EPRM Implementation Workshop

Session 1: Why EPRM

Efficiency, Effectiveness & Policy
**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
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
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

CRITICALITY (C)
Captures elements of information needed to identify pertinent policy/practices/etc.

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 critical elements of risk-based assessments
  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)
  - Supports information protection (IP) assessments AF-wide (Added May 2016)
  - Supports Service/Agency Insider Threat Program assessments
- Future modules in discussion with OPRs
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

Sample of Vulnerability Screen

Sample of Risk Dashboard
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
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