Naval Air Systems Command (NAVAIR) Cyber Developmental T&E

16 March 2016

Presented to:

ITEA Cyber Workshop

Presented by:

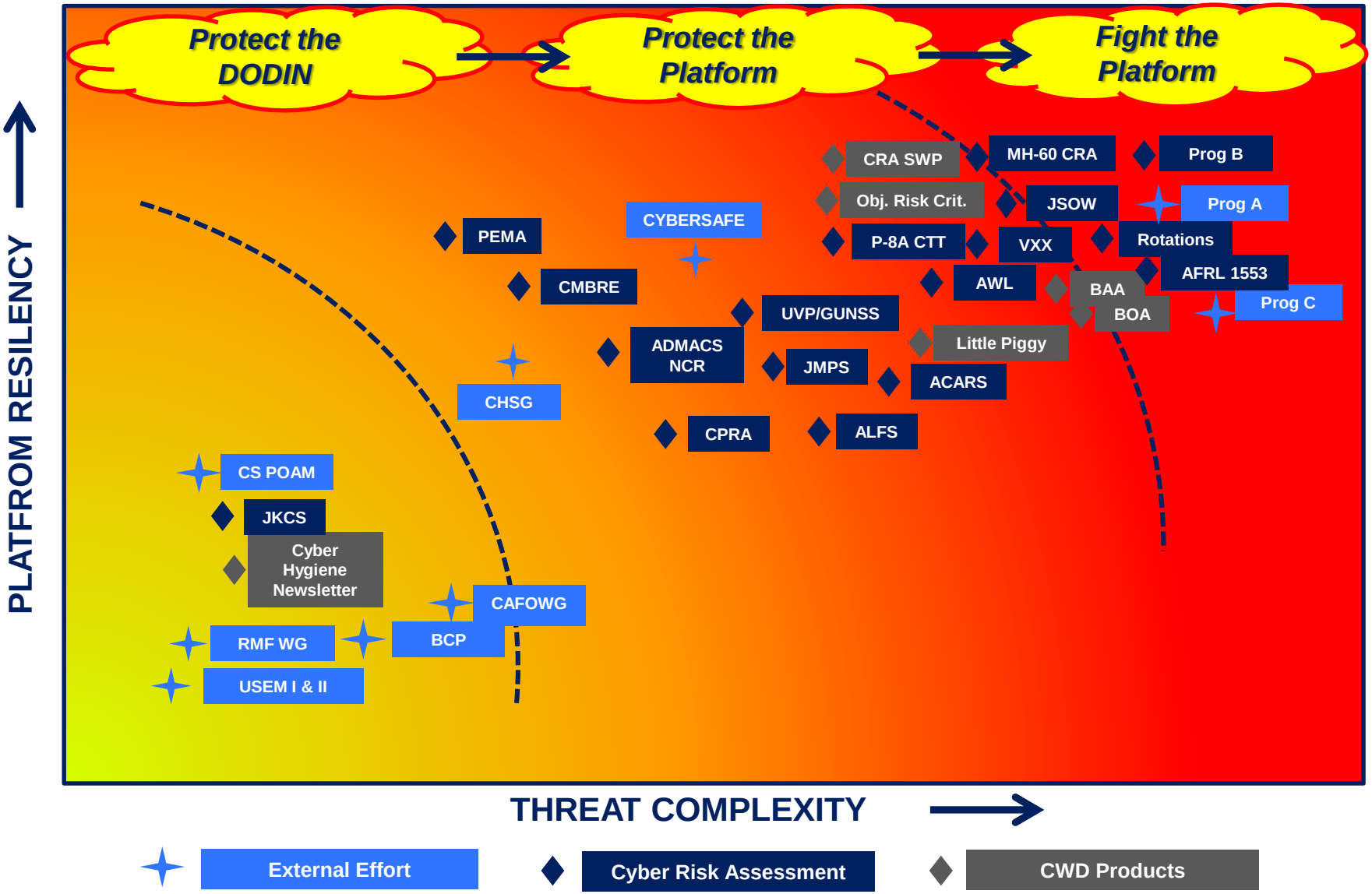
Mr. Stu Young (SES), AIR-00I

Director, I&I, Cyber Warfare Detachment

Cyber Warfare Requirements

- **What do our aircraft really need?**
  - Keep the bad out
    - Identify and isolate bad data, provide for redundancies and graceful degradation
      - No single measure is good enough
    - Know when & where there are problems – use risk-based prioritization to solve
  - Keep what we have working
    - Day to day reliability
    - Operate through an attack
      - "Play hurt" and play pro
    - Post event restoration
- **Keep the fleet operating**

Reducing Cyber Risk to NAVAIR Weapons Systems



On-Aircraft Cyber Testing

Tools:

- Wireless
- Aviation busses
- Avionics specific hardware
- Code analysis

Tool development in cooperation with:

- USAFRL, NSA, MIT LL, Sandia Labs, & industry

Software Defined Radio

1553 Data Sensor

Specific Tests

- **Performance Baseline**
- **Vulnerability Scans**
  - Assured Compliance Assessment Solution (ACAS)
- **Code Alteration**
- **Exfiltration**
- **Geo-fencing**
- **Awareness**
- **Restoration**
- **Penetration Test**
- **Counter Navigation**
- **Resiliency**
  - RF, Bus & Memory

Black Box

- **Scanning**
- **Fuzz Inputs**
- **Interface**
- **Abuse**
- **Exfiltration**

Testing Unknown vs. Known Systems

Cracked Box

- **Introspection**
- **Parsing**
- **Memory Management**
- **Stack Overflow**
- **Heap Spraying**
- **Exploit Development**
- **Arbitrary Code Execution**

Cyber Test Use Cases/Threat Vectors

- Brief access to unpowered aircraft
- Access by non-privileged personnel
- Unauthorized use by privileged personnel
- Malicious use by privileged personnel

External attack with no access

- Flight
- Maintenance
- Mission Planning
- Coalition Operations

Tools – Facilities & Equipment

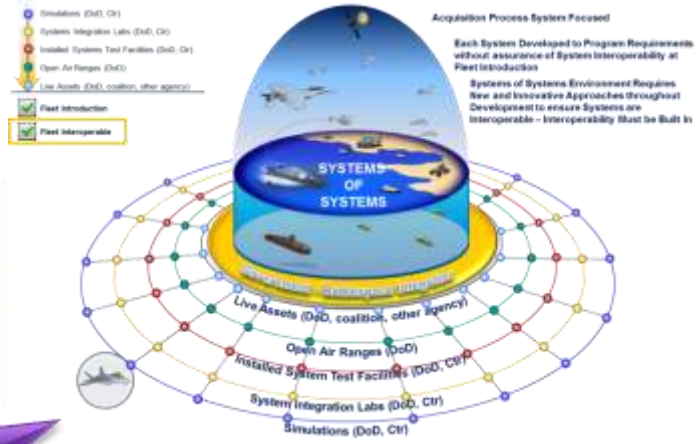
- Excellent baseline & good spaces to work in:
  - Multi-Level Security across many facilities
  - Instrumented
    - Individual Aircraft & Weapon System Labs (AWL/WSSL)
      - Likely to be the primary test site for Cybersecurity T&E
    - General purpose test
      - Rapid Prototyping Facility (RPF)
      - Advanced Systems Integration Lab (ASIL)
      - Ship Air Integration Lab (SAIL)
      - Manned Flight Simulator (MFS)
  - Defense Research & Engineering Network (DREN)
    - Connects facilities and connects us to outside facilities
      - National Cyber Range (NCR) & Joint Information Operations Range (JIOR)
  - Dedicated Cyber Labs
    - Sandbox and tool development

Infrastructure Development Strategy

- Component Box- Level
- System / Platform
- System Test Integration Laboratory
- Cyber LVC Environment
- Distributed DT&E
- Regional Naval Cyber Events
- Joint Cyber Events
- Operational Test Support
- Cyber Life-cycle support

System Integration Platform Level

SIL



Mission System Environment

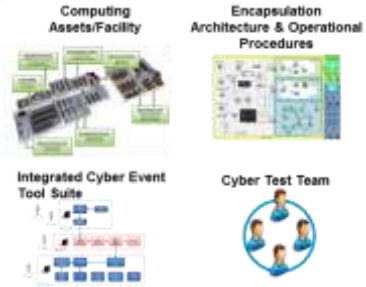
ESSIPE

System Component

PEMA

Path to Distributed Cyber Test

NCR



Cyber Contested Test Environment Multiple Platform Capability

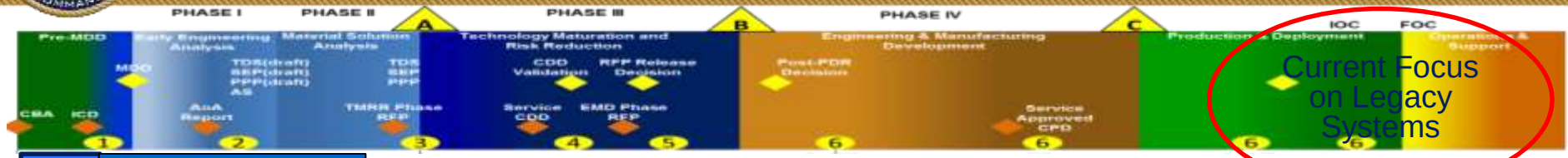
RSDP

Local Cyber Test Environment with Node Capability

Navy WAN T&E

- Cyber Logistics / Supply Chain
- Cybersecurity RMF
- Cyber Table Top
- CYBERSAFE
- Cyber Platform Risk Assessment
- CRA V&V
- Pen Testing / Cooperative Vulnerability Assessment
- M&S and LVC for Risk Reduction and SoS
- Integrated NAVAIR/Navy DT&E
- National Cyber Range / Regional Service Delivery Point
- Red Team - Adversarial Assessment
- Cyber Sustainment / Survivability

CYBERSAFE Flowchart



RMF Steps

CYBERSAFE

Airworthiness

1: Categorize System

2: Select Security Controls

3: Implement Security Controls / Harden System/ACAS scans

4: Assess Security Controls (IATTS as needed)

5: Authorize System (ATO)

6: Monitor Security Controls

Cybersecurity Controls

Identified Vulnerabilities

CRA Findings & corrections

- **Legacy**
- Developmental

Determine CSL

1- SoF
2- Org Mission
3- Net Mission
4- Sustain

Assign CYBERSAFE Grade using CYBERSAFE Grade Criteria (Standards)

CTT/CRA SWP

Update/Mod (w/TDP)

Verification (Cooperative & Adversarial)

Mitigation (Solution Development)

Validation (Cooperative & Adversarial)

DT&E/OT&E

Risk Management

CYBER Risk Review Board

CSPD Approval

Objective Risk Criteria

CS Certification

TAEs

CIO

CYBER Product Development

IT

SYSCOMS

Plan

Customer input

Request

Support

Review

Final

Cert Releaser

Certification

DON Requirements → **Acquisition** → **Sustainment**

Discussion/Questions?

Acronyms

ACARS-	AIRCRAFT COMMUNICATIONS ADDRESSING AND REPORTING SYSTEM
ADMACS–	AIR DATA MANAGEMENT AND CONTROL SYSTEM
AFRL-	AIR FORCE RESEARCH LAB
ALFS-	AIRBORNE LOW FREQUENCY SONOR
AWL-	ADVANCED WEAPONS LABORATORY
BAA-	BROAD AGENCY ANNOUNCEMENT
BCP-	BASELINE CONFIGURATION PILOT
BOA-	BASIC ORDERING AGREEMENT
CAFOWG-	CYBERSECURITY ARCHITECTURE FRAMWORK OWG
CHSG-	CYBER HARDENED STRIKE GROUP
CMBRE-	COMMON MUNITIONS BIT/REPROGRAMMING EQUIPMENT
CS POAM–	CYBERSECURITY PLAN OF ACTIONS AND MILESTONES (NAVIFOR)
CRA-	CYBER RISK ASSESSMENT
CTT-	CYBER TABLE TOP ASSESSMENT
CWD-	CYBER WARFARE DETACHMENT
GUNSS-	GEOINT UNIFIED NAVAL STREAMING SYSTEM
HBT-	HAPPY BIRTHDAY TAMMY
JKCS-	JOINT KNOWLEDGE CACHING SERVER
JSOW-	JOINT STAND-OFF WEAPON
NCR-	NATIONAL CYBER RANGE
PEMA-	PORTABLE ELECTRONIC MAINTENANCE AID
RMF-	RISK MANAGEMENT FRAMEWORK
SWP-	STANDARD WORK PACKAGE
USEM-	UNSUPPORTED SOFTWARE ERADICATION AND MITIGATION
UVP-	UNIFIED VIDEO PORTAL