

Attachment 3
Cybersecurity and Resiliency Contract Data Requirements Lists

Cybersecurity and Resiliency Acquisition Strategy Panel Chart

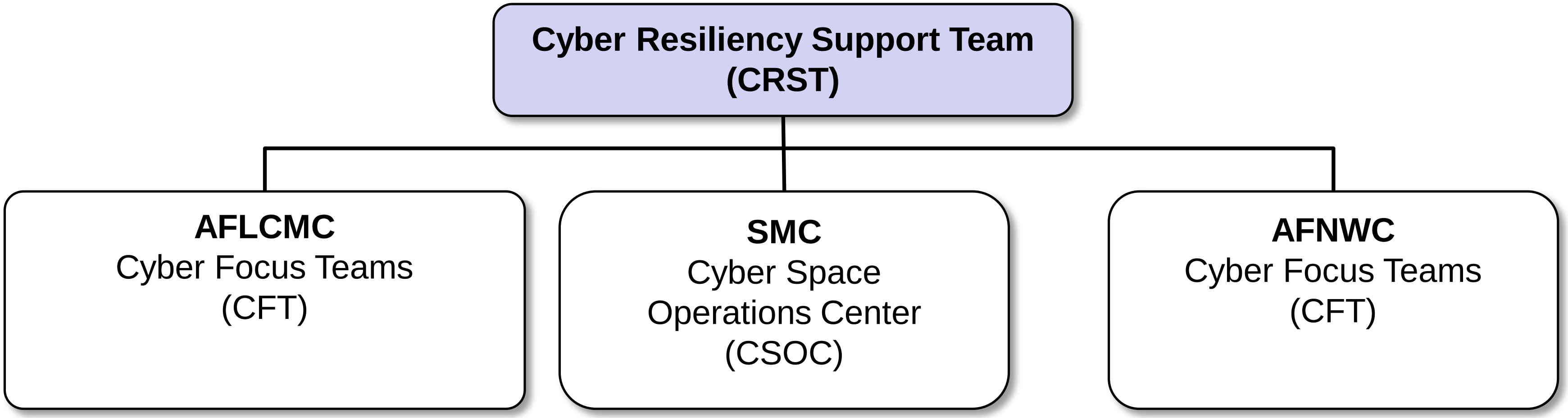
CyberSecurity and Resiliency	Authority and Date concurrence	SRD/Spec	Statement of Objectives (SOO) / Statement of Work (SOW) / Performance Work Statement (PWS)	Request for Proposal (RFP) Section L / Section M	FAR / DFARS / AFFARS Clauses	Sufficiency Assessment
Program Protection			Ex: Section 2.3			Ex: G
Cybersecurity (to include Trusted Systems and Networks (TSN))						
Critical Program Information (Anti-Tamper (AT))						
Security Management						
Cyber Resiliency						

Integrity – Service – Excellence

- Based on the AF SSE Acquisition Guidebook
- Contact: crows@us.af.mil

Approved for Public Release;
Distribution Unlimited. Case 2019-0702

Cyber Resiliency Support Team (CRST)



Cyber Resiliency Support Team (CRST)

AFLCMC
Cyber Focus Teams
(CFT)

SMC
Cyber Space
Operations Center
(CSOC)

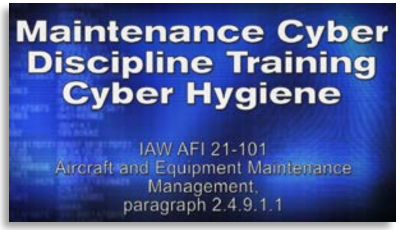
AFNWC
Cyber Focus Teams
(CFT)

Cyber Resiliency Support Team

Cross Enterprise support to CFTs and PMOs

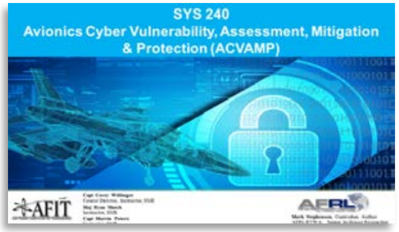
- CFT On-Board Training
- CROWS published products
- ID/Distribute Lessons Learned/Best Practices
- Feedback loop to CROWS

Cyber Training Fielded

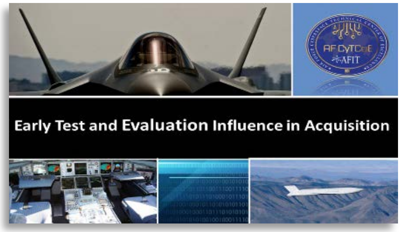


Maintenance Cyber Discipline Training
Cyber Hygiene

IAW AFI 21-101
Aircraft and Equipment Maintenance Management,
paragraph 2.4.9.1.1



SYS 240
Avionics Cyber Vulnerability, Assessment, Mitigation & Protection (ACVAMP)



Early Test and Evaluation Influence in Acquisition

- **Cyber Hygiene for Maintainers**
  - Fielded and mandated by AF/A4 for ~130k Active Duty, Guard and Reserve maintenance personnel (IAW 21-101)
  - Training requests received from acquisition and operations units across Centers, MAJCOMs, Services and International Partners
- **Avionics Cyber Vulnerability, Assessment, Mitigation & Protection (ACVAMP)**
  - CROWS sponsored course to be formalized into the AFIT course catalogue (SYS-240)
  - Over 1,000 students trained across multiple acquisition bases
- **Test & Evaluation Concepts & Policy for Cyber**
  - AFIT workshop initially offered in conjunction with SYS 252 & 253; Approaching 500 students trained
  - Incorporated into SYS 253 *Early Test and Evaluation Influence in Acquisition*, Spring 2018

CROWS Cyber Resiliency Support Team (CRST) & Cyber Focus Teams (CFTs) will provide cyber expertise to PMOs in CY19 – These courses are available NOW!

Common Security Environment

"…because they are not sharing vulnerability and threat information across programs, programs are unaware of their full risk exposure and DOD may have less insight into vulnerabilities across its weapon systems portfolio."

-- Oct 2018 GAO Report on Weapon Systems Cybersecurity

CROWS Initiatives:

- **Program & enterprise-wide cybersecurity classification guide**
- **Build common, accredited secure facilities to permit PEOs, Engineers, Intel & Acquisition Security teams to understand and mitigate threats**

FIGHTER-BOMBER DIRECTORATE
Quia Omnis Mollitia
Cyber Resiliency Office For Weapon Systems

Approved for Public Release;
Distribution Unlimited. Case 2019-0702

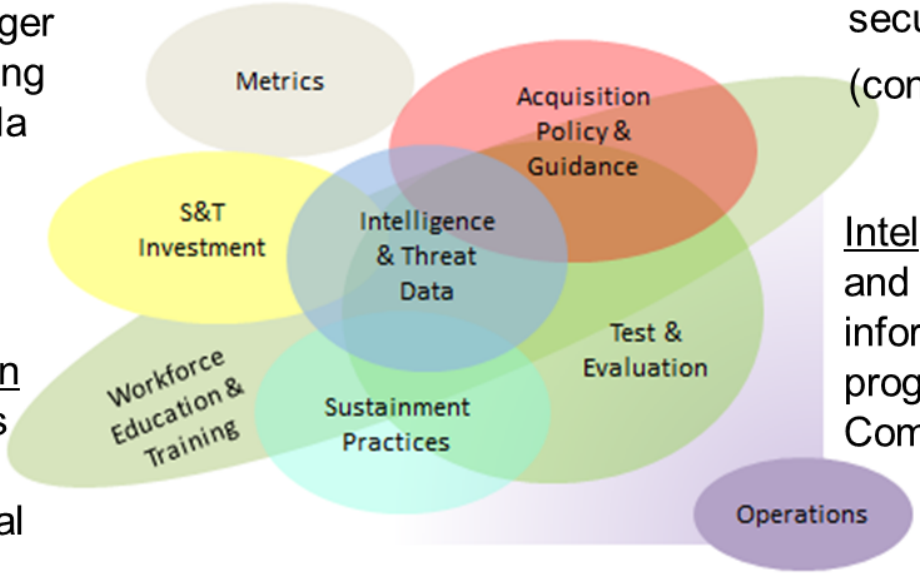
Technical Integration & Governance

An Integrated, Holistic Strategy

<u>Metrics</u> – Reporting metrics and measuring progress

<u>S&T</u> – Address longer term gaps by aligning AF research agenda

<u>Acquisition</u> – Policy & processes for acquiring secure resilient systems (contracting language)


Metrics
Acquisition Policy & Guidance
S&T Investment
Intelligence & Threat Data
Test & Evaluation
Workforce Education & Training
Sustainment Practices
Operations

<u>Workforce Education & Training</u> – Across ALL Centers for awareness, technical expertise

<u>Intel</u> – Communicating and sharing cyber threat information to acquisition programs, S&T and Test Community

<u>Sustainment</u> – Processes and methods to ensure and improve the security posture of operational systems

<u>T&E</u> – Effective ways of testing protection and resiliency & allocating appropriate resources

Cyber S&T Thoughts

- Engineering Cyber Resilience in Weapons Systems
  - Criteria, Observables, Behaviors – What does Cyber Resiliency look like?
  - Requirements, Cost, Measures & Metrics – How to specify and measure Cyber Resiliency?
  - Acquisition Language, Design Standards – How to execute and implement Cyber Resiliency?

- Need to Secure
  - Software
  - Hardware
  - Integrated SW & HW
  - Carbon Based Units

- To Securely
  - Design & Develop Capabilities
  - Operate System/Missions
  - Maintain and Sustain Capabilities

Enable Cyber Mission Assurance

- Defining the problem space
  - Criteria
  - Observables
  - Behaviors

- To Define the Needs:
  - Mitigations
  - Capabilities
  - Investment Areas

Identify Any Gaps

- Solutions and S&T needs follow Gaps

Summary

- Cyber resiliency is a team sport – CROWS business model is based on partnerships
- CROWS has multiple efforts ongoing, with more planned
  - Assessments & Analysis
  - Mitigations
  - Provide PMOs cyber tools and manpower
  - Incubation of emerging technologies
  - Intelligence integration

Providing knowledge, tools, training, skilled workforce, and secure environments to the enterprise to enable programs to increase Weapon Systems Cyber Resiliency

Approved for Public Release;
Distribution Unlimited. Case 2019-0702

Cyber Resiliency Enablers
First Step – Systems Engineering

- What is the System? What does it do? CONOPS? Missions?
- What is the System Architecture? Weapon System (e.g. Aircraft), Ground Systems, Maintenance systems, Training systems……
- List of Hardware (LRU), Software and providence of each (e.g. supply chain); identification of Critical Program Information (CPI), Critical Components (CC); Technical Orders, Operational procedures
- Identification of all external communications access points
- How does Data flow into, thru and out of the system? What type of data? How is it protected? Where does it come from? Where does it go? What is it used for?
- What Threat/Intel information is available?

Approved for Public Release;
Distribution Unlimited. Case 2019-0702

Cyber Resiliency Office for Weapon Systems (CROWS)

Integrity - Service - Excellence

Questions & Discussion

CROWS@US.AF.MIL