Headquarters U.S. Air Force

Integrity - Service - Excellence

EPRM
Enterprise Protection
Risk Management

EPRM Implementation Workshop

Session 1: Why EPRM

Efficiency, Effectiveness & Policy

U.S. AIR FORCE

Session Objectives

- **Learning Objective:** To receive an orientation to the EPRM tool and its role within Air Force information protection (IP) and Operations Security (OPSEC) communities to help create efficiencies, generate a converged security output for commanders and to become compliant with the Defense Security Enterprise (DSE) risk framework

- **Enabling Learning Objectives**: The student will be able to:
  - ❑ Identify the three main reasons behind the creation of EPRM
  - ❑ Be able to paraphrase the relationship between EPRM and the DoD 5200.43 Defense Security Enterprise and AFPD 16-14 Air Force Security Enterprise
  - ❑ Identify the protection areas in EPRM 1.0
  - ❑ Identify the three critical data-elements in a risk-based assessment/inspection

Overview

Video #2: Why EPRM

1. Personnel
2. DSE Policy
3. Converged Risk Picture for Commander

Personnel Drivers

- **Manpower Cuts Drive Need for Efficiencies**
  - 2011 Resource Management Decision (RMD 703) in 2011
    - SAF/AAZ, MAJCOM/IP & Wing IP office lost positions
  - 2013 Civilian manpower reductions
    - Some IPs lost more positions
  - 2015 Headquarters staff reductions
    - MAJCOM IPs lost positions
  - 2015-2016 Wing IP Manpower Study
    - Some IPs will lose positions
    - No archival centralized database to capture historical workload processes
      - Led to Inconsistencies in data submitted to 4th Manpower Resource Sqdrn (MRS)—impacted manpower numbers
  - 2017 Federal government hiring freeze
    - Many IP positions are vacant and cannot be filled

IP Workload

- Workload has increased, despite manpower reductions
  - “Doing More With Less” is a decreasingly viable expectation
- Individual IP staff members required to cover multiple protection areas
  - Need to standardize processes between protection areas
  - Need to provide tools to decrease training time need to work cross-discipline
- “Risk-based” requirements are coming into effect
  - Will require HQ-funded tools and training to ensure it does not increase workload.

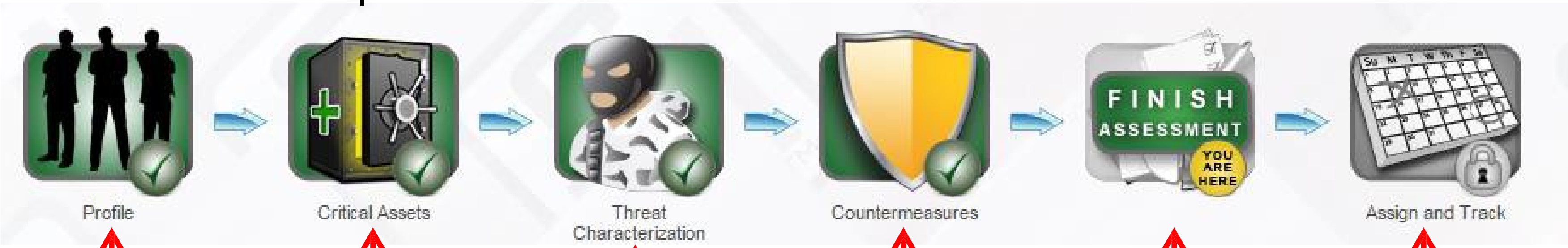
EPRM as a solution to manning/workload

- **Centralized automation brings efficiency by reducing workload**
  - Creates repository for past inspections
    - No more spending time in email looking for old reports/write-ups
  - Comprehensive checklists require less time at MAJCOM/Wings who currently create their checklists each time regulations are updated
  - Reduces manual staff processes
    - Reports generated automatically (e.g. Self-Inspection Report "viewed" from Wing IP up to SAF/AAZ)
    - Queries decrease need for 'data calls' responding to HHQ and CC

EPRM as a solution to manning/workload

EPRM Enterprise Protection Risk Management

- On-screen workflow decreases Wing IP workload by:
  - Allowing preloading to reduce redundant data entry
  - Auto-generating individual and aggregate reports
  - Allowing some protection areas to leverage unit personnel to provide data for inspections/assessments



Captures elements of information needed to Identify pertinent policy/ practices/ etc.

CRITICALITY (C)

Contains asset selections, categorizes assets & characterizes consequence criteria for each (impact of loss)

THREAT (T)

Baseline threat-source, methods and capability/intent preloaded

(Preloads provided by DIA & NASIC)

Allows local tailoring of threat

VULNERABILITY (V)

Provides automated checklists and evaluation guidance for self-assessments and staff assist visits

Countermeasures library mapped to the threat tactics that they mitigate

Risk analysis views based on **C*T*V** plus compliance analysis of baseline levels of protection

Outputs (exports) in .doc, .pdf, .xls & .ppt

Aggregate analysis and reporting

Tracking for remediation plan or facility enhancements

Policy Drivers

- DoDD 5200.43 (Defense Security Enterprise Governance - SECDEF)
  - 4. Standardized security processes shall be implemented, to the maximum extent possible and with appropriate provisions for unique missions and security environments, across the enterprise to ensure maximum interoperability, consistent quality assurance, and cost savings…process is risk-managed and results-based and that informs the DoD.

- AFPD 16-14 (Air Force Security Enterprise Governance (AFSE) - SECAF)
  - 2.1 Develop and sustain an enterprise security framework and strategic plan, incorporating mission assurance, to provide an integrated risk-managed structure to guide AFSE policy implementation, inform investment decisions, and to provide a sound basis for oversight and evolution.

- Commanders have self-assessments/staff assist visits required by:
  - AFI 10-701 (OPSEC)
  - AFI 16-1404 (INFOSEC)
  - AFI 16-1406 (INDUSEC)
  - AFI 31-501 (PERSEC)
  - National Insider Threat Task Force (NITTF) (Service-level reporting)
  - UFC 4-010-01 (Assessments of off-base facilities to Interagency Security Committee (ISC) standards)
  - (Next) NIST 900-37 & 53 (Cyber assessments of acquired weapon systems)

EPRM Addresses emerging DoD policy

- EPRM Initiated & advocated by the Air Force Security Enterprise Executive Board (AFSEEB) for the AFSE
  - SECAF's executive body for security enterprise and mission assurance policy development, risk management, resource advocacy, oversight, implementation and training *(AFPD 16-14)*
  - AFSEEB directed EPRM to be a cross-disciplinary, all-hazards decision support tool for security compliance and risk assessments; facilitates and standardizes risk assessment processes and promotes early implementation of cost-effective countermeasures.

- Provides Wing/unit-level users with mechanism to address the three <u>critical elements of risk-based assessments</u>
  1. Threat likelihood and severity
  2. Asset criticality
  3. Vulnerability to threat activity

Challenges for Commanders

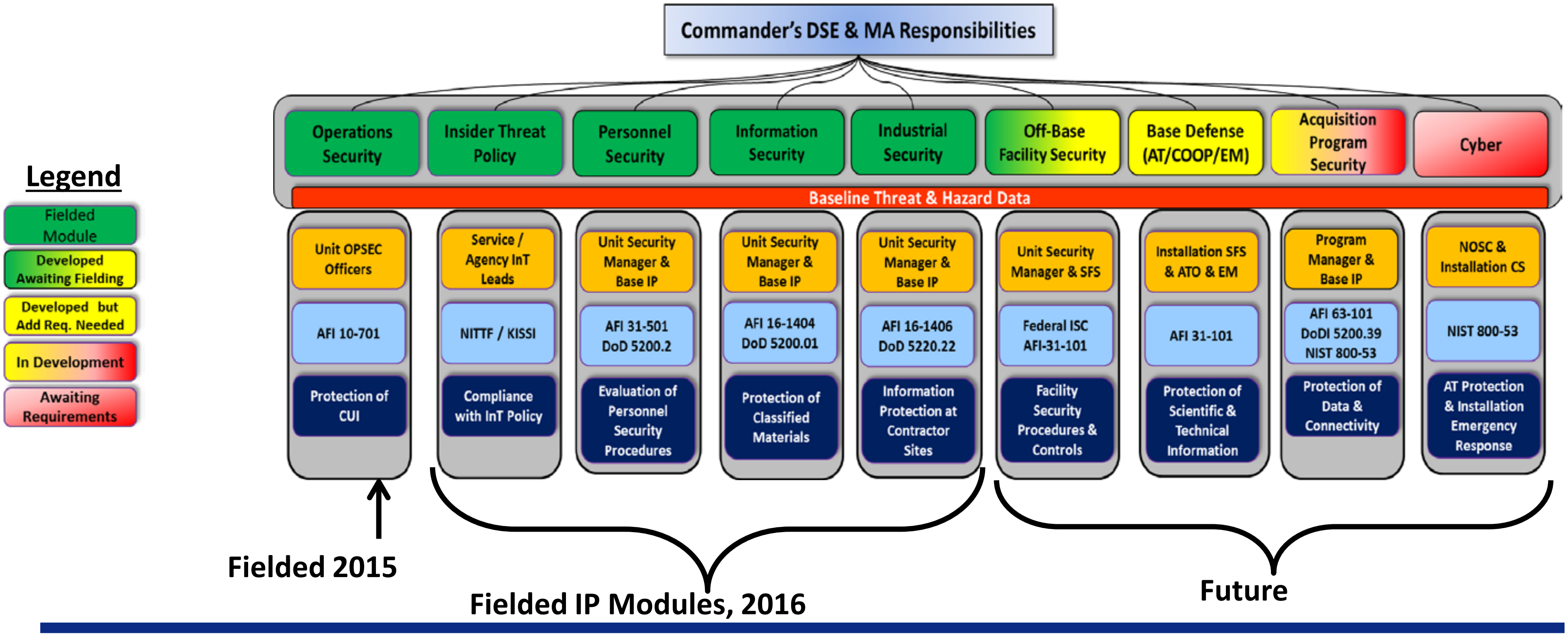
- Maintaining situational awareness of factors that contribute to risk
  - Across protection areas, commanders are presented with assessments that differ in methodology, metrics, terms and frequency
  - Many assessments are not linked to local threat or operational (mission) requirements
  - No common construct to quantify or communicate risk mitigation, risk acceptance, risk avoidance or risk reduction

- Justifying and prioritizing remediation decisions based on overall risk mitigation and risk reduction per dollar

- Demonstrating compliance with OPSEC, INFOSEC, Industrial Security and PERSEC instructions

Cross-Disciplinary Situational Awareness

- Common process & metrics across protection areas
  - Supports OPSEC assessments DoD-wide (900+ users)
    - Absorbed the Operations Security Collaboration Architecture (O.S.C.A.R., 2007-2014)
  - Supports information protection (IP) assessments AF-wide (Added May 2016)
  - Supports Service/Agency Insider Threat Program assessments
- Future modules in discussion with OPRs



Commander's DSE & MA Responsibilities

Baseline Threat & Hazard Data

Operations Security	Insider Threat Policy	Personnel Security	Information Security	Industrial Security	Off-Base Facility Security	Base Defense (AT/COOP/EM)	Acquisition Program Security	Cyber
Unit OPSEC Officers	Service / Agency InT Leads	Unit Security Manager & Base IP	Unit Security Manager & Base IP	Unit Security Manager & Base IP	Unit Security Manager & SFS	Installation SFS & ATO & EM	Program Manager & Base IP	NOSC & Installation CS
AFI 10-701	NITTF / KISSI	AFI 31-501 DoD 5200.2	AFI 16-1404 DoD 5200.01	AFI 16-1406 DoD 5220.22	Federal ISC AFI-31-101	AFI 31-101	AFI 63-101 DoDI 5200.39 NIST 800-53	NIST 800-53
Protection of CUI	Compliance with InT Policy	Evaluation of Personnel Security Procedures	Protection of Classified Materials	Information Protection at Contractor Sites	Facility Security Procedures & Controls	Protection of Scientific & Technical Information	Protection of Data & Connectivity	AT Protection & Installation Emergency Response

Legend

- Fielded Module
- Developed Awaiting Fielding
- Developed but Add Req. Needed
- In Development
- Awaiting Requirements

Fielded 2015

Fielded IP Modules, 2016

Future

Converged Analysis for Commanders

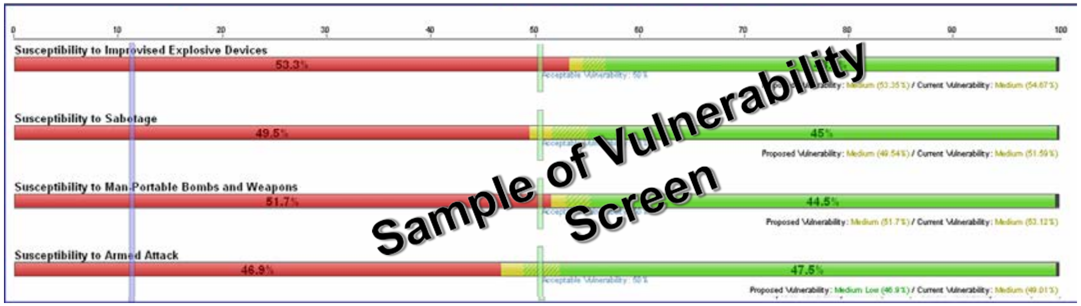
- Supports commanders in making better informed, risk-based decisions on where to best allocate resources
  - Ties assessments to local threat & operational (mission) requirements
  - Provides standardized/common analytical framework
  - Promotes risk-based analysis, beyond just compliance
  - Converges multiple protection disciplines in a single analysis

No plans to mitigate

Will be mitigated by countermeasures that have been approved by commander but not yet implemented

Mitigated by countermeasures that were approved and have now been implemented

Mitigated by countermeasures that were in-place originally



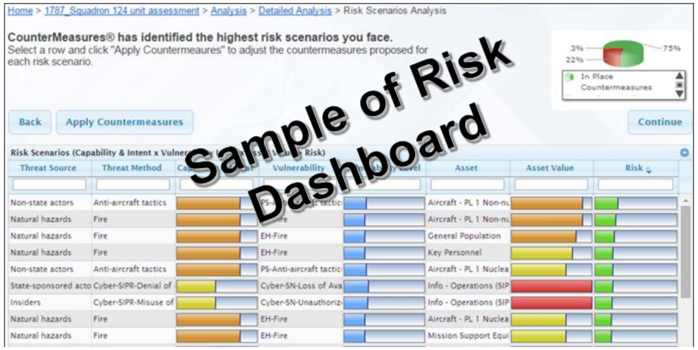
Susceptibility to Improvised Explosive Devices
53.3%
Acceptable Vulnerability: 50%
Proposed Vulnerability: Medium (53.35%) / Current Vulnerability: Medium (54.67%)

Susceptibility to Sabotage
49.5%
45%
Proposed Vulnerability: Medium (49.54%) / Current Vulnerability: Medium (51.59%)

Susceptibility to Man-Portable Bombs and Weapons
51.7%
44.5%
Proposed Vulnerability: Medium (51.7%) / Current Vulnerability: Medium (53.12%)

Susceptibility to Armed Attack
46.9%
47.5%
Acceptable Vulnerability: 50%
Proposed Vulnerability: Medium Low (46.9%) / Current Vulnerability: Medium (49.01%)

Sample of Vulnerability Screen



Home > 1787_Squadron 124 unit assessment > Analysis > Detailed Analysis > Risk Scenarios Analysis

CounterMeasures® has identified the highest risk scenarios you face.
Select a row and click "Apply Countermeaures" to adjust the countermeasures proposed for each risk scenario.

Risk Scenarios (Capability & Intent x Vulnerability Level x Asset Value = Risk)

Threat Source	Threat Method	Capability & Intent	Vulnerability	Vulnerability Level	Asset	Asset Value	Risk
Non-state actors	Anti-aircraft tactics		PS-Anti-aircraft tactic		Aircraft - PL 1 Non-nu		
Natural hazards	Fire		EH-Fire		Aircraft - PL 1 Non-nu		
Natural hazards	Fire		EH-Fire		General Population		
Natural hazards	Fire		EH-Fire		Key Personnel		
Non-state actors	Anti-aircraft tactics		PS-Anti-aircraft tactic		Aircraft - PL 1 Nuclea		
State-sponsored acto	Cyber-SIPR-Denial of		Cyber-SN-Loss of Ava		Info - Operations (SIP		
Insiders	Cyber-SIPR-Misuse of		Cyber-SN-Unauthoriz		Info - Operations (SIP		
Natural hazards	Fire		EH-Fire		Aircraft - PL 1 Nuclea		
Natural hazards	Fire		EH-Fire		Mission Support Equi		

Sample of Risk Dashboard

Where EPRM is Now

- Hosted on SIPRNET at DISA DECC-Montgomery
- Assessed and authorized program of record
  - Full authority to operate (ATO)
  - Clinger-Cohen Act compliant
  - Approved by DoD Investment Review Board (NDAA 2005 certified)
- Funded through FY22 for development and sustainment
- Managed by SAF/AA with modules designed to requirements of OPR SMEs
- Advocated by OUSD(I) as a best practice for the Defense Security Enterprise
  - 1000+ users across DoD Services/Agencies
  - User-base expanding in response to new capabilities

What's next for EPRM

- **Training**
  - On demand training soon to be on CDSE.edu (currently on SAF/AAZ SharePoint and *http://eprmhelp.countermeasures.com*)
  - Web-based instruction (screen-by-screen videos)
    - Web classes on: Elements of Risk, Risk management principles, Implementing EPRM for a Wing or MAJCOM
  - 2-day workshop on-site at each MAJCOM and DRU
- **Policy**
  - SAF/AA policy authorizing implementation (signed Sept 2016)
  - Updating 16-1404 to make EPRM the mechanism for the INFOSEC annual self-inspection report
  - Update 1405 & 1406 to incorporate EPRM
- **MICT Update**
  - Use EPRM to satisfy commanders self-assessment checklists requirements for INFOSEC, PERSEC, Industrial Security
  - Include EPRM in requirements for MICT

Session Review

- What are the three main driving reasons behind the creation of EPRM?
- What is relationship between EPRM and the DoD 5200.43 DSE and AFPD 16-14 AFSE
- What are the protection areas in EPRM 1.0?
- Identify the three critical data-elements in a risk-based assessment/inspection