U.S. Air Force

Integrity - Service - Excellence

AF Cyber Resiliency Office for Weapon Systems (CROWS)

NDIA Systems Engineering Conference

Mr. Danny Holtzman, HQE
Cyber Technical Director
SL, Cyber Security Engineering & Resiliency
daniel.holtzman.1@us.af.mil

25 October 2017

Cyber Resiliency – A War Winning Capability

DISTRIBUTION A. Approved for public release: distribution unlimited.

Overview

- AF Cyber Campaign Plan
- Cyber Resiliency Office for Weapon Systems (CROWS)
- Technical Integration & Governance
- Cyber Resiliency S&T Needs
- An Authorizing Official Perspective

facebook.com/DivineFeminineReawakening
Be around the Light Bringers, the Magic Makers, the World Shifters. They challenge you, break you open, uplift and expand you. They don't let you play small with your Life. These Heartbeats are your people. These people are your tribe.

AF Cyber Campaign Plan (CCP) Bottom Line Up Front

- AF Cyber Campaign Plan's (CCP) overall mission has two goals:
  - #1 "Bake-In" cyber resiliency into new weapon systems
  - #2 Mitigate "Critical" vulnerabilities in fielded weapon systems

- Established the Cyber Resiliency Steering Group (CRSG)
  - 8 voting members (SAF/AQR, LCMC, SMC, NWC, AFTC, Intel, SAF/CISO, & 24AF/CV)
  - Governance body to guide the AF Cyber Campaign Plan (CCP)

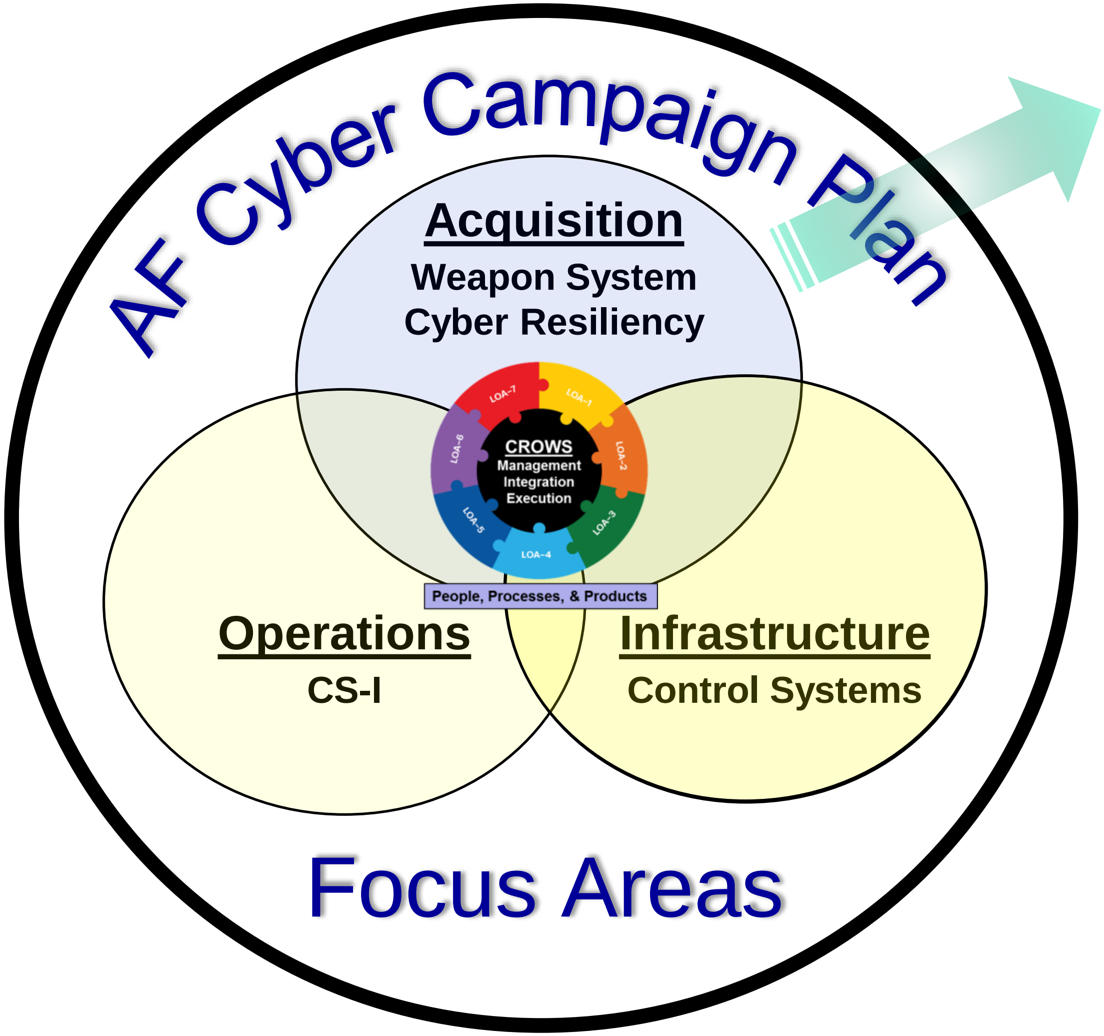
- Established dedicated office to manage execution ➡ Cyber Resiliency Office for Weapon Systems (CROWS)
  - Executing 7 Lines of Actions
  - Manage/execute the NDAA 1647 Weapon System Assessments and Mitigations

- Coordination with:
  - Cyber Squadron Initiative (Operational)
  - Industrial Control Systems (ICS) cyber protection measures (Infrastructure)
  - Test and Evaluation (infrastructure & capability growth)

Collaborate, Integrate and Execute

AF Cyber Campaign Plan (CCP)

Weapon System Vision, Mission and Goals



AF Cyber Campaign Plan

Acquisition

Weapon System Cyber Resiliency

CROWS

Management

Integration

Execution

People, Processes, & Products

Operations

CS-I

Infrastructure

Control Systems

Focus Areas

Vision

Cyber resiliency ingrained in AF culture

Mission

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

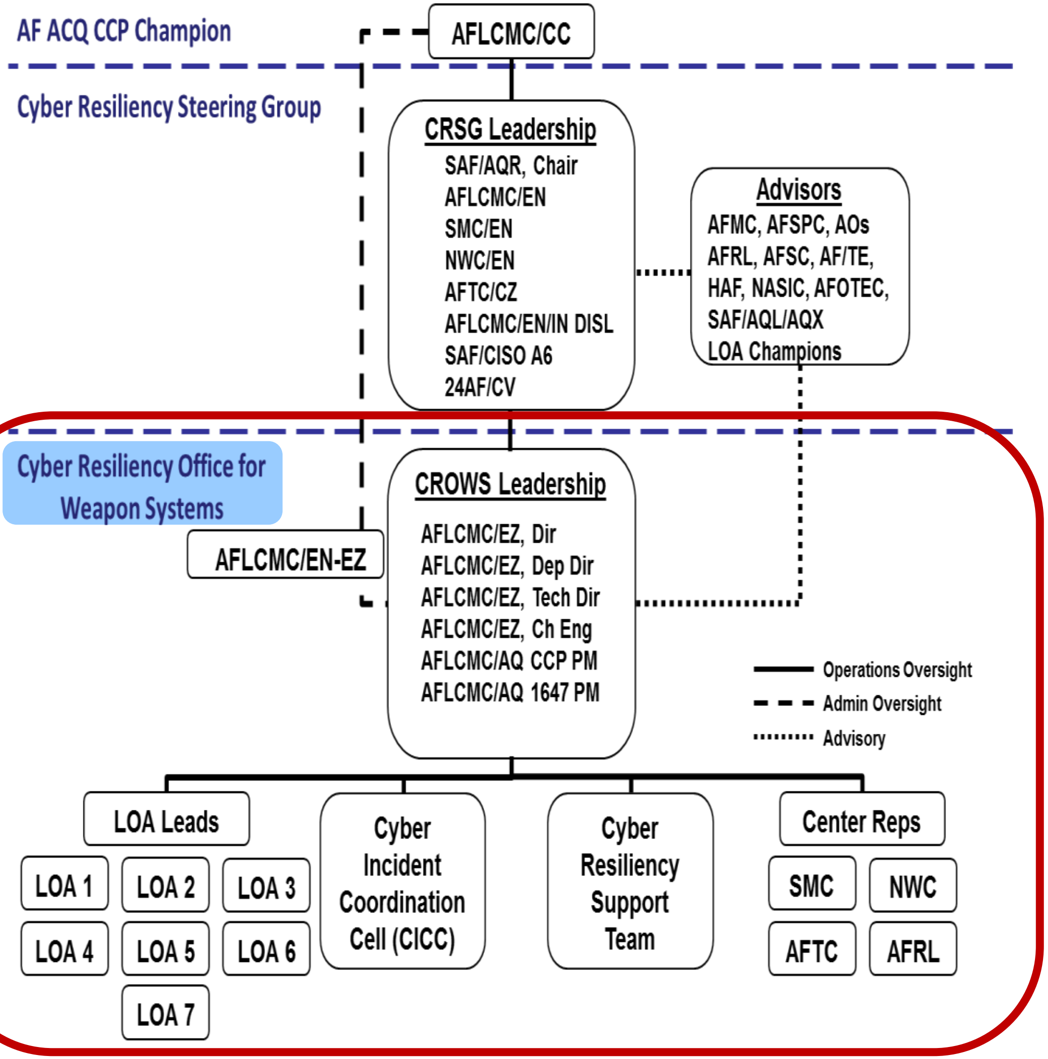
Goals

#1 "Bake-In" cyber resiliency into new weapon systems

#2 Mitigate "Critical" vulnerabilities in fielded weapon systems

Cyber Resiliency Office for Weapon Systems (CROWS)

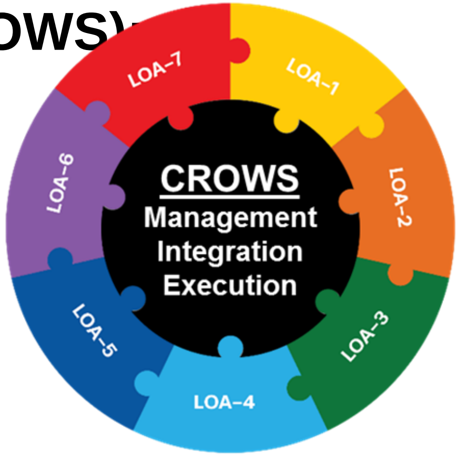
- Charter
  - Stakeholder signatures
  - AFLCMC/CC approval
- Scope
  - Weapon system cyber resiliency support for the acquisition community
  - CRSG/CROWS will collaborate and leverage the other CCP efforts to maximize the benefits for the AF mission and stakeholders



DISTRIBUTION A. Approved for public release: distribution unlimited.

Weapon System Cyber Campaign (CCP) Overview

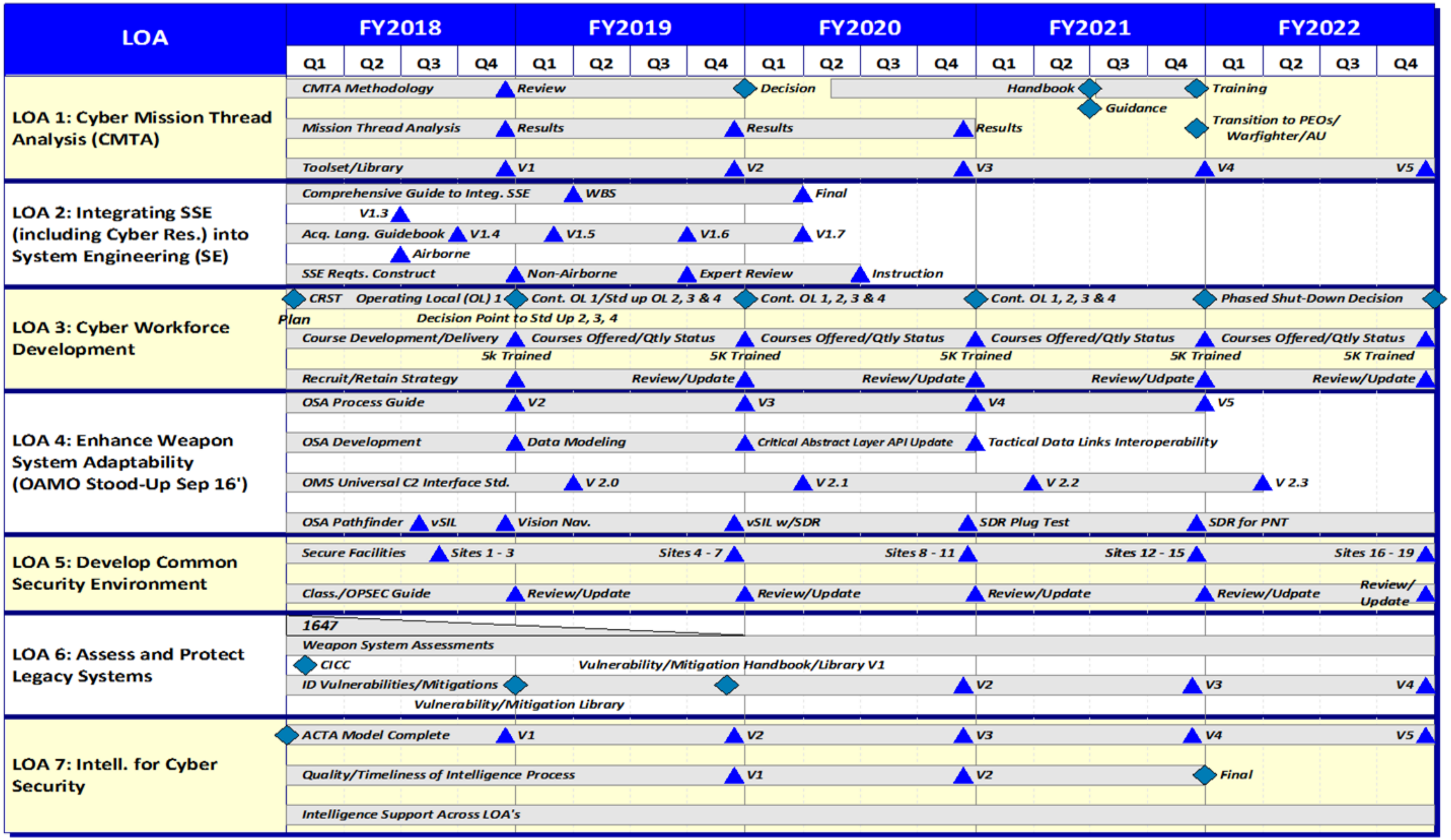
- **Cyber Resiliency Office for Weapon Systems (CROWS):**
  - Execution of Acquisition/Weapon System Cyber Campaign Plan
  - Execution of NDAA 1647 weapon system assessments
- **7 Lines of Action (LOAs)**
  - LOA 1: Cyber Mission Thread Analysis
  - LOA 2: Integrate SSE/Cyber Resiliency into SE
  - LOA 3: Cyber Workforce Development
  - LOA 4: Weapon System Agility & Adaptability
  - LOA 5: Common Security Environment
  - LOA 6: Assess & Protect Fielded Fleet
  - LOA 7: Cyber Intel Support



People, Processes, & Products

- **Cyber Resiliency Steering Group (CRSG):**
  - Weapon System CCP Guidance and Direction
  - 8 Voting Members:
    - SAF/AQR (Chari), LCMC, SMC, NWC, AFTC, Intel, SAF/CISO, 24AF

Weapon System Cyber Campaign Plan Schedule



LOA

FY2018 FY2019 FY2020 FY2021 FY2022

Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4

LOA 1: Cyber Mission Thread Analysis (CMTA)

CMTA Methodology – Review – Decision – Handbook – Training

Guidance

Mission Thread Analysis – Results – Results – Results

Transition to PEOs/ Warfighter/AU

Toolset/Library – V1 – V2 – V3 – V4 – V5

LOA 2: Integrating SSE (including Cyber Res.) into System Engineering (SE)

Comprehensive Guide to Integ. SSE – WBS – Final

V1.3

Acq. Lang. Guidebook – V1.4 – V1.5 – V1.6 – V1.7

Airborne

SSE Reqts. Construct – Non-Airborne – Expert Review – Instruction

LOA 3: Cyber Workforce Development

CRST Plan – Operating Local (OL) 1 – Cont. OL 1/Std up OL 2, 3 & 4 – Cont. OL 1, 2, 3 & 4 – Cont. OL 1, 2, 3 & 4 – Phased Shut-Down Decision

Decision Point to Std Up 2, 3, 4

Course Development/Delivery – Courses Offered/Qtly Status – Courses Offered/Qtly Status – Courses Offered/Qtly Status – Courses Offered/Qtly Status

5k Trained – 5K Trained – 5K Trained – 5K Trained – 5K Trained

Recruit/Retain Strategy – Review/Update – Review/Update – Review/Udpate – Review/Update

LOA 4: Enhance Weapon System Adaptability (OAMO Stood-Up Sep 16')

OSA Process Guide – V2 – V3 – V4 – V5

OSA Development – Data Modeling – Critical Abstract Layer API Update – Tactical Data Links Interoperability

OMS Universal C2 Interface Std. – V 2.0 – V 2.1 – V 2.2 – V 2.3

OSA Pathfinder – vSIL – Vision Nav. – vSIL w/SDR – SDR Plug Test – SDR for PNT

LOA 5: Develop Common Security Environment

Secure Facilities – Sites 1 - 3 – Sites 4 - 7 – Sites 8 - 11 – Sites 12 - 15 – Sites 16 - 19

Class./OPSEC Guide – Review/Update – Review/Update – Review/Update – Review/Udpate – Review/ Update

LOA 6: Assess and Protect Legacy Systems

1647

Weapon System Assessments

CICC – Vulnerability/Mitigation Handbook/Library V1

ID Vulnerabilities/Mitigations – V2 – V3 – V4

Vulnerability/Mitigation Library

LOA 7: Intell. for Cyber Security

ACTA Model Complete – V1 – V2 – V3 – V4 – V5

Quality/Timeliness of Intelligence Process – V1 – V2 – Final

Intelligence Support Across LOA's

DISTRIBUTION A. Approved for public release: distribution unlimited.

Breaking Barriers … Since 1947

Coming together is a beginning; keeping together is progress; working together is success.

Henry Ford

Cyber Resiliency for Weapon Systems

Technical Integration & Governance

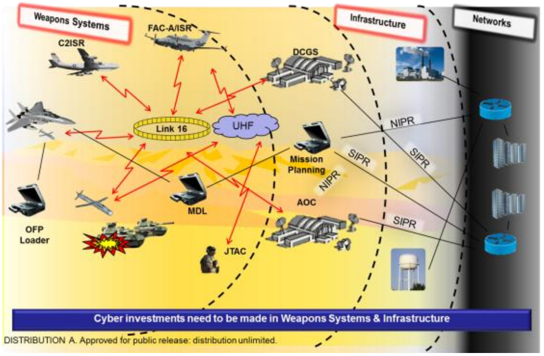
Mr. Daniel C. Holtzman, HQE
SL, Cyber Security Engineering & Resiliency

Cyber Resiliency for Weapon Systems On Going Alignment of Efforts

- ✓ **CR Technical Reference Architecture (CR-TRA)**
  - Framework for Cyber Resiliency in Weapon Systems
- ✓ **CR Technical Flight Plan (CR-RFP)**
  - Alignment of Technical Work Program
- ✓ **CR Advisory Council (CR-TAC)**
  - Alignment to Technical Flight Plan, Staffing/Comment adjudication, Technical recommendations, Technical Coordination/Reviews
- ✓ **FFRDC/UARC Collaboration**
  - AF Security Engineering Team (AFSET)
- ✓ **PEO / Programs**
  - Cyber Resiliency Review (Bi Annual)
  - PEO Directors of Engineering (DOE) Council
- ✓ **Industry**
  - Engagement via NDIA SE/SSE/T&E Committee's
  - Cyber Resiliency for Weapon Systems Round Table
- ✓ **Service's, OSD, Academia, NIST**

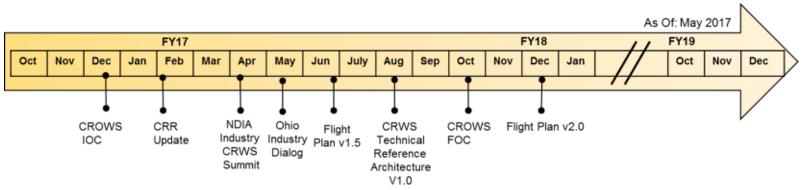
Cyber Resiliency Government Reference Architecture

- CR Technical Reference Architecture (CR-TRA)
- CR Technical Flight Plan (CR-TFP)
- CR Technical Advisory Council (CR-TAC)



Cyber investments need to be made in Weapons Systems & Infrastructure

DISTRIBUTION A. Approved for public release: distribution unlimited.



Technical Advisory Council (CRWS-TAC)

- Chair – AF Cyber Technical Director
- CO Chair – AFCISO

Criteria → **Design** → **Hardware**
Observables → **Operate** → **Software**
Behaviors → **Maintain** → **Carbon Based Units**

DISTRIBUTION A. Approved for public release: distribution unlimited.

Breaking Barriers … Since 1947

Communications & Collaborations On Going Efforts

- Information Sharing
  - Classification
  - Configuration Management
  - Mechanism/Process
  - Expectation Management
- Cyber Flash
  - Within Organization
  - External to Organization

- FFRDC/UARC – AFSET
  - Nine FFRDC/UARCs
- Industry – NDIA SE/SSE/TE Committee
  - 2017 NDIA Cyber Resiliency Summit
  - 2018 AF/Industry CRWS Round Table
- **CRWS Round Table**
  - Quarterly Industry Sponsored / Hosted
  - Adoption of Anti Tamper Model (as applicable)
- YOUR IDEAS HERE !!

Establishing an AF / Industry Cyber Resiliency for Weapon Systems Round Table

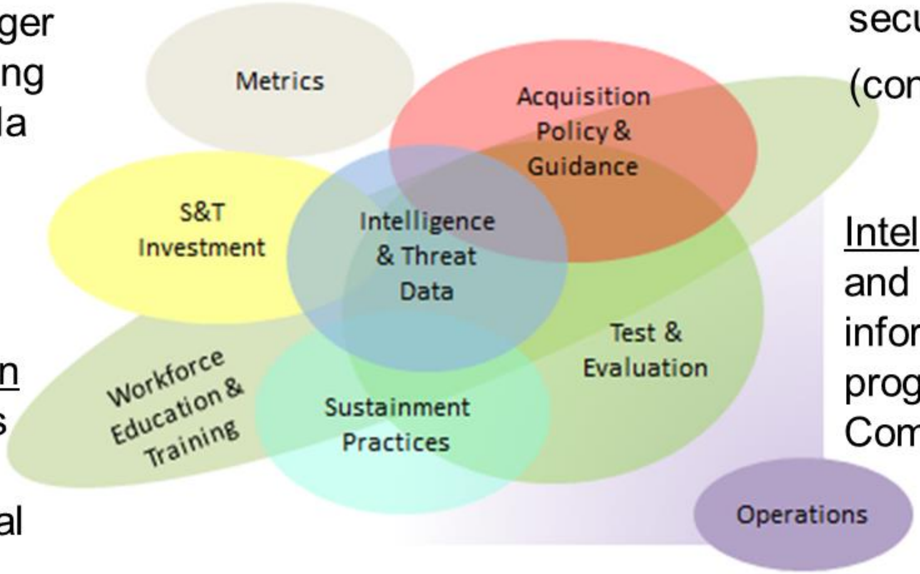
Technical Integration & Governance

Cyber Resiliency for Mission Assurance Requires an Integrated, Holistic Strategy

Metrics – Reporting metrics and measuring progress

Acquisition – Policy & processes for acquiring secure resilient systems (contracting language)

S&T – Address longer term gaps by aligning AF research agenda


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

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

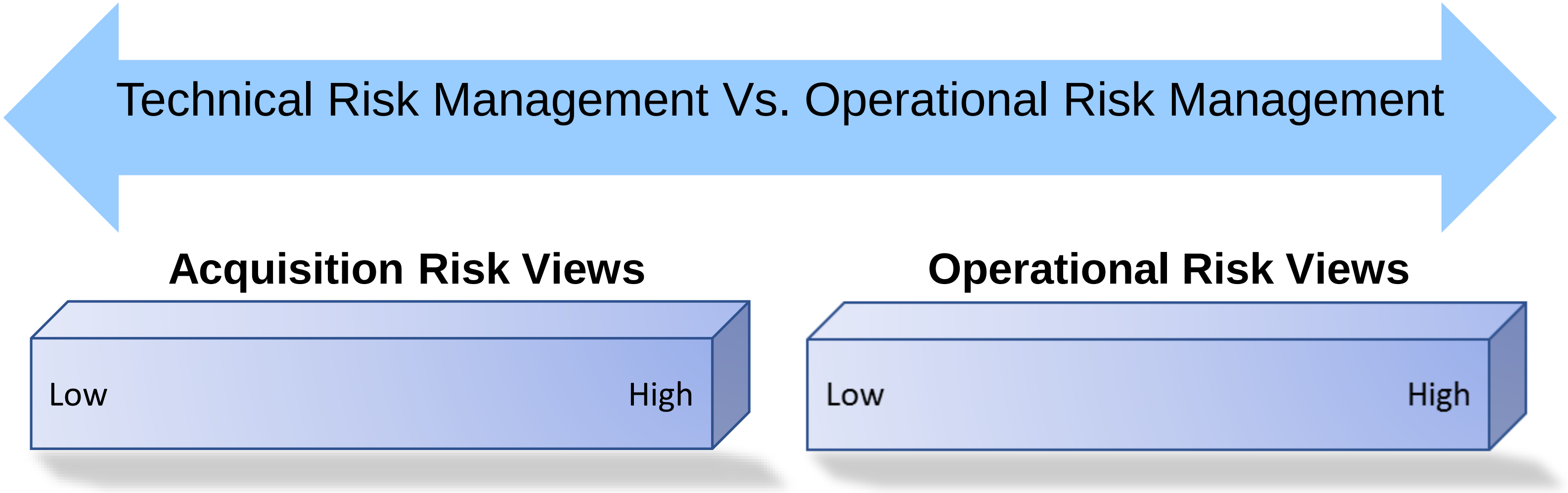
Workforce Education & Training – Across ALL Centers for awareness, technical expertise

Sustainment – Processes and methods to ensure and improve the security posture of operational systems

T&E – Effective ways of testing protection and resiliency & allocating appropriate resources

DISTRIBUTION A. Approved for public release: distribution unlimited.

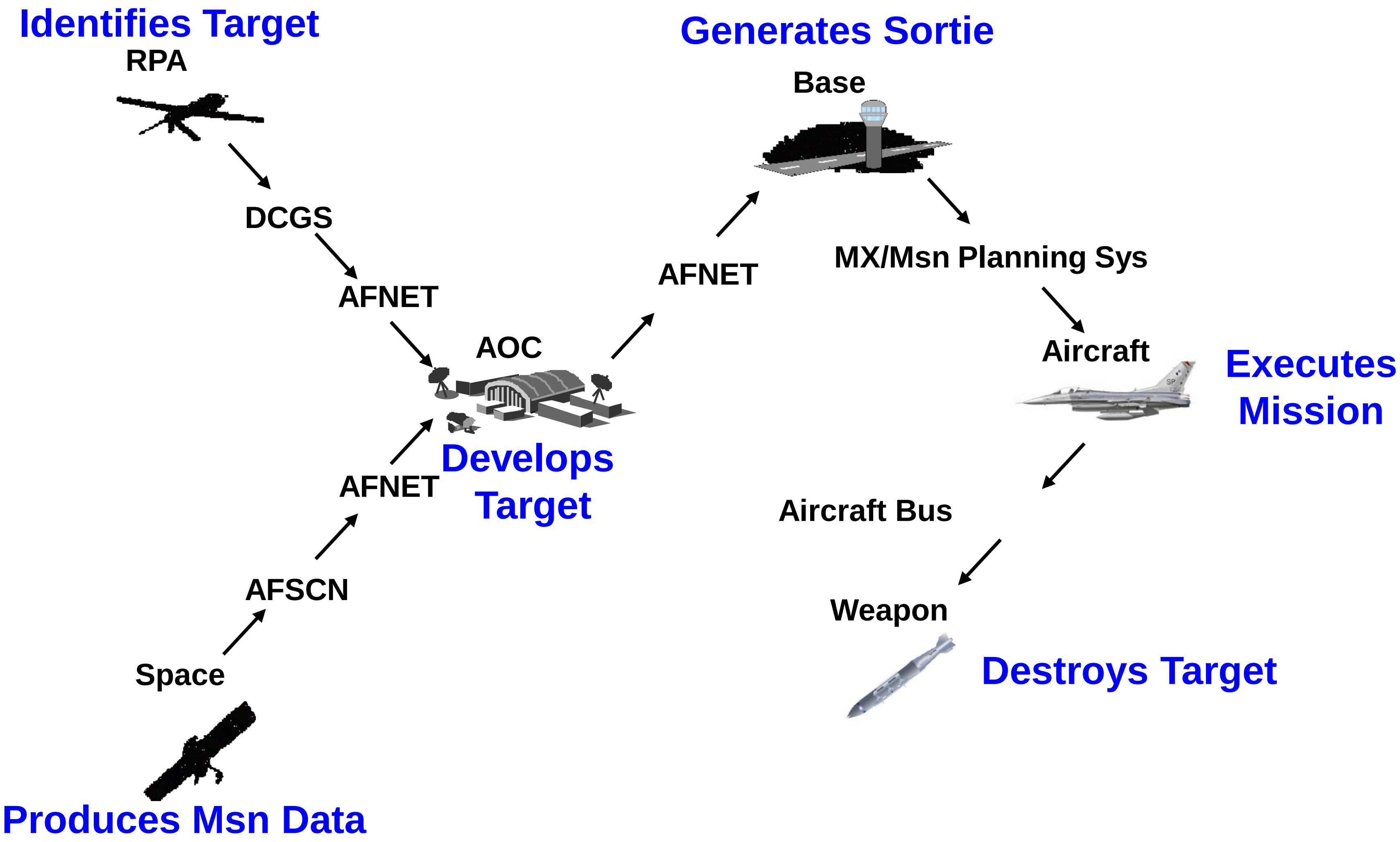
Risk Management - A Temporal perspective



- Manage risks through system engineering and requirements throughout Lifecycle
- Bake security in and establish an initial security posture and burn tech. risk down
- Validate security is “good enough to operate” – issue ATO
- Accept that Systems operate in contested environments in ways not indented
- Over time systems are not as secure due to obsolesce/patching/resources/etc.

Risk view is different at different points in time

Cyber Resiliency Government Reference Architecture
Simple AF Mission Example



Identifies Target

RPA

DCGS

AFNET

AOC

Produces Msn Data

Space

AFSCN

AFNET

Develops Target

AFNET

Generates Sortie

Base

MX/Msn Planning Sys

Aircraft

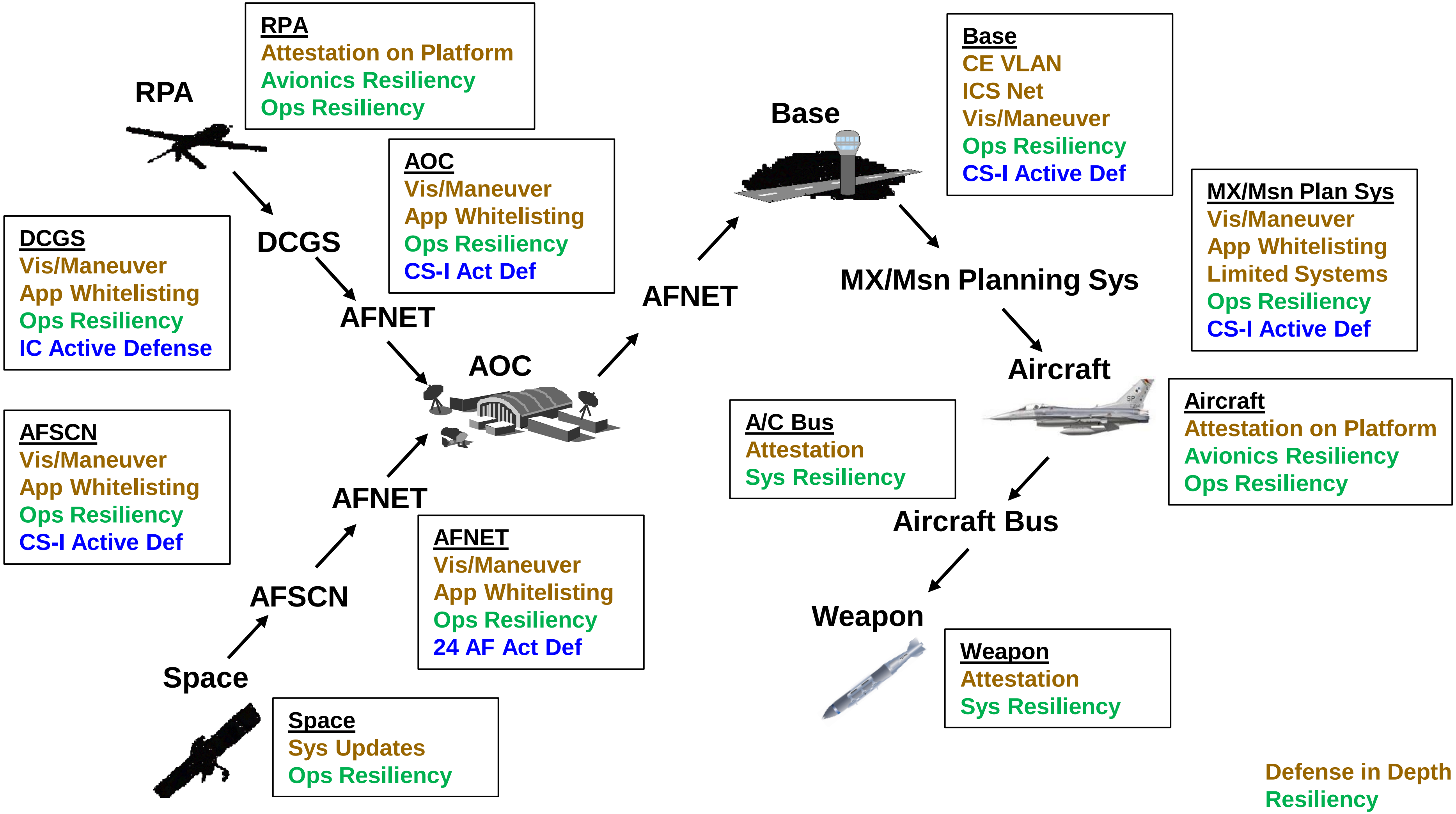
Executes Mission

Aircraft Bus

Weapon

Destroys Target

Cyber Resiliency Government Reference Architecture
Five Year Vision (aka "To Be")



RPA
Attestation on Platform
Avionics Resiliency
Ops Resiliency

AOC
Vis/Maneuver
App Whitelisting
Ops Resiliency
CS-I Act Def

Base
CE VLAN
ICS Net
Vis/Maneuver
Ops Resiliency
CS-I Active Def

MX/Msn Plan Sys
Vis/Maneuver
App Whitelisting
Limited Systems
Ops Resiliency
CS-I Active Def

DCGS
Vis/Maneuver
App Whitelisting
Ops Resiliency
IC Active Defense

AFSCN
Vis/Maneuver
App Whitelisting
Ops Resiliency
CS-I Active Def

A/C Bus
Attestation
Sys Resiliency

Aircraft
Attestation on Platform
Avionics Resiliency
Ops Resiliency

AFNET
Vis/Maneuver
App Whitelisting
Ops Resiliency
24 AF Act Def

Weapon
Attestation
Sys Resiliency

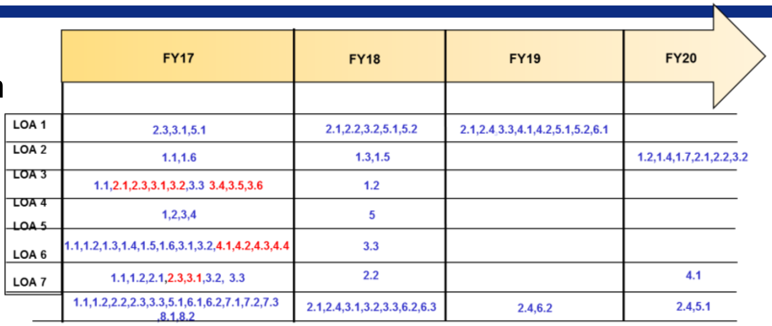
Space
Sys Updates
Ops Resiliency

Defense in Depth
Resiliency
Active Defense

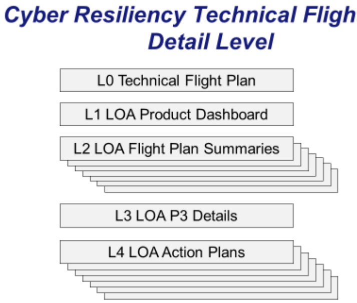
DISTRIBUTION A. Approved for public release: distribution unlimited.

Cyber Resiliency Technical Flight Plan (CR-TFP)

Level 0
Technical Flight Plan
Strategic Objectives



	FY17	FY18	FY19	FY20
LOA 1	2.3,3.1,5.1	2.1,2.2,3.2,5.1,5.2	2.1,2.4 3.3,4.1,4.2,5.1,5.2,6.1	
LOA 2	1.1,1.6	1.3,1.5		1.2,1.4,1.7,2.1,2.2,3.2
LOA 3	1.1,2.1,2.3,3.1,3.2,3.3 3.4,3.5,3.6	1.2		
LOA 4 LOA 5	1,2,3,4	5		
LOA 6	1.1,1.2,1.3,1.4,1.5,1.6,3.1,3.2,4.1,4.2,4.3,4.4	3.3		
LOA 7	1.1,1.2,2.1,2.3,3.1,3.2, 3.3	2.2		4.1
	1.1,1.2,2.2,2.3,3.3,5.1,6.1,6.2,7.1,7.2,7.3 ,8.1,8.2	2.1,2.4,3.1,3.2,3.3,6.2,6.3	2.4,6.2	2.4,5.1



Cyber Resiliency Technical Flight Plan Detail Level

L0 Technical Flight Plan

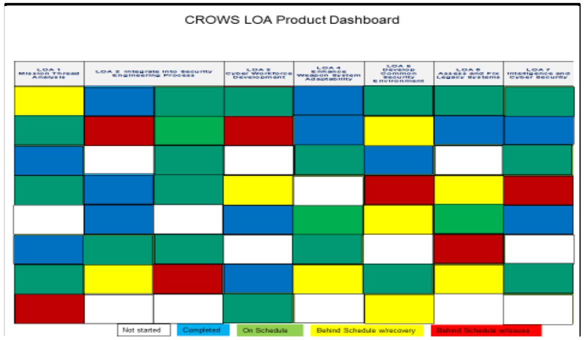
L1 LOA Product Dashboard

L2 LOA Flight Plan Summaries

L3 LOA P3 Details

L4 LOA Action Plans

Level 1
Yearly High Level
Product Dashboard

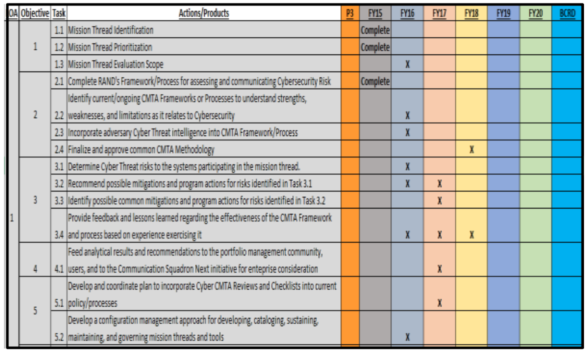


CROWS LOA Product Dashboard

LOA 1 Mission Thread Analysis	LOA 2 Integrate into Security Engineering Process		LOA 3 Cyber Workforce Development	LOA 4 Enhance Weapon System Adaptability	LOA 5 Develop Common Security Environment	LOA 6 Assess and Fix Legacy Systems	LOA 7 Intelligence and Cyber Security
🟨	🟦	🟩	🟩	🟦	🟩	🟩	🟩
🟩	🟥	🟩	🟥	🟦	🟨	🟦	🟦
🟦	⬜	🟩	⬜	🟩	🟦	⬜	🟩
🟩	🟦	🟩	🟨	⬜	🟥	🟨	🟥
⬜	🟦	⬜	🟦	🟩	🟨	🟩	🟦
🟦	🟩	🟩	⬜	🟩	⬜	🟥	⬜
🟩	🟨	🟥	🟦	🟨	🟩	🟨	🟩
🟥	⬜	⬜	🟩	⬜	🟨	⬜	⬜

⬜ Not started 🟦 Completed 🟩 On Schedule 🟨 Behind Schedule w/recovery 🟥 Behind Schedule w/issues

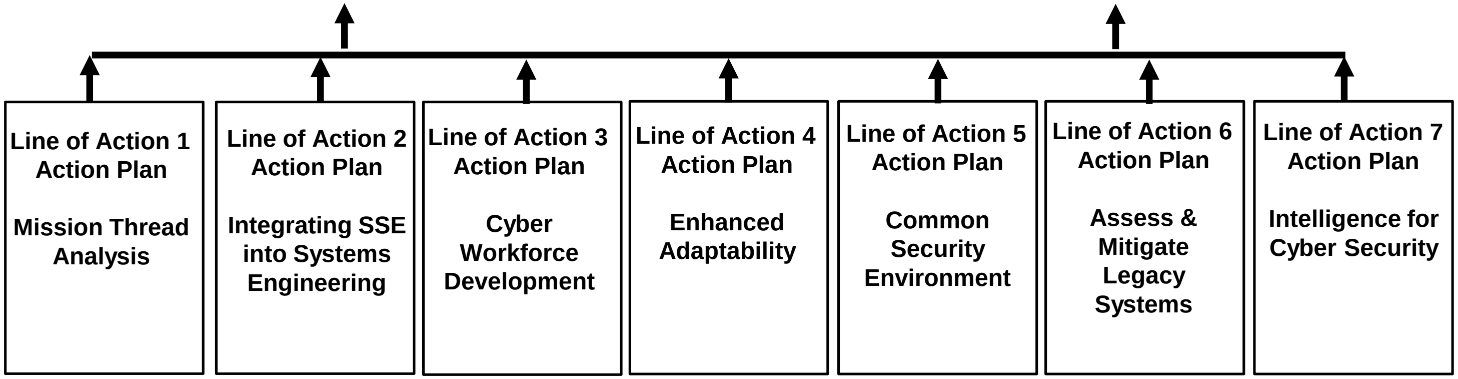
↔



OA	Objective	Task	Actions/Products	P3	FY15	FY16	FY17	FY18	FY19	FY20	BCRD
1	1	1.1	Mission Thread Identification		Complete						
		1.2	Mission Thread Prioritization		Complete						
		1.3	Mission Thread Evaluation Scope			X					
	2	2.1	Complete RAND's Framework/Process for assessing and communicating Cybersecurity Risk		Complete						
		2.2	Identify current/ongoing CMTA Frameworks or Processes to understand strengths, weaknesses, and limitations as it relates to Cybersecurity			X					
		2.3	Incorporate adversary Cyber Threat intelligence into CMTA Framework/Process			X					
		2.4	Finalize and approve common CMTA Methodology					X			
	3	3.1	Determine Cyber Threat risks to the systems participating in the mission thread.			X					
		3.2	Recommend possible mitigations and program actions for risks identified in Task 3.1			X	X				
		3.3	Identify possible common mitigations and program actions for risks identified in Task 3.2				X				
		3.4	Provide feedback and lessons learned regarding the effectiveness of the CMTA Framework and process based on experience exercising it			X	X	X			
	4	4.1	Feed analytical results and recommendations to the portfolio management community, users, and to the Communication Squadron Next initiative for enteprise consideration				X				
	5	5.1	Develop and coordinate plan to incorporate Cyber CMTA Reviews and Checklists into current policy/processes				X				
		5.2	Develop a configuration management approach for developing, cataloging, sustaining, maintaining, and governing mission threads and tools			X					

Level 2 & 3
P3 - People,
Process,
Products

Level 4
Multi Year
Action Plans



Line of Action 1 Action Plan

Mission Thread Analysis

Line of Action 2 Action Plan

Integrating SSE into Systems Engineering

Line of Action 3 Action Plan

Cyber Workforce Development

Line of Action 4 Action Plan

Enhanced Adaptability

Line of Action 5 Action Plan

Common Security Environment

Line of Action 6 Action Plan

Assess & Mitigate Legacy Systems

Line of Action 7 Action Plan

Intelligence for Cyber Security

Weapon System Cyber Reporting

Weapon System Cyber Security

2 Feb 2017

SAF/AQ SAE
&
HAF A6 CIO

Weapon System Cyber Resiliency

11 Apr 2017

SAF/AQ SAE

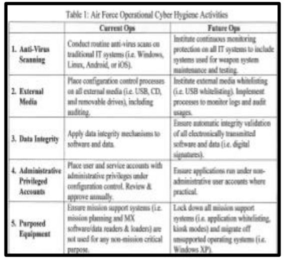


Table 1: Air Force Operational Cyber Hygiene Activities

	Current Ops	Future Ops
1. Anti-Virus Scanning	Conduct routine anti-virus scans on traditional IT systems (i.e. Windows, Linux, Android, or iOS).	Institute continuous monitoring protection on all IT systems to include systems used for weapon system maintenance and testing.
2. External Media	Place configuration control processes on all external media (i.e. USB, CD, and removable drives), including auditing.	Institute external media whitelisting (i.e. USB whitelisting). Implement processes to monitor logs and audit usages.
3. Data Integrity	Apply data integrity mechanisms to software and data.	Ensure automatic integrity validation of all electronically transmitted software and data (i.e. digital signatures).
4. Administrative Privileged Accounts	Place user and service accounts with administrative privileges under configuration control. Review & approve annually.	Ensure applications run under non-administrative user accounts where practical.
5. Purposed Equipment	Ensure mission support systems (i.e. mission planning and MX software/data readers & loaders) are not used for any non-mission critical purpose.	Lock down all mission support systems (i.e. application whitelisting, kiosk modes) and migrate off unsupported operating systems (i.e. Windows XP).

Reporting Requirements

Reporting Requirements

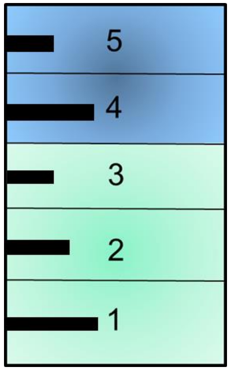
PEO Monthly Status Email

PEO Status Reporting

<In Development>

Prototyping with PEO DOE Involvement

Cyber Resiliency Assurance Metric (CRAM)



Allows for multiple views and perspectives
- Mission Level
- System Level
- Component Level

Weapon System Integrated Reporting and Metric

DISTRIBUTION A. Approved for public release: distribution unlimited.

Cyber Resiliency Assurance Metric (CRAM)

- Integrated Metric – Focus is on Cyber Assurance in Mission context
  - Incorporates all available risk assessments - Evidentiary Analysis & Data based
  - Linked to Cyber Hygiene Reporting requirements and Authorizations (e.g. ATO, ATC)
- Based on Risk analysis and Confidence factors – Risk Management vs Compliance
- Provides for Situational Awareness of Cyber Assurance over Time
  - WS CR Dashboard in development

Cyber Hygiene

- Builds in Security
- Assumes a set of known "Knowns"

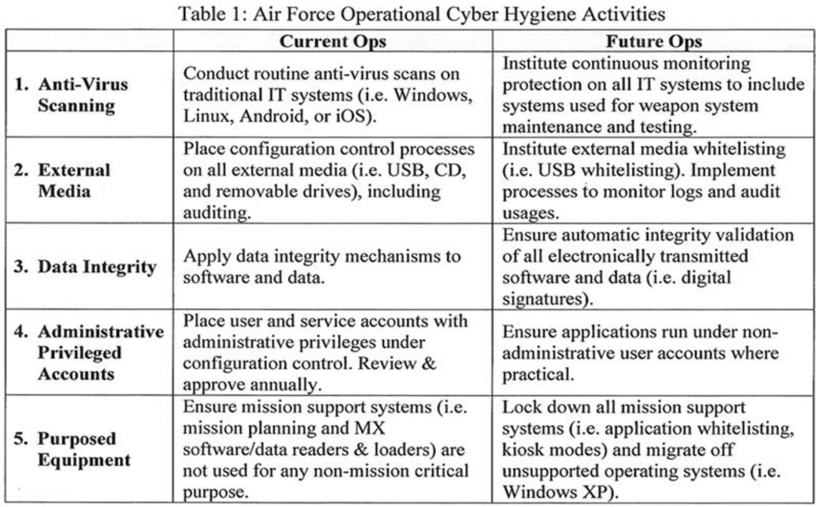
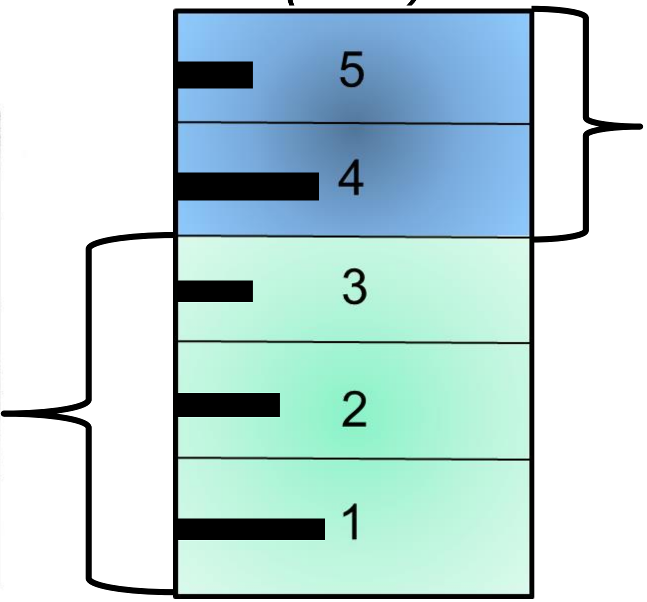


Table 1: Air Force Operational Cyber Hygiene Activities

	Current Ops	Future Ops
1. Anti-Virus Scanning	Conduct routine anti-virus scans on traditional IT systems (i.e. Windows, Linux, Android, or iOS).	Institute continuous monitoring protection on all IT systems to include systems used for weapon system maintenance and testing.
2. External Media	Place configuration control processes on all external media (i.e. USB, CD, and removable drives), including auditing.	Institute external media whitelisting (i.e. USB whitelisting). Implement processes to monitor logs and audit usages.
3. Data Integrity	Apply data integrity mechanisms to software and data.	Ensure automatic integrity validation of all electronically transmitted software and data (i.e. digital signatures).
4. Administrative Privileged Accounts	Place user and service accounts with administrative privileges under configuration control. Review & approve annually.	Ensure applications run under non-administrative user accounts where practical.
5. Purposed Equipment	Ensure mission support systems (i.e. mission planning and MX software/data readers & loaders) are not used for any non-mission critical purpose.	Lock down all mission support systems (i.e. application whitelisting, kiosk modes) and migrate off unsupported operating systems (i.e. Windows XP).

Cyber Resiliency Assurance Metric (CRAM)



Cyber Resiliency

- Buys down Risk
- Assumes Unknowns Happen
- Enables ability to Play Hurt
- Operational Contingency

Table 1: Air Force Operational Cyber Hygiene Activities
In Development

DISTRIBUTION A. Approved for public release: distribution unlimited.

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 the Gaps

- Solutions and S&T needs follow Gaps

Cyber S&T Needs

- Automated Continuous Monitoring
- Persistent monitoring at bus level
- Supply Chain Risk Management scalability
- Awareness Education & Training
- Autonomy at the application level
- Automated vulnerability enumeration
- Use of autonomy in detection and response
- Measurement and attestation of system-of-system stack

- Software Assurance
- Automated Software Analysis & Repair
- Secure Operating System
- Autonomous Analysis & Detection
- Real Time Human in the loop HW simulations
- Threat detection & continuous monitoring
  - SWaP-C constrained environment

Initial Set Defined 2017

DISTRIBUTION A. Approved for public release: distribution unlimited.

Summary

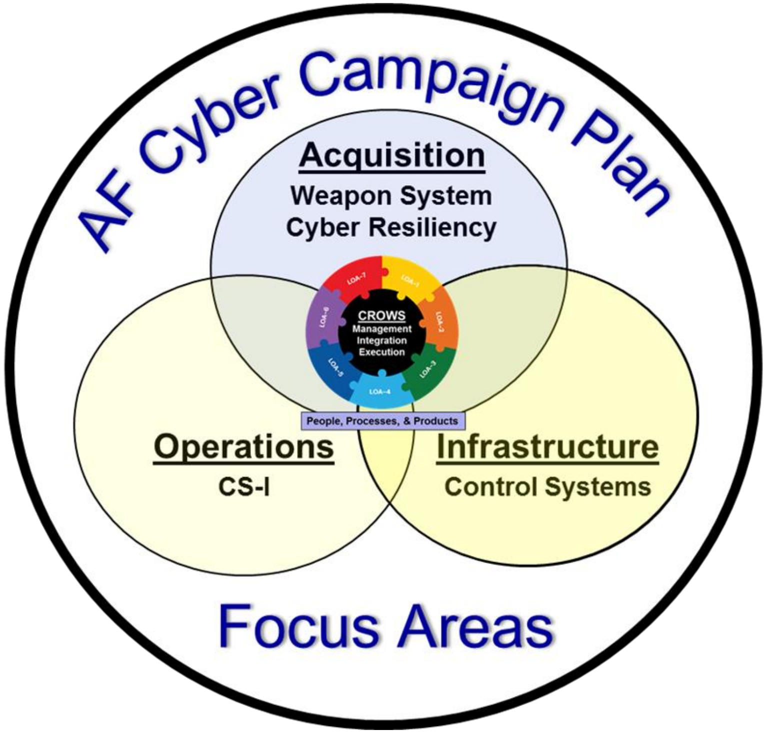
- **Challenge: Cyber resiliency impacts all AF missions -- new threats require new approaches to improve mission assurance**

- **Cyber Campaign Plan addresses this challenge in an integrated, holistic manner to enable AF to address cyber resiliency by:**
  - Making cyber security/resiliency a requirement in all weapon system acquisition programs
  - Assisting program managers to ensure cyber security/resiliency is fully considered and implemented in all aspects of acquisition programs across the lifecycle
  - Ensuring cyber security and resiliency becomes engrained in the AF acquisition culture

- **We are already seeing results due to awareness, training, TT&Ps, and identifying key enterprise vulnerabilities/mitigation solutions**

Cyber Resiliency is as important as the next weapon system

Authorizing Official (AO) Perspective



Mr. Daniel C. Holtzman, HQE
Command & Control (C2)
And
Rapid Cyber Acquisition (RCA)
Authorizing Official
daniel.holtzman.1@us.af.mil

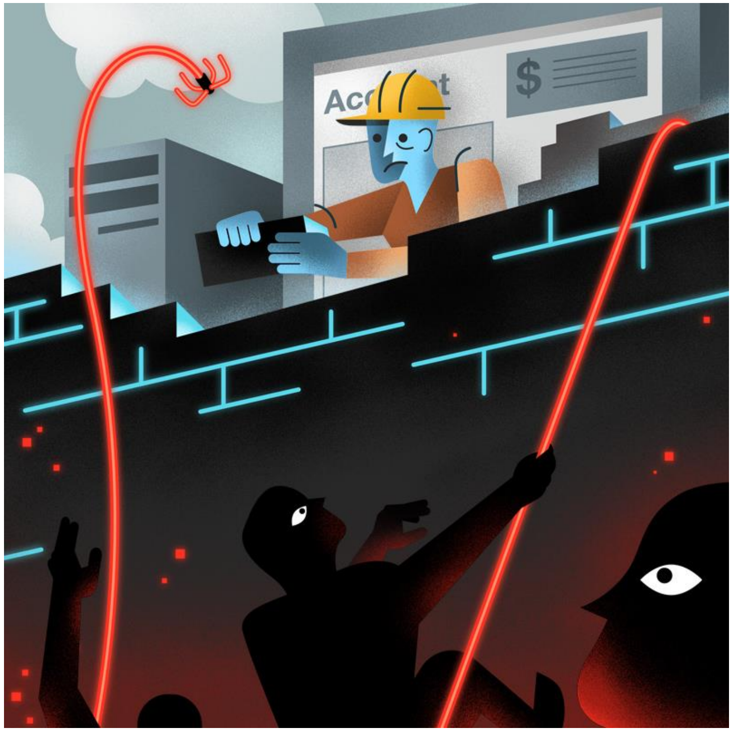
25 October 2017

Cyber Resiliency – A War Winning Capability

Weapon System Security & Resiliency

- Security & Resiliency are symbiotic
  - Each have objectives but can't achieve success without the other
  - Neither are sufficient alone to provide mission assurance
- Resiliency is the ability to play hurt

Can you take a punch?



DISTRIBUTION A. Approved for public release: distribution unlimited.

USB port for Aircraft

Everything that connects to an Aircraft acts like an USB Port

- **All Access points need to be considered**
- **Need to ensure chain of trust and confidence**
- **There are no "Air Gaps" in the 21 Century**

DISTRIBUTION A. Approved for public release: distribution unlimited.

Bottom Line Up Front
C2 & RCA Authorizing Official Objectives

- Objectives
  - Make decisions faster, Make transparent decisions, Foster reciprocity
  - Facilitate risk management, from acquisition through operations & sustainment
  - Enable Program Managers, to advance Cyber Security & Cyber Resiliency

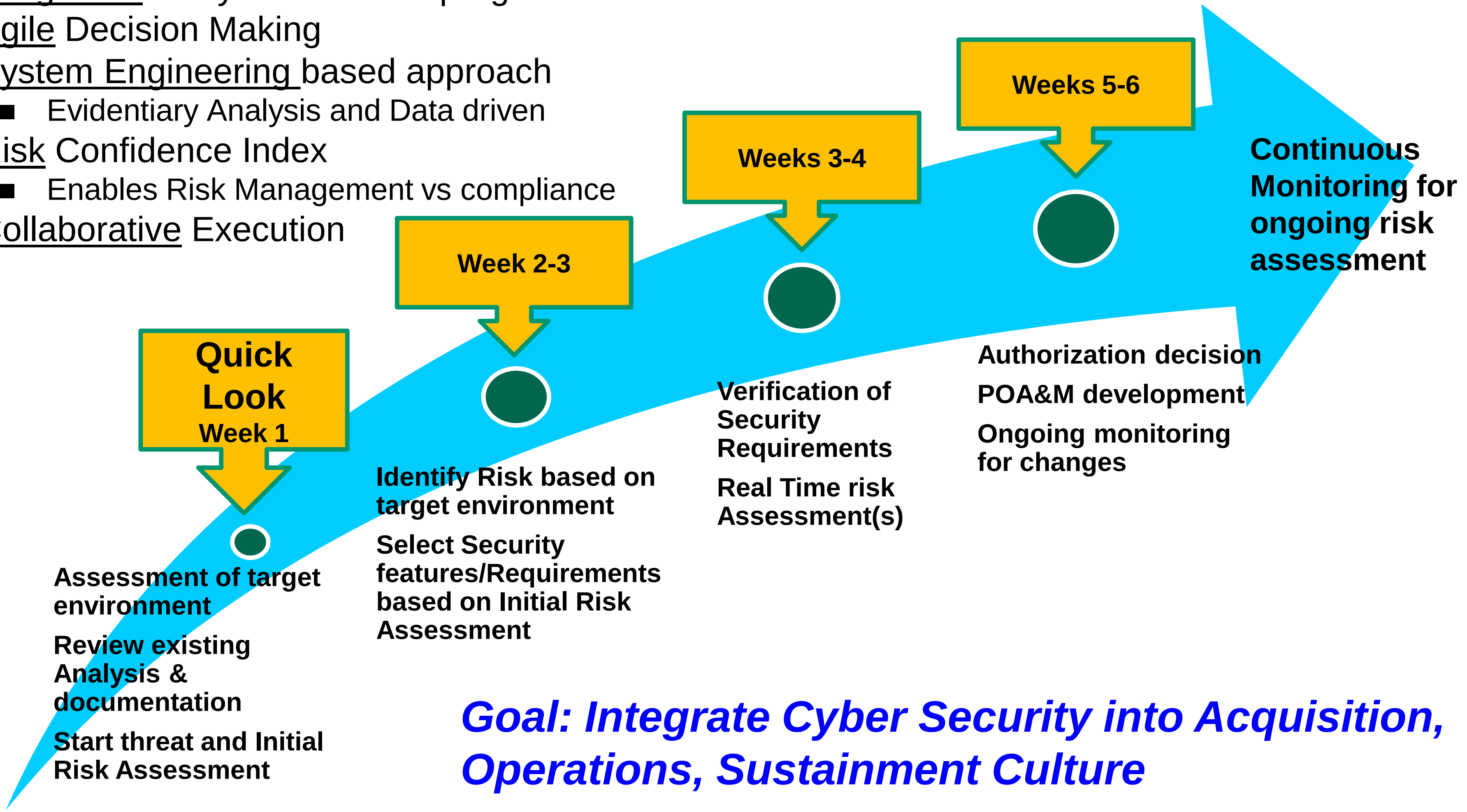
- Enablers
  - Set clear requirements and increase agility in decision making process – Decision Briefing
  - Programs bring standard System Engineering - Evidentiary Analysis & Data
  - Provide programs with single AO POC for each Weapon System – Streamline expectations
  - Focus Cybersecurity on risks that matter – Risk Management vs Compliance perspective

- Collaborative Execution
  - Cyber Risk Assessors (CRA), formerly called SCA, are focused on assessing risks
  - Authorizing Official is focused on informing enterprise decision makers on Risks
  - Partnerships with PEO's, DOEs, PMs, Users, and Sustainers enables a holistic approach
  - Focus is on risk identification and management – Programs & AOs
  - Enable Cyber Resiliency – Foster Mission Assurance

Increase Decision Making Ability & Focus on Risk Management

C2 & RCA implementation approach

- Integration of Cyber Risk into program Risk
- Agile Decision Making
- System Engineering based approach
  - Evidentiary Analysis and Data driven
- Risk Confidence Index
  - Enables Risk Management vs compliance
- Collaborative Execution



Quick Look
Week 1

Assessment of target environment

Review existing Analysis & documentation

Start threat and Initial Risk Assessment

Week 2-3

Identify Risk based on target environment

Select Security features/Requirements based on Initial Risk Assessment

Weeks 3-4

Verification of Security Requirements

Real Time risk Assessment(s)

Weeks 5-6

Authorization decision

POA&M development

Ongoing monitoring for changes

Continuous Monitoring for ongoing risk assessment

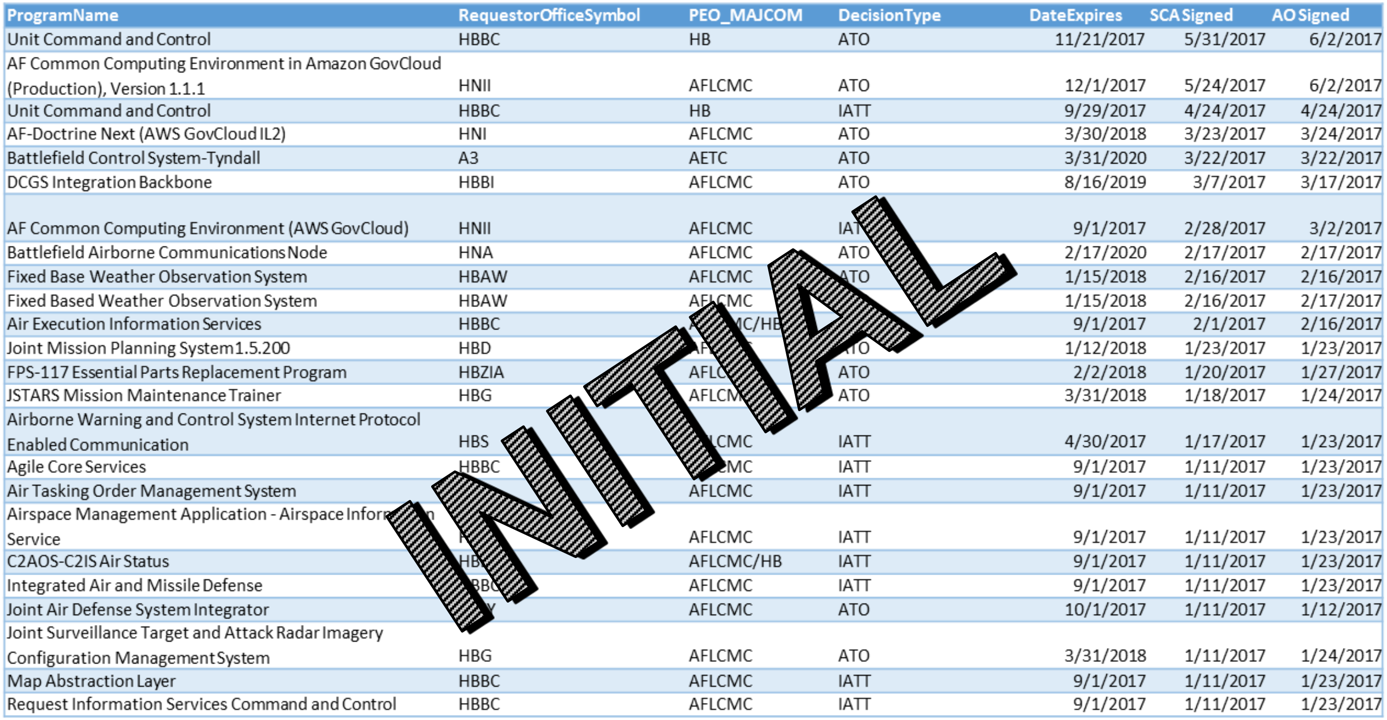
Goal: Integrate Cyber Security into Acquisition, Operations, Sustainment Culture

DISTRIBUTION A. Approved for public release: distribution unlimited.

C2 & RCA MAR Dashboard

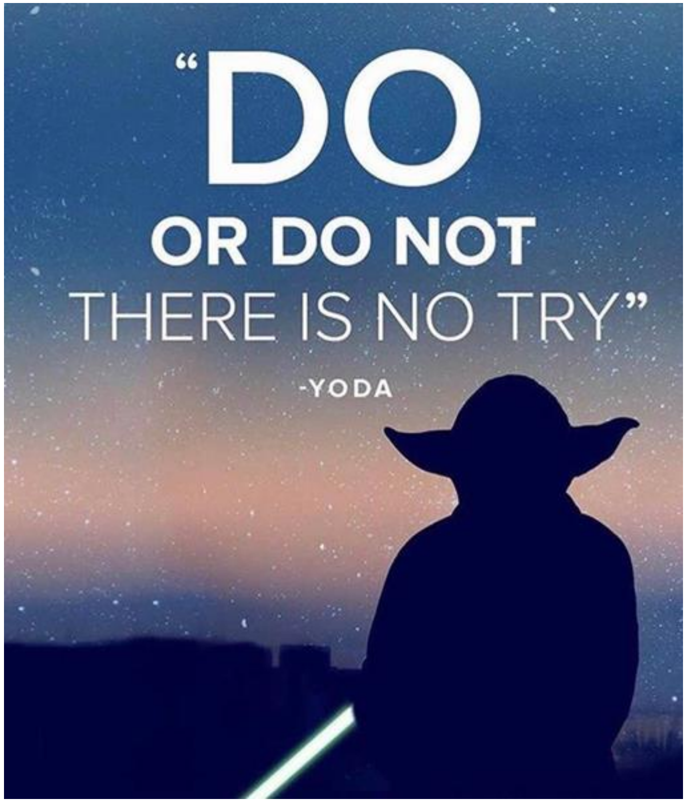
(In Development)

- **BLUF: Execute C2 & RCA AO responsibility as any other – Cost, Schedule, Performance**
- **Quarterly PMR with CIO – Asses C2 & RCA AO enterprise, Big Rocks, Issues/Opportunities**
- **Monthly reviews with Users (e.g. PEOs, MAJCOMS, Other Stakeholders)**
- **90 Day look ahead – Proactive vs Reactive**



ProgramName	RequestorOfficeSymbol	PEO_MAJCOM	DecisionType	DateExpires	SCA Signed	AO Signed
Unit Command and Control	HBBC	HB	ATO	11/21/2017	5/31/2017	6/2/2017
AF Common Computing Environment in Amazon GovCloud (Production), Version 1.1.1	HNII	AFLCMC	ATO	12/1/2017	5/24/2017	6/2/2017
Unit Command and Control	HBBC	HB	IATT	9/29/2017	4/24/2017	4/24/2017
AF-Doctrine Next (AWS GovCloud IL2)	HNI	AFLCMC	ATO	3/30/2018	3/23/2017	3/24/2017
Battlefield Control System-Tyndall	A3	AETC	ATO	3/31/2020	3/22/2017	3/22/2017
DCGS Integration Backbone	HBBI	AFLCMC	ATO	8/16/2019	3/7/2017	3/17/2017
AF Common Computing Environment (AWS GovCloud)	HNII	AFLCMC	IATT	9/1/2017	2/28/2017	3/2/2017
Battlefield Airborne Communications Node	HNA	AFLCMC	ATO	2/17/2020	2/17/2017	2/17/2017
Fixed Base Weather Observation System	HBAW	AFLCMC	ATO	1/15/2018	2/16/2017	2/16/2017
Fixed Based Weather Observation System	HBAW	AFLCMC	[illegible]	1/15/2018	2/16/2017	2/17/2017
Air Execution Information Services	HBBC	AFLCMC/HB	[illegible]	9/1/2017	2/1/2017	2/16/2017
Joint Mission Planning System 1.5.200	HBD	AFLCMC	ATO	1/12/2018	1/23/2017	1/23/2017
FPS-117 Essential Parts Replacement Program	HBZIA	AFLCMC	ATO	2/2/2018	1/20/2017	1/27/2017
JSTARS Mission Maintenance Trainer	HBG	AFLCMC	ATO	3/31/2018	1/18/2017	1/24/2017
Airborne Warning and Control System Internet Protocol Enabled Communication	HBS	AFLCMC	IATT	4/30/2017	1/17/2017	1/23/2017
Agile Core Services	HBBC	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
Air Tasking Order Management System	[illegible]	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
Airspace Management Application - Airspace Information Service	[illegible]	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
C2AOS-C2IS Air Status	HB[illegible]	AFLCMC/HB	IATT	9/1/2017	1/11/2017	1/23/2017
Integrated Air and Missile Defense	HBBC	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
Joint Air Defense System Integrator	[illegible]	AFLCMC	ATO	10/1/2017	1/11/2017	1/12/2017
Joint Surveillance Target and Attack Radar Imagery Configuration Management System	HBG	AFLCMC	ATO	3/31/2018	1/11/2017	1/24/2017
Map Abstraction Layer	HBBC	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017
Request Information Services Command and Control	HBBC	AFLCMC	IATT	9/1/2017	1/11/2017	1/23/2017

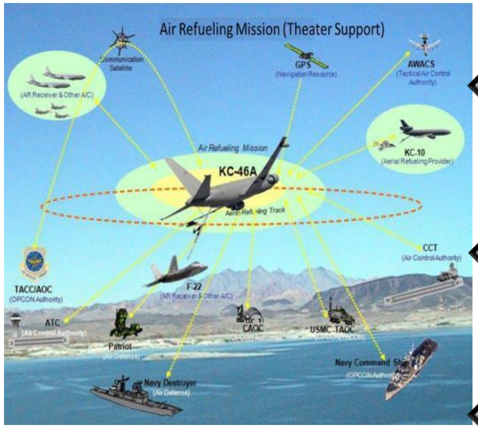
Questions & Discussion



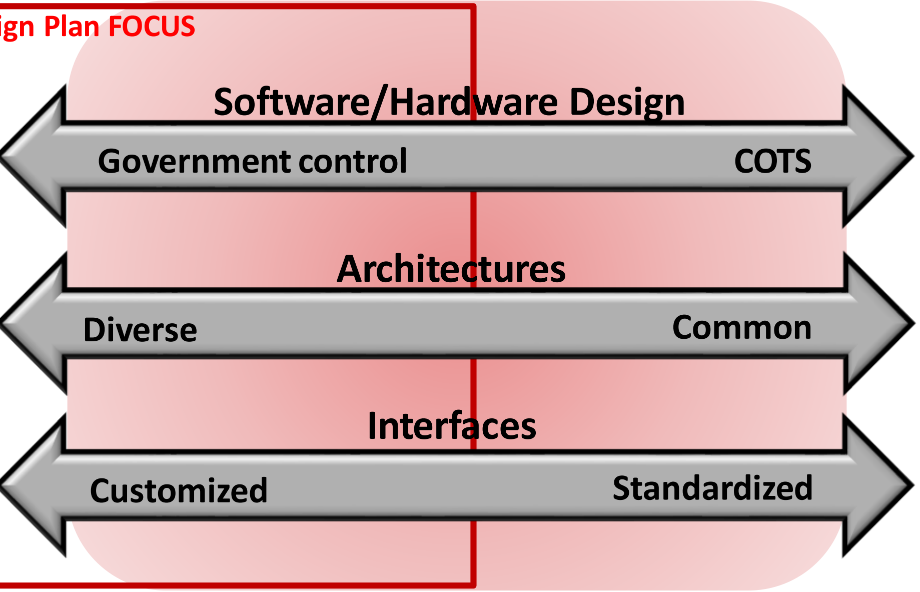
Weapon System Cyber Resiliency Critical to Mission Assurance

- We define the Cyber Resiliency of Military systems to be:
  - The ability of weapon systems ***to maintain mission effective capability*** under adversary offensive cyber operations
  - To ***manage the risk*** of adversary cyber intelligence exploitation
- Weapon systems differ from general administrative and business IT systems in ways that matter for implementing Cyber Resiliency

Cyber Campaign Plan FOCUS



Weapon Systems


Software/Hardware Design

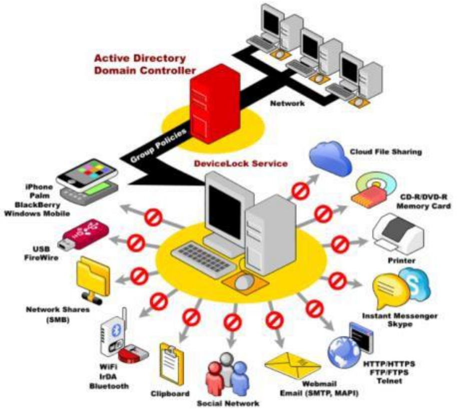
Government control — COTS

Architectures

Diverse — Common

Interfaces

Customized — Standardized



IT Systems

DISTRIBUTION A. Approved for public release: distribution unlimited.

Cyber Resiliency

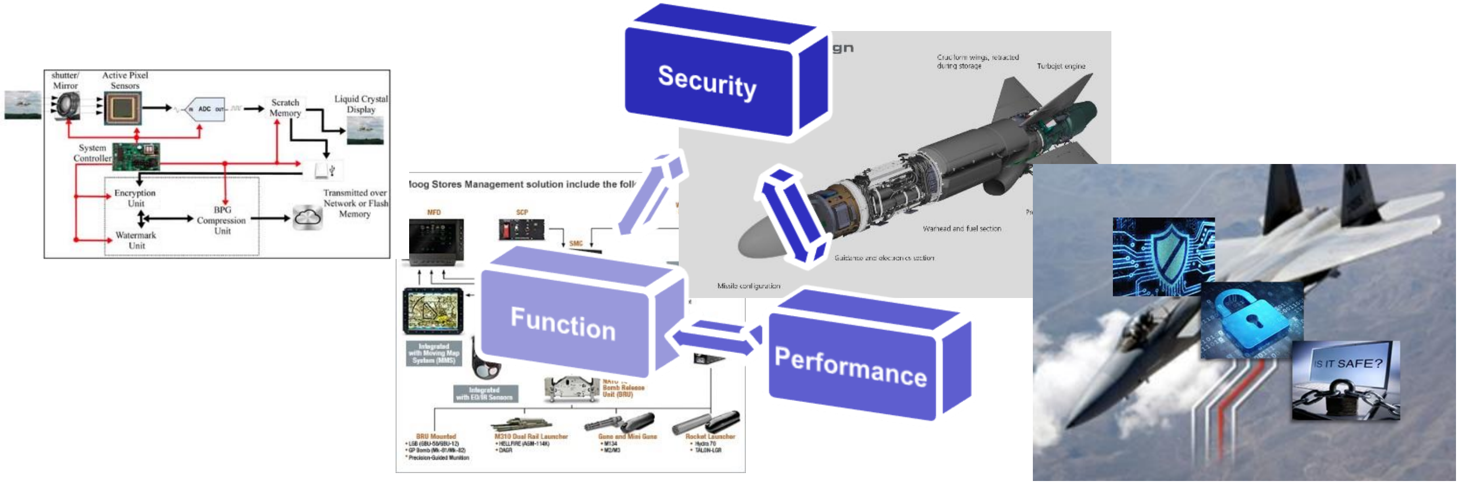
- **Definition (What does it mean?)**
  - **Cyber Resiliency = *<u>The ability to provide required capability despite adversity</u>*, that impacts the Cyber aspects of the Systems**
  - **"Cyber Aspects" = Software, Firmware and data in electronic form and the associated hardware**
- **Cyber Resilience, 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".**

Design, Secure, Assess
Build, Secure, Assess

Bolted-on

COST

Baked-in



Best Countermeasure

- Cyber security will improve as system design improves.
- Essentially, if built properly, security will be an **inherent property**

- Best **countermeasures:**
  - Better design (Bake it in)
  - Proper use of technology (Plan for Resiliency)
- **Enable** systems:
  - To be resilient to rapid change

Change
&
Diversity

DISTRIBUTION A. Approved for public release: distribution unlimited.

Weapons System Cybersecurity Guidance
Operational Cyber Hygiene Activities

	Current Operations	Future Operations
Anti-Virus Scanning	Conduct routine anti-virus scans on traditional IT systems (i.e. Windows, Linux, Android, or iOS).	Institute continuous monitoring protection on all IT systems to include systems used for weapon system maintenance and testing.
External media	Place configuration control processes on all external media (i.e. USB, CD, and removable drives), including auditing.	Institute external media whitelisting (i.e. USB whitelisting). Implement processes to monitor logs and audit usages.
Data integrity	Apply data integrity mechanisms to software and data.	Ensure automatic integrity validation of all electronically transmitted software and data. (I.e. digital signatures).
Administrative privileged accounts	Place user and service accounts with administrative privileges under configuration control. Review & approve annually.	Ensure applications run under non-administrative user accounts where practical.
Purposed equipment	Ensure mission support systems (i.e. mission planning and MX software/data readers & loaders) are not used for any non-mission critical purpose.	Lock down all mission support systems (i.e. application whitelisting, kiosk modes) and migrate off unsupported operating systems (i.e. Windows XP).

Public Release Approval

Case Number: 2017-0421 (original case number(s): AFIMSC-2017-0039; 66ABG-2017-0114) The material was assigned a clearance of CLEARED on 23 Oct 2017. If local policy permits, the Review Manager for your case, Deborah Powers, deborah.powers@us.af.mil, will prepare a hard copy of the review and will forward it via mail or prepare it for pick up.

DISTRIBUTION A. Approved for public release: distribution unlimited.