Cybersecurity and Tech Insertion Workshop

Panel Members:

Frank Zahiri – AFSC/EN
Lance Ray – SCAR, AFLCMC Cybersecurity
Bill Chenevert – National Center for Manufacturing Sciences (NCMS)
James Clark – Mercer Engineering and Research Center (MERC)
Alain Lussier – Solavitek
Cybersecurity/Tech Insertion Workshop

Agenda

• Introduction/Challenge Statement.....................Bill Chenevert
• Government Requirements..............................Frank Zahiri/Lance Ray
• Cybersecurity/IATT Process Steps..................Frank Zahiri/Lance Ray
• IATT vs. ATO.................................................Frank Zahiri/Bill Chenevert
• AMUET Case Study/Lessons Learned..............James Clark/Alain Lussier
• Summary/Recommendations............................Frank Zahiri/Bill Chenevert
• Q&A/Open Discussion...........................................Audience
Challenge Statement

• Requirements for Cybersecurity continue to evolve and become more stringent

• Gaining an understanding of those requirements as well as learning how best to meet them has become a challenge

• Insertion of new, innovative technology is dependent on obtaining successful Cybersecurity assessment and Interim Authority to Test (IATT) or Authority to Operate (ATO) on a timely basis
Gap/ Needs

• Understanding of Cybersecurity/IATT/ATO requirements lacking
• Responsibilities not clear for new technologies impacting maintenance and sustainment
• Process to meet Cybersecurity/IATT requirements of new technology for Proof of Concept/Demos/Pilots needs clarity (vs. ATO)
• Demonstrate via Case Study issues at hand (Panelists)
• How can process be streamlined to help accelerate technology innovation for maintenance and sustainment (Audience)
so I connected the unclassified black & classified red wires for ONE com & data channel...

I modified the interface!

I didn’t have enough wire...

I’m picking up a lot of GREAT information!!

Here’s the classified mission data on my thumb drive, from home...

Great! I’ll load it on the mission computer.

Good thing they didn’t disable WiFi on this Mx computer

and our group account is admin!
What is Cybersecurity?

DoD Instruction 8500.01, Para 1(d), adopts the term “cybersecurity” as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 to be used throughout the DoD instead of the term “information assurance (IA).”

Cybersecurity Defined
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
The Risk Management Framework implements cybersecurity technical policies through the application of security controls, not by numerous standalone policies, memos, and checklists.
### NIST

<table>
<thead>
<tr>
<th>Document</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST SP 800-39</td>
<td>Managing Information Security Risk</td>
</tr>
<tr>
<td>NIST SP 800-37</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>NIST SP 800-30</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>NIST SP 800-53</td>
<td>Cybersecurity Controls and Enhancements</td>
</tr>
<tr>
<td>NIST SP 800-53A</td>
<td>Cybersecurity Control Assessment Procedures</td>
</tr>
<tr>
<td>NIST SP 800-137</td>
<td>Continuous Monitoring</td>
</tr>
<tr>
<td>NIST SP 800-60</td>
<td>Mapping Types of Information to Security Categories</td>
</tr>
<tr>
<td>NIST SP 800-160 (DRAFT)</td>
<td>Security Engineering Guideline</td>
</tr>
</tbody>
</table>

### DoD

- **DoDI 8500.01** “Cybersecurity” IT Definitions
  - Security Controls Guidance
  - Enterprise Governance
- **DoDI 8510.01** “Risk Management Framework for DoD IT”

### NSS

- **CNSSP 22** IA Risk Management Policy for NSS
- **CNSSI 1253** Categorization Baselines NSS Assignment Values
- **DRAFT CNSSI 1253A** Implementation and Assessment Procedures
- **CNSS 4009** Information Assurance/Cybersecurity Definitions

---

**RMF Alignment Documents and Guidance**

**NIST** – National Institute of Standards and Technology  
**NSS** – National Security Systems
Cybersecurity Applicability

All DoD-owned IT or DoD-controlled IT that receives, processes, stores, displays, or transmits DoD information

- All DoD information in electronic format
- Special Access Program (SAP) information technology, other than SAP IS handling sensitive compartmented information (SCI)
- IT supporting research, development, test and evaluation (T&E) and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD

_DoD information technology (IT) is broadly grouped as DoD information systems (ISs), platform IT (PIT), IT services, and products_
Air Force Information Technology
Managing cybersecurity risks is complex and requires the involvement of the entire organization including
- Senior leaders planning and managing DoD operations
- Developers, implementers, and operators of IT supporting operations

Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions and includes
- Cost, performance, and schedule risk for programs of record
- All other acquisitions of the DoD

The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources
Integrated DoD-Wide Risk Management

Traceability and Transparency of Risk-Based Decisions

Organization-Wide Risk Awareness

Inter-Tier and Intra-Tier Communications

Feedback Loop for Continuous Improvement

DoD CIO/SISO, DoD SRMC

WMA, BMA, FEMA, DIMA PAOs

DoD Component CIO/SISO

Authorizing Official (AO) System Cybersecurity Program

TIER 3
PLATFORM IT INFORMATION SYSTEMS

TIER 2
MISSION / BUSINESS PROCESSES

TIER 1
ORGANIZATION

STRATEGIC RISK

TACTICAL RISK

CS105-1-12
System Cyber Security Program

- Authorizing Official (AO)
- Information System Owners (ISO) of DoD IT
- Information Owner (IO), Program Manager (PM)
- Information System Security Manager (ISSM)
- Information System Security Officer (ISSO)
Authorizing Official

• Usually defined by Focus Area (e.g., Weapons, Logistics)
• Air Force has 25 AOs including Aircraft (Dr. K. Patel) and Industrial Depot Maintenance (Mr. K. Stamey)
• Navy and other Services have similar AO organizations
Risk Management Framework

Monitoring risk, managing change, reporting progress

Categorize

How important is the Mission/system/information

Select

What Cyber requirements apply? Requirements analysis

Authorize

Acceptable risks and/or plans to reduce risks to acceptable levels. Issue authorization?

Assess

How effective are the cyber requirements. What are the risks?

RMF

Monitor

O&M

Implement

Dispose

Initiate

Design in Cyber requirements via Systems Engineering and Test & Evaluation

Implement

Design
Cybersecurity RMF Six Step Process

Step 1. Categorize Information System

– Create description and boundary
– Categorize system and assign personnel (e.g., AO, ISO, IO, ISSM)
– Submit IT Categorization documentation for approval by AO
– Once approved, register into IT system (EDTDR/ITIPS, eMASS or equivalent)
Sample
Simple PIT Boundary
Sample Complex PIT Boundary

Safety and Surveillance
- Aircraft Flight Parameter Data (PCMCIA card)
- Terrain Database / Flight History Data (PCMCIA card)
- Mission Planning
- Cryptographic Key Data (SKL)
- Radar Reflectivity
- Return Data
- Atmospheric Conditions
- Weather Radar (LRU)

Communication
- Satellite Voice/ACARS Message Data
- VHF Voice/ACARS Message Data
- Non-Secure Voice Data
- Ground Station/ATC/Aircraft via VHF R/T (LRU)
- Ground Station/ATC/Aircraft via HF voice R/T (LRU)
- Ground Station/ATC/Aircraft via UHF voice R/T (LRU)

Navigation
- Position Data
- Tactical Air Navigation Data
- NDB Ground Stations/Navigational Systems
- E-1: ADF receiver (LRU)
- E-2: DME receiver (LRU)
- Position Data
- Civil/Military GPS
- Satellite Voice/ACARS Message Data
- INMARSAT SATCOM Network
- Satellite R/T (SAT-906) / ACARS CMU
- Satellite Voice/ACARS Message Data
- Satellite Ground Stations/Landing Systems
- GPS/ILS Multiple Mode Receiver

Software Updates and Mission Planning
- Cryptographic Key Data (SKL)
- Mission Planning
- ACARS message via Multifunction Control Display Unit (CMU)
- Mission Planning
- Floppy Disk via Airborne Data Loader (ADL)
- Aircraft Flight Parameter Data
- Aircraft/ATC via ATC/TCAS Computer
- Aircraft Identification Data (IFF)
- Aircraft/IFF Transponder (LRU)
- Ground Station/ATC/Aircraft via IFF Fill Panel

Legend
- Classified
- Unclassified
- E-# External Interface
10. Approval

1. The program office/ISO will integrate cybersecurity and cybersecurity risk management into their overall systems engineering, acquisition, test and evaluation, and risk management processes.

2. The program office/ISO will complete Risk Management Framework (RMF) steps to obtain an Interim Authority to Test, or Authority to Operate, as appropriate, before system testing or operations commence.

3. For systems AF IT (see AFI 33-141/17-110) the program office/ISO will ensure the system is registered in the Enterprise Information Technology Data Repository (EITDR) and/or Enterprise Mission Assurance Support Service (eMASS).
Step 2. Select Security Controls

– Common control identification (from applicable security controls – see CNSSI)
– Select security control baseline or use overlay selection if available
– Tailor security control selection to your IT system (modification)
– Develop Information Security Continuous Monitoring (ISCM) strategy
– Submit ISCM strategy for AO review and approval
– Once approved, register into IT system (EITDR/ITIPS, eMass or equivalent)
Sample Security Control Assessment

IR-6 / Incident Reporting

<table>
<thead>
<tr>
<th>Information Types</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>L M H</td>
<td>L M H L M H</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stolen, Damaged, or Lost AMUET laptop</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>unclassified</td>
</tr>
<tr>
<td>AMUET report outputs are readouts from the EWIS under test ONLY. Approved EWIS tech data will not be altered in any fashion from AMUET outputs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk mitigation shown below in IR-6/ Incident Reporting reinforces overall risk factor: Low.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The user organization requires personnel to report stolen equipment, laptop, and other AMUET components.

- AMUET test team will maintain control of all AMUET components throughout the assessment level 1 project evaluation.
- All data contained in AMUET is non classified and limited to platform wiring list
- Stolen test units and interface cable serial numbers will be blacklisted.
- Incident Policy requires replacement of all encryption key and passwords of laptop/router/TBUs.
- Original AMUET data results (i.e., hardcopy print, electronic media files, or on laptop memory) shall be retained in the possession of the AMUET operator for the duration of the aircraft subsystem under test (i.e., intercom subsystem). Signed copies of the aforementioned official data may be requested by authorized MX and SPO personnel. Once testing is complete, the original and signed copies of AMUET data results must be destroyed.
Cybersecurity RMF Six Step Process

Step 3. Implement Security Controls

– Implement security controls from approved RMF assessment

– Document implementation of security controls (artifacts demonstrating security controls – Design docs, Interface Control docs, SCRM Plans, SW Dev Plans, Test results, etc.)

– Team (ISSM, ISO, System Engr, PM) prepares the Security Assessment Report (SAR) and includes in the IATT/ATO package for submittal for AO review

– Register results into IT system (EITDR/ITIPS, eMASS or equivalent)
Cybersecurity RMF Six Step Process

Step 4. Assess Security Controls

– IATT/ATO Package submitted to SCA (Security Control Assessor) by team (ISSM, ISO, System Engr, PM)

– SCA conducts assessment of security controls in accordance with assessment procedures

– SCA submits assessment report including risk analysis and recommendations

– Team conducts initial remediation actions based on recommendations including Plan of Action and Milestones (POA&M)
Cybersecurity RMF Six Step Process

Step 5. Authorize System
– SCA reviews the Security Assessment Report (SAR) with concurrence and recommendation to AO for a decision
– AO reviews documentation and renders authorization that balances mission, business needs and security concerns

Step 6. Monitor Security Controls
– Monitor system changes and evaluate impact on security controls
– Perform ongoing assessments including remediation
– Document and report security status to AO
IATT vs. ATO

• AO renders a final determination of risk to DoD operations and assets, individuals, other organizations, and the Nation from the operation and use of the system

• DoD authorization decision is expressed as an Authorization To Operate (ATO), an Interim Authorization to Test (IATT), or a Denial of Authorization to Operate (DATO)

• IATT is required for all testing and evaluation of new technologies in a Development Test and Evaluation (DT&E) environment. ATO is required if testing in an Operational (OT&E) environment

• IATT is not an Authority to Operate on an ongoing basis

• IATT is timebound

• IATT system boundary may be different than ATO final system boundary
Voice-Directed Inspection Maintenance System
VIMS

**Technology**
- Voice directed system provides step by step verbal instructions while capturing inspection data in a hands-free, eyes-free mode.
- How it works:
  - Conventional paper or electronic checklists are converted into voice inspection plans through the use of built-in software tools.
  - Asset-specific inspection plans are provided to the maintainer on the floor through audio commands via the headset.
  - Maintainer responds to the instructions with spoken inputs.
  - Spoken data is transcribed into text format and sent to the data management systems for generating reports and record keeping.

**Participants**
- WR-ALC (Lead), Ogden and OC ALCs (Observers)
- AMXG, C5 SPO, WR IT, 559 LRDP
- AFLCMC
- Honeywell Sustainability and Productivity Solutions
- National Center for Manufacturing Sciences (NCMS)

**Schedule**
- Kickoff 4QFY16
- Subsysitems ID’d; baseline data collected 1QFY17
- VIMS programmed, training provided 1QFY17
- VIMS implementation/pilot completed 3QFY17
- Pilot results reported, Final Report issued 4QFY17

**Funding ($000)**
- CTMA Technology Award 125K
- NCMS Support (in-kind) 50K

**Benefits**
- Supports Air Force CBM+ Program Strategy
- Saves time (33% estimated)
- Improves accuracy of data input
- Enhances compliance to SOP (Std Oper Practices)
- Offers expedited inspection results to planner
- Gives advanced notice for long lead parts ordering
- Reduces aircraft inspection and repair flow days
VIMS IATT Boundary

Step 1 - On Flight Line

Data collected on the flight line and batched on the device.

Wired Headset Worn By Inspection Worker

Flight Line POC Boundary

Step 2 - on a separate secured network (in a faraday cage if needed) off of the Flight Line

Batched data from Flight Line uploaded to VoiceCheck for analysis and validation of POC success criteria.

Oracle or SQL DB VoiceCheck Server

Standalone POC Boundary
Simple – So What’s the Problem?

AMUET Case Study
AMUET Project Background

- Objective: Expand testing (beyond Proof of Concept completed in Phase I) of a new advanced wiring tester (AMUET) on multiple aircraft (C5, C130, CV22) electrical subsystems; validate benefits via a BCA
- Project Funding: $350K + $85K = $435K
- Funding Source: FCT (Foreign Comparative Testing Office - OSD)
- FCT Mission: Test technologies of our foreign allies that have a high Technology Readiness Level (TRL) to satisfy defense requirements more quickly and economically
- Team Members: Robins AFSC/EN, C5/C130 SPO Engrg, Robins ATS, Solavitek (Technology Provider), MERC (BCA), NCMS, Aircraft AO SCARs, FCT, NCMS
- Project Timing: 12-18 months (starting Feb, 2015)
AMUET - COTS
(70 lbs – 2 Pelican case)

All Platforms
Maintenance

Laptop (5 lbs)
10 TBU with router (25 lbs)
Galaxy phone is shown only to compare size
14 generic mates (40 lbs)

AMUET- TPS
Scope of work
(30 lbs – 1 Pelican case)

C5
Ready

C130J
Ready

Fuel Quantity (5 lbs) Intercom (15 lbs)
Turnaround time: 10 days / 40 days

Anti-skid (10 lbs)
Turnaround time: 10 days
AMUET Project Progress

- Graphic showing timeline and progress of project (from March 2015 to September 2015) when requirement for full CS approval was identified. *Takeaway -- everything was moving according to plan.*

- Graphic showing 14 month effort to achieve CS/IATT approval (show deadends and final path to approval). *Takeaway -- many lessons learned from the experience.*
AMUET Project Timeline

- **AMUET Kick Off Meeting** – Mar 2015
- **BCA Contractor Identified** – May 2015
- **Advised Cybersecurity Approval Needed to Proceed** – Sep 2015
- **Test Subsystems Identified** – Apr 2015
- **Test Plans Developed and Approved** – Jun 2015
- **Requirements Provided to Tech Provider** -- May 2015
- **AMUET H/W & S/W Ready for Testing** – Aug 2015
### Path to Cybersecurity/IATT Approval

<table>
<thead>
<tr>
<th>Step</th>
<th>Timeframe</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consulted with SPO Engrg on Cybersecurity Req’ts</td>
<td>Oct 2015</td>
<td>--</td>
</tr>
<tr>
<td>Waiver from full Cybersecurity approval. Denied</td>
<td>Nov 2015</td>
<td>--</td>
</tr>
<tr>
<td>SPO Engrg advised not responsible for ATE Cybersecurity approval</td>
<td>Dec 2015</td>
<td>--</td>
</tr>
<tr>
<td>Consulted with ATS Office on Cybersecurity ATE Approval</td>
<td>Jan 2016</td>
<td>--</td>
</tr>
<tr>
<td>Initiated RMF Assessment Process</td>
<td>Feb 2016</td>
<td>--</td>
</tr>
<tr>
<td>ATS advised they lacked budget to continue support</td>
<td>May 2015</td>
<td>--</td>
</tr>
<tr>
<td>ATS recommended A/C SCAR to work with core AMUET Team</td>
<td>Jun 2016</td>
<td>--</td>
</tr>
<tr>
<td>SCAR advised proper documentation required for submittal to AO</td>
<td>Jul 2016</td>
<td>--</td>
</tr>
<tr>
<td>Completed Categorization Doc and RMF Assessment</td>
<td>Sept 2016</td>
<td>--</td>
</tr>
</tbody>
</table>

3 Mo. | 5 Mo. | 4 Mo.
Path to Cybersecurity/IATT Approval (Cont’d)


Categorization Document approved by AO -- Oct 2016

Submitted IATT approval request to AO -- Nov 2016

IATT approved by AO – Nov 2016

AMUET Project Timeline (Cont’d)

Project resumed -- Dec 2016

Test Plan (new) finalized – Feb 2017

C130 testing complete (3 subsystems) -- Mar 2017

2 Mo.

14 Mo. Total

GO

GO
RMF Initiation Process

• Standard AMUET architecture has intrinsic cyber security protection features including:
  o OSD security standards (security access, anti-virus, encrypted hard disk). No access to US DoD intranet or any internet communications and Windows 7 operating system, during Project Test
  o Laptop hardware and operating systems will be purchased through USAF IT channels and existing cyber security controls applied
  o Gateway and TBUs configured using WPA2 encryption security protocol
  o The power (gain) settings limited to the immediate perimeter of the aircraft being tested
  o AMUET commands and data sharing between TBU and laptop
    - TBUs do not support wireless reprogramming
    - Data sharing with laptop i) TBU serial number ii) harness serial number iii) voltage measurements
RMF Initiation Process

• Two assessment levels were established, ASSESSMENT LEVEL 1 - Project Test Environment and ASSESSMENT LEVEL 2 - Future Production-Ready Environment

• Use of pertinent NIST Risk Management Framework Processes (SP 800-37) and NIST’s guidance for information security continuous monitoring (SP-800-137):
  - AC-17 Remote Access
  - AC-18 Wireless Access
  - AC-19 Access Control for Mobile Devices
  - CA-3 System Interconnections
  - IR-6 Incident Reporting
  - MP-2 Media Protection
  - SA-5 Information System Documentation
  - SI-12 Information Media Handling and Retention

• A more rigorous RMF examination effort must be completed and compliance assured for future ASSESSMENT LEVEL 2 application of the AMUET, to obtain ATO
Future ATO Approval

Artifacts

(ATO) Cybersecurity Impact Evaluation Package for AMUET

Weapon system Waiver Letters

AMUET Risk Mgmt Framework Controls Assessment Package


EMASS

(ATO) Authority to Operate Letter

Stakeholders: C-130, CV-22 Program Offices, MX & Field Ops, ATS, OSD FCT, AMUET Team

Independent Analyses and Assessments of PIT

Phase II Testing Completion Hurlburt Field Possible Phase III Integration Program

ATO Cybersecurity Impact Evaluation for AMUET

Artifact Generation

Authority to Operate Package

Approved ATO

Signed AO letter for ATO

Yes
Observations

- Cybersecurity DoD Risk Management Process is a separate and distinct from the Technology Development and Insertion Process (per AFCCI-101) for new technology prove out and testing at a DoD facility
- Difficult to find knowledgeable Cybersecurity resources for a new Mx-related technology not yet in the acquisition phase
- AO responsible for approving Mx-related new Test and Evaluation equipment (that touches an aircraft) turned out to be a gray area
- Required to follow same approval path as complete Weapons Systems
- Process is long and time consuming, required considerable hand holding
## Platform Information Technology System Cybersecurity Activities

<table>
<thead>
<tr>
<th>PIT Cybersecurity and Assessment &amp; Authorization (A&amp;A)</th>
<th>Develop and coordinate Cybersecurity Strategy for IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Cybersecurity analysis for Communication, Navigation, and Systems/Air Traffic Management (CNS/ATM)</td>
<td>Conduct threat/vulnerability analysis</td>
</tr>
<tr>
<td>Develop and coordinate PIT Determination Packages</td>
<td>Conduct Site Cybersecurity audits</td>
</tr>
<tr>
<td>Conduct PIT architecture, hardware and software analysis</td>
<td>Conduct Supply Chain Risk Management (SCRM) of PIT systems</td>
</tr>
<tr>
<td>Apply PIT Cybersecurity Risk Management Framework (RMF)</td>
<td>Conduct hardware and software assurance assessments</td>
</tr>
<tr>
<td>Develop IATT and/or ATO approval packages</td>
<td>Support Anti-Tamper (AT) assessments</td>
</tr>
<tr>
<td>PIT Cybersecurity testing of hardware and software</td>
<td>Support cryptography analysis</td>
</tr>
<tr>
<td>Support PIT Authorization Official (A0)</td>
<td>Support airworthiness Certification</td>
</tr>
<tr>
<td>Develop and coordinate PIT System Security Plans (SSP)</td>
<td></td>
</tr>
</tbody>
</table>
Cybersecurity SMEs Desired Characteristics

- Aligned with DoD Cybersecurity Risk Management Policies
- Expert in Cybersecurity and RMF approval processes/guidebooks (e.g., Industrial Depot Maintenance Authorizing Official Guidebook, December 2016)
- Knowledgeable in Mx technologies and the Technology Development and Integration Process (TDIP)
- Capability to train and advise new technology stakeholders (tech providers, tech owners, IOs) through prove out/testing of Mx-related technologies (prior to full acquisition)
• MX Technology Integration
  – System & MX Process Knowledge, Design, Testing, and Integration Capabilities
  – Technology Development and Insertion Process (TDIP)

• MX Technology Worthiness on Aircraft, Weapons, and Facilities
  – Authoring/reviewing, providing comments on, and/or modifying existing Installation Plans, Security Test Plans, Test procedures, and a variety of other Air Worthiness, System Safety, and Cybersecurity documentation
CS SMEs, Alignment w/ AFLCM, AFCEC & AFSC RMF policies

– Testing Requirements

  • Determination/Characterization/Impact/Vulnerability Analyses, IV&V, Pen Testing
  • Independent Evaluation: Cybersecurity Centers of Excellence for Collaborative Testing and Training Expertise
  • Formal MX Technology Training for Cyber Compliance

– Proactive Accreditation Pre-Testing, Accreditation Worthiness Assessment, and Compliance Testing

– Individual Accreditations. I.e.. IC2 Approved and Sponsored Organizations
• Cybersecurity Regulatory Experience
  – CS Guidebook(s) for targeted MX technologies in support of the RMF Process (i.e. Industrial Depot Maintenance Authorizing Official Guidebook, December 2016)
  – Risk Management Framework (RMF) processes (SP 800-37), NIST’s guidance for information security continuous monitoring (SP-800-137), the NIST Cyber Security Framework, DoDI 8500.01, DoDI 8510.01, AF 17-101, and CNSSI 1254
Lessons Learned

• Identify Cybersecurity/IATT team upfront including AO for new Mx-related technologies requiring test and prove-out in DoD environment

• Obtain full commitment from stakeholders to support through entire Cybersecurity process (including RMF Assessment)

• Define PIT Boundary for IATT vs. ATO (Objective: Prove new technology works before considering buying/integrating into secure IT systems)

• Assure experienced Cybersecurity/IT SMEs are available to train and advise team

• Allow up to 5 months for Cybersecurity/IATT approval (perfect world)
Recommendations

• More streamlined targeted Cybersecurity approval process for new Mx-related technologies that require demonstration, prove-out, testing, piloting at DoD maintenance facilities

• Integrate Cybersecurity Approval Process with the Technology Development and Insertion Process (TDIP) and utilize resources for such integration

• Establish formal Cybersecurity Approval Process training for Mx-related activities working to test and evaluate new technologies

• Simplify and reduce Cybersecurity/TDIP req’d documentation