Headquarters U.S. Air Force

Integrity - Service - Excellence

Cyber Resiliency Office for Weapon Systems (CROWS)

Mr. Danny Holtzman, HQE
Cyber Technical Director
daniel.holtzman.1@us.af.mil

7 March 2017

DISTRIBUTION A. Approved for public release: distribution unlimited.

CROWS Stand-up

- FY14 NDAA called for Services to develop a plan to increase cyber resiliency of weapon systems

- Jan 15: SECAF, AFMC & AFSPC teamed to establish Cyber Resiliency Steering Group (CRSG) to develop AF Cyber Campaign Plan (CCP)

- CRSG identified 7 Lines of Action (LOAs) plus coordination with:
  - Comm Squadron Next (now called Cyber Squadron Initiatives)
  - Test and Evaluation (infrastructure & coordination)
  - Industrial Control Systems/SCADA cyber protection measures

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

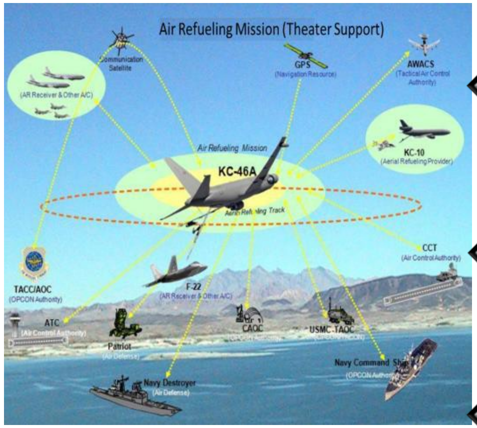
- Jun 16: AFMC/CC approved standup of dedicated team to manage Cyber Campaign Plan → CROWS

DISTRIBUTION A. Approved for public release: distribution unlimited.

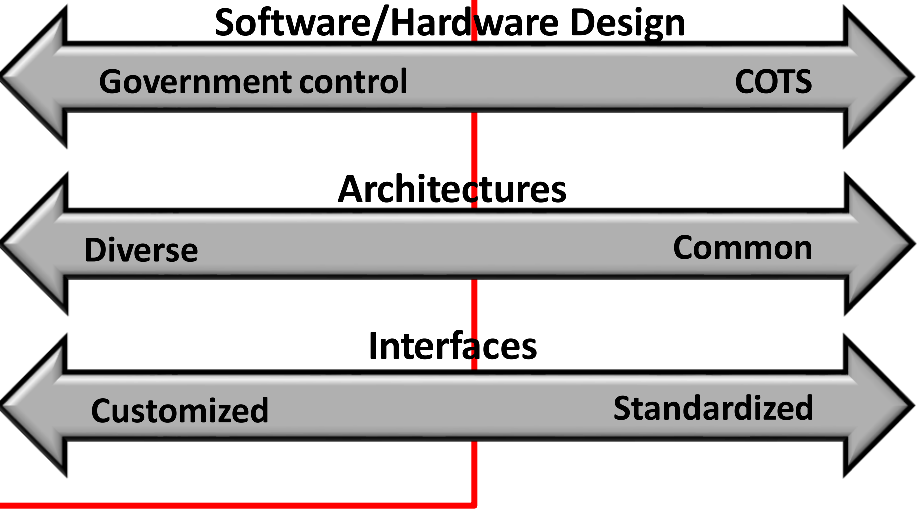
Weapon System Cyber Resiliency Critical to Mission Assurance

- We define the <u>Cyber Resiliency of Military systems</u> 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

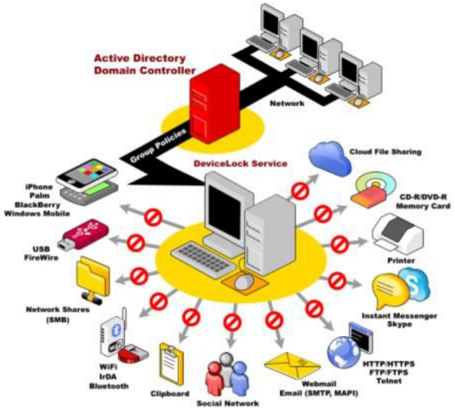
Government control ⟷ COTS

Architectures

Diverse ⟷ Common

Interfaces

Customized ⟷ Standardized

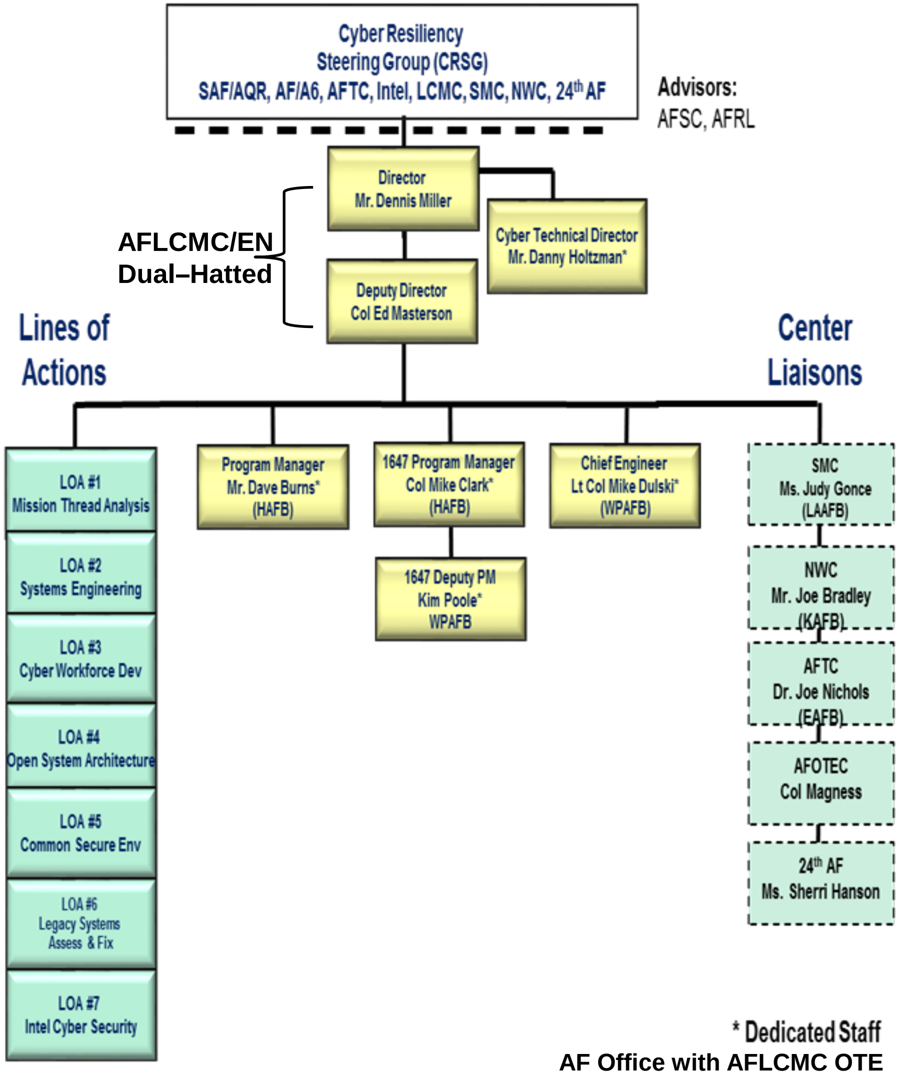


IT Systems

DISTRIBUTION A. Approved for public release: distribution unlimited.

CROWS Organization

- Vision
  - Cyber resiliency ingrained in AF culture
- Mission
  - Increase cyber resiliency of Air Force weapon systems to maintain mission effective capability under adverse conditions
- Status
  - IOC Declared: 21 Dec 2016
  - FOC Projected: 1 Oct 2017
  - Integrate & Execute Campaign Plan (7 LOAs)
  - Executing NDAA 1647



Cyber Resiliency Steering Group (CRSG)
SAF/AQR, AF/A6, AFTC, Intel, LCMC, SMC, NWC, 24th AF

Advisors:
AFSC, AFRL

AFLCMC/EN Dual–Hatted

Director
Mr. Dennis Miller

Deputy Director
Col Ed Masterson

Cyber Technical Director
Mr. Danny Holtzman*

Lines of Actions

LOA #1
Mission Thread Analysis

LOA #2
Systems Engineering

LOA #3
Cyber Workforce Dev

LOA #4
Open System Architecture

LOA #5
Common Secure Env

LOA #6
Legacy Systems
Assess & Fix

LOA #7
Intel Cyber Security

Program Manager
Mr. Dave Burns*
(HAFB)

1647 Program Manager
Col Mike Clark*
(HAFB)

1647 Deputy PM
Kim Poole*
WPAFB

Chief Engineer
Lt Col Mike Dulski*
(WPAFB)

Center Liaisons

SMC
Ms. Judy Gonce
(LAAFB)

NWC
Mr. Joe Bradley
(KAFB)

AFTC
Dr. Joe Nichols
(EAFB)

AFOTEC
Col Magness

24th AF
Ms. Sherri Hanson

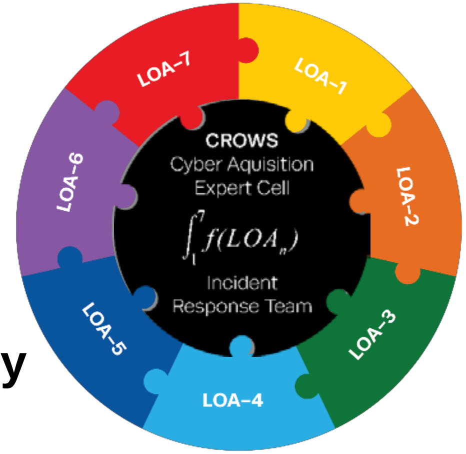
* Dedicated Staff

AF Office with AFLCMC OTE

DISTRIBUTION A. Approved for public release: distribution unlimited.

AF Cyber Campaign Plan: Weapon System Focus

- 7 Lines of Action (LOAs)
  - LOA 1: Perform Cyber Mission Thread Analysis
  - LOA 2: “Bake-In” Cyber Resiliency
  - LOA 3: Recruit, Hire & Train Cyber Workforce
  - LOA 4: Improve Weapon System Agility & Adaptability
  - LOA 5: Develop Common Security Environment
  - LOA 6: Assess & Protect Fielded Fleet
  - LOA 7: Provide Cyber Intel Support



People, Processes, & Products

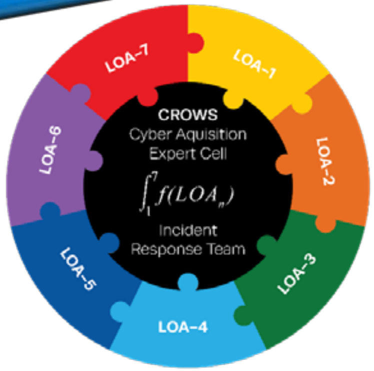
- Cyber Squadron Initiatives
- Test & Evaluation (infrastructure & capability growth)
- Industrial Control Systems/SCADA cyber protection measures

Ensure mission success in a cyber contested environment

Roadmap to Resiliency

Present

Future



Mission Assurance

- Mission Thread Analysis

- Develop assessment methodology framework
- Develop cyber acquisition workforce

System Assurance

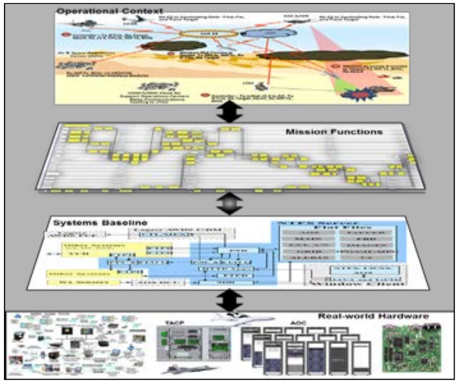
- Assess and Fix

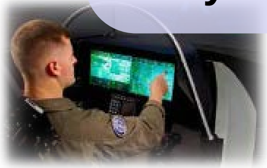
- Assess cyber posture of fielded systems
- Enable weapon system adaptability

Institutionalize

- “Baked” in resiliency

- Institutionalized methodology, tools, T&E infrastructure
- Skilled workforce
- Integrated cyber tools, policy, etc.





Mx and Aircrew Trainers

Off Board Mission Support

DISTRIBUTION A. Approved for public release: distribution unlimited.

On Going Alignment of Efforts

- **AF Technical Reference Architecture**
  - Framework for Cyber Resiliency in Weapon Systems
  - Criteria, Observables, Behaviors, Measures
  - Design, Operate, Sustain securely to improve Mission Assurance
- **Technical Coordination/Reviews –**
  - Alignment to Technical Flight Plan, Staffing/Comment adjudication, Technical recommendations
- **FFRDC/UARC**
  - AF Security Engineering Team (AFSET)
- **PEO / Programs**
  - PEO Directors of Engineering (DOE) Council
- **Service's, OSD, Academia, NIST**
  - Mitigation Handbook and rubric for efficient application
- **Industry**
  - Engagement via NDIA SE/SSE/T&E Committee's
  - **18-20 April NDIA Cyber Resiliency for Weapon Systems Summit (AF/OSD Collaboration)**

DISTRIBUTION A. Approved for public release: distribution unlimited.

See AF News Article (4 Jan 17)

- “AF looks to ensure cyber resiliency in weapons systems through new office”

http://www.af.mil/News/ArticleDisplay/tabid/223/Article/1041426/af-looks-to-ensure-cyber-resiliency-in-weapons-systems-through-new-office.aspx

DISTRIBUTION A. Approved for public release: distribution unlimited.

Summary

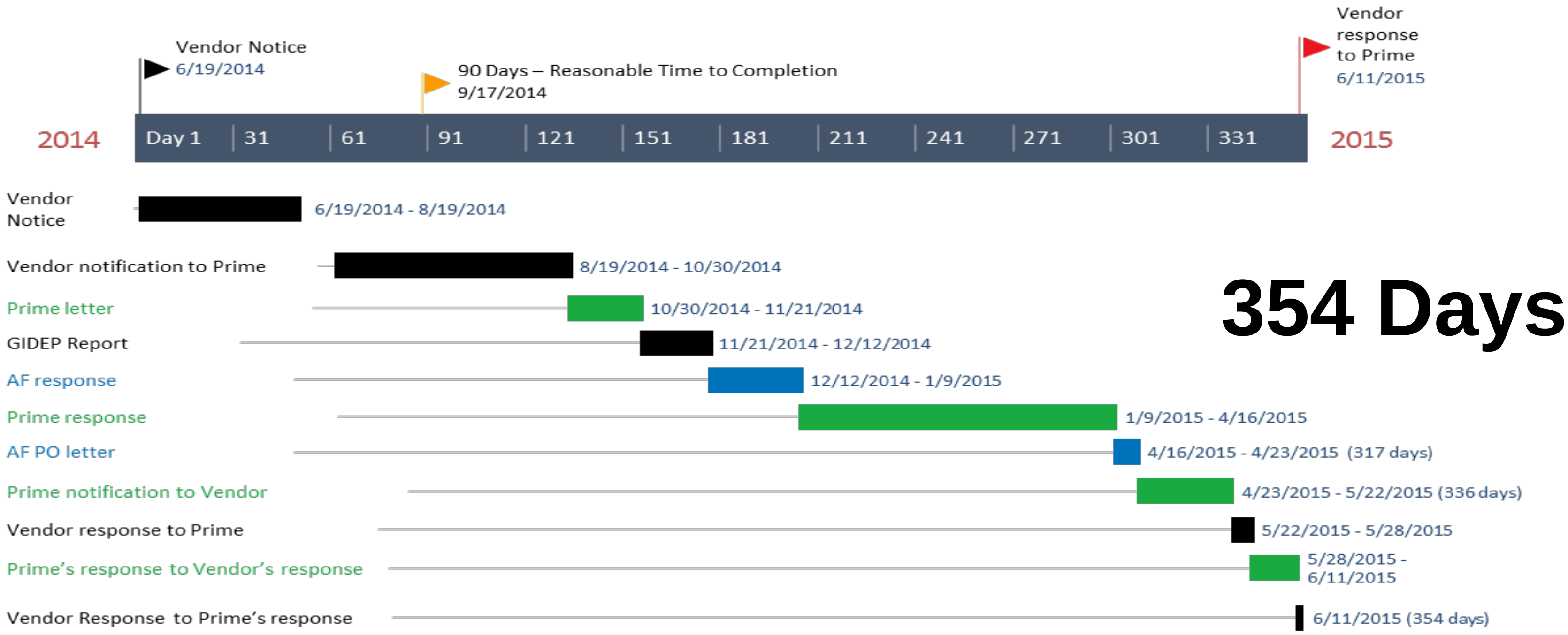
- Cyber resiliency impacts all AF missions
- New threats require new approaches

Cyber Resiliency is as important as the next weapon system

DISTRIBUTION A. Approved for public release: distribution unlimited.

Challenge to the community – Increasing the agility in decision making

- **Example case**: Supply Chain – Counterfeit Part
  - FAR/DFAR clauses on contract, flow down from Government to prime to sub
  - Process took maximum time at every point
  - 354 days after notification of event, action was taken
- **Challenges: How do we work collaboratively to reduce these timelines?**



354 Days

DISTRIBUTION A. Approved for public release: distribution unlimited.

Headquarters U.S. Air Force

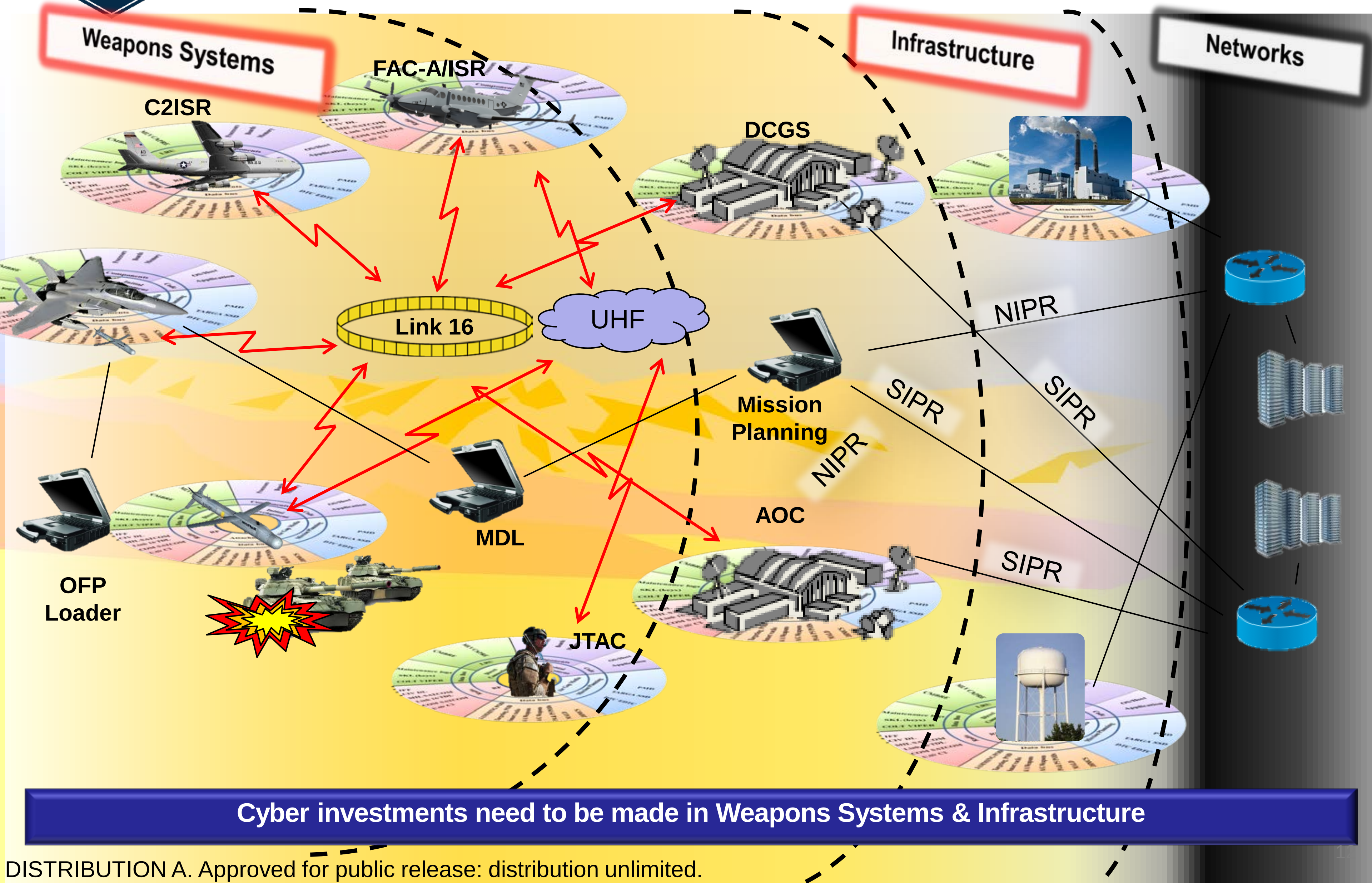
Integrity - Service - Excellence

Questions

&

Discussion

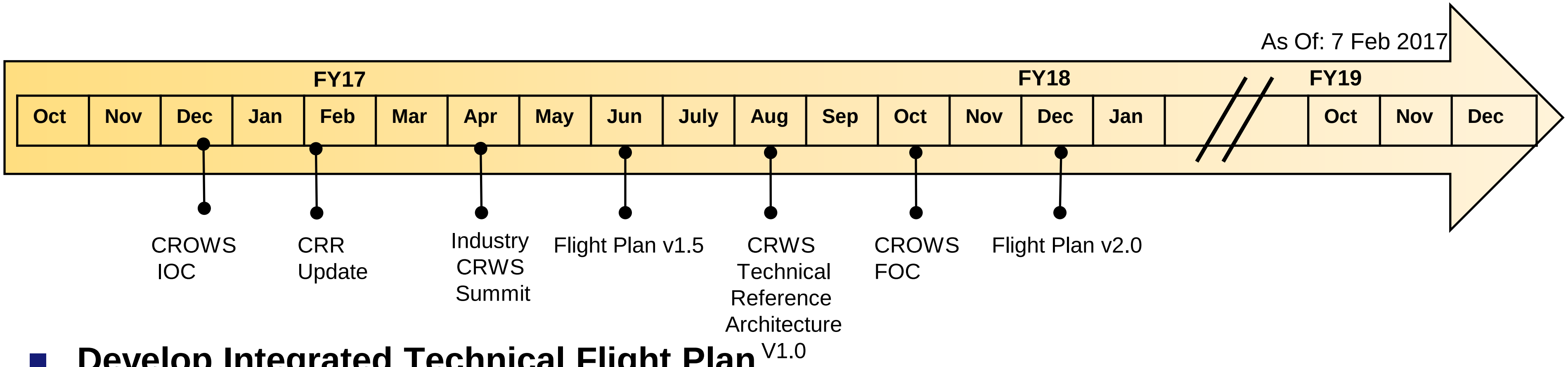
AF Cyber Boundary Framework



Cyber investments need to be made in Weapons Systems & Infrastructure

DISTRIBUTION A. Approved for public release: distribution unlimited.

Technical Flight Plan v1.0



As Of: 7 Feb 2017

FY17 | FY18 | FY19

Oct Nov Dec Jan Feb Mar Apr May Jun July Aug Sep Oct Nov Dec Jan // Oct Nov Dec

CROWS IOC

CRR Update

Industry CRWS Summit

Flight Plan v1.5

CRWS Technical Reference Architecture V1.0

CROWS FOC

Flight Plan v2.0

- **Develop Integrated Technical Flight Plan**

- **Establish Cyber Resiliency for Weapon Systems Technical Reference Architecture (CRWS TRA)**
  - **Align all efforts, products to the CRWS TRA – along the Technical Flight Plan**

- **Integrate across the AF CCP and stakeholder communities**
  - **AO, AT, TSN, etc.**

- **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?**

DISTRIBUTION A. Approved for public release: distribution unlimited.

CRWS-TAG

How Does it Work?

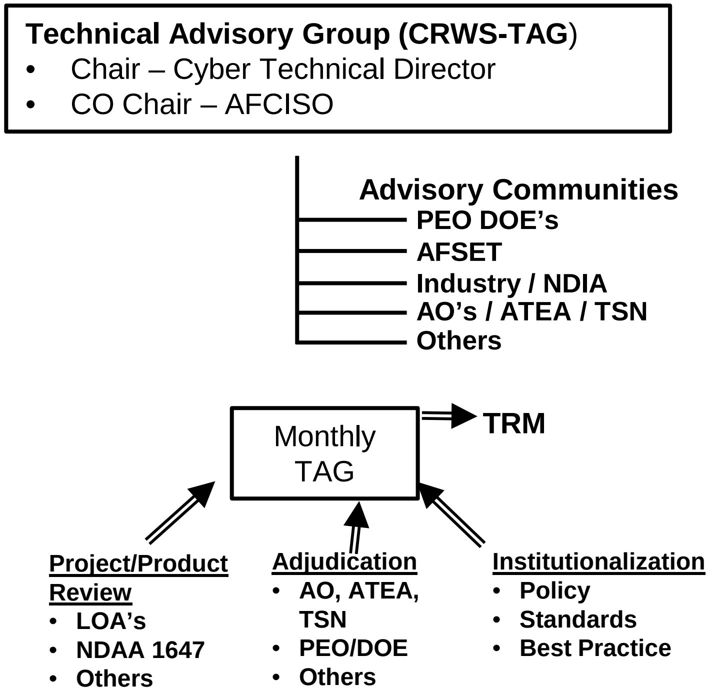
- Capture views of others
- Coordination across stakeholder communities
- Adjudication of items
- Produce Technical Recommendation Memo
  - Document findings with recommended Courses of Action

Examples

A. LOA Products
  - Products
  - Process Recommendations
  - Etc.

B. Institutionalization
  - Policy
  - Standards
  - Best Practices

C. Adjudication Requests



Technical Advisory Group (CRWS-TAG)
- Chair – Cyber Technical Director
- CO Chair – AFCISO

Advisory Communities
- PEO DOE's
- AFSET
- Industry / NDIA
- AO's / ATEA / TSN
- Others

Project/Product Review
- LOA's
- NDAA 1647
- Others

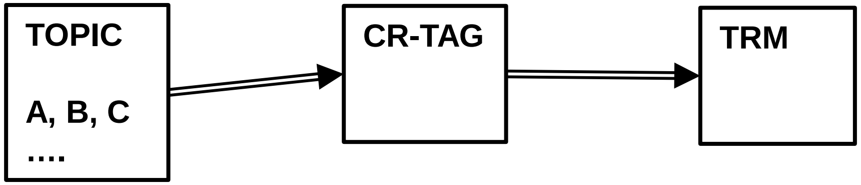
Adjudication
- AO, ATEA, TSN
- PEO/DOE
- Others

Institutionalization
- Policy
- Standards
- Best Practice

Objective:
Holistic Integration of Cyber security and Resiliency efforts

Cadence:
Scheduled Monthly Agenda

Technical Recommendation Memo:
- Staff Summary Sheet
- Documents
  - Coordination
  - Views of others
  - Decision Risk Space
  - Alignment to Flight Plan



AO – Authorizing Official
ATEA – Anti Tamper Executive Agent
TSN – Trusted Systems & Networks
LOA – Lines of Action

PEO – Program Executive Officers
DOE – Directors of Engineering
AFSET – Air Force Security Engineering Team (FFRDC/UARC collaboration)

DISTRIBUTION A. Approved for public release: distribution unlimited.

Cyber Resiliency

- **Definition (What does it mean?)**
  - **Cyber Resiliency = The ability to provide required capability despite adversity, 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".**

DISTRIBUTION A. Approved for public release: distribution unlimited.

Key Considerations (1/4)

- Design and build systems to operate securely
  - Protecting important information about the system (e.g. Critical Program Information)
  - Ensuring Supply Chain is trusted (e.g. Critical Components)
  - Protecting the Integrity of information (e.g. Information Assurance)
  - Resiliency to operate in face of faults (e.g. Regardless of type)
- Operate in a secure manner
  - Follow prescribed protection measures/procedures (e.g. NO Thumb drives!)
  - Understanding of Risk Tolerance and Acceptance (e.g. Who is accepting what Risk? When? Why?)
- Sustain ability of system to be operated securely
  - Understand dependencies on critical infrastructure (e.g. Power, HVAC, etc.)
  - Maintain systems view (e.g. DMS, P3I, “Form, Fit, Function)

Resiliency, in any dimension, requires a full life cycle view

DISTRIBUTION A. Approved for public release: distribution unlimited.

Key Considerations (2/4)

- **Mission Assurance ← System Assurance ← Systems Engineering**
- **Systems engineering spans a spectrum of related, interacting, conflicting, complimentary, system properties**
  - **Adaptability, agility, resilience, safety, security, survivability**

- **These properties are achieved through application of a common set of foundational systems, control systems, and specialty principles and concepts**

- **The composition of a specific property is embodied in the *viewpoint* of the system**
  - **Singularly: Safety viewpoint, security viewpoint, resilience viewpoint, etc.**
  - **Composed: safe, secure, and resilient, etc.**

DISTRIBUTION A. Approved for public release: distribution unlimited.

Key Considerations (3/4)

- Cyber resilience assumes presence and intent of an intelligent adversary
  - Modified hardware, software, or firmware system element
    - Counterfeit component, malicious insertion
  - Trusted individual misuse or abuse of system
    - Unauthorized use of system function/service
    - Unauthorized use of data/information

- Cyber resilience assumes the adversary presence may not be detectable
  - May be masked completely, or be interpreted as non-persistent or byzantine fault or failure

Key Considerations (4/4)

- Cyber resilience has the objective to limit the extent of damage due to intelligent adversary actions
  - Data/information loss and loss consequences
  - Function/service loss and loss consequences

- Cyber resilience focuses on specific cases of system correctness in system ability to deliver specified function
  - Correctness is system integrity
  - Deliver specified function is availability and continuity

- Objectives of cyber resilience overlap with other emergent property objectives with focus on intelligent adversary presence
  - Achieving *only* the specified
    - Behaviors
    - Interactions
    - Outcomes

DISTRIBUTION A. Approved for public release: distribution unlimited.