SPRING 2024 EPRM NEWSLETTER
Sent to all users on 9 May 2024

EPRM Users,

EPRM is getting an extensive update in early 2025 (details below). To keep you aware of the changes and obtain feedback, we will be sending more regular communications.

EPRM PROGRAM MANAGEMENT

In October 2023, the management of EPRM transitioned from the Administrative Assistant to the Secretary of the Air Force (SAF/AA) to the Air Force Life Cycle Management Center Cybersecurity Division (AFLCMC/EZC), Cyber Resiliency Office for Weapons Systems (CROWS). This transition had no impact on the daily operations of the tool and all fielded modules remain operational. This communication is being sent on behalf of the current program manager:

Mr. Shawn Quillen
shawn.quillen.1@us.af.mil

MODERNIZATION

The EPRM application is being reengineered and is moving to the cloud in early 2025. This change will result in a smoother user experience and a streamlined interface. The update will include:

- A hierarchy driven dashboard which is customizable,
- Faster performance,
- Better screen utilization,
- Improved flow from assessment to analysis,
- Default to "No" responses (removal of no-to-all button),
- On-grid text of comments (removal of "view comments" icon), and
- Updated reports, including PowerPoint.
- We are looking for ideas and examples of reports that you would like the system to generate. Please send examples or suggestions to the user support team.

SEEKING VOLUNTEERS

The modernization of EPRM will require testing and early implementers. If you would like to test the application and provide preliminary feedback, please send an email to our user support team. Preliminary testing is expected to begin in late summer/early fall. Testers will receive instructions and access to the testing environment. Feedback will be used to ensure the tool is meeting the needs of the field.

TRAINING

The User Support team has supported requests for live virtual instruction when requested. Continue to route such requests through the user support team. Later this year we hope to offer more regularly scheduled webinars of how to use the tool.

SURVEY MONKEY
In our next newsletter, we will be using a Survey Monkey questionnaire to seek feedback and understand the priorities of those regularly logging into EPRM.

MODULES AVAILABLE FOR USE IN EPRM ON SIPR
The Enterprise Protection Risk Management (EPRM) application is a web based, cross-disciplinary decision support tool for security compliance and risk assessments. The tool facilitates and standardizes processes and promotes early implementation of cost-effective countermeasures.

Acquisition Security Module (ASM)
The ASM addresses the lack of standardized and automated methodology to generate traditional security countermeasures; objectively evaluates countermeasure effectiveness; produces quantifiable data for Security, Engineers, Program Managers (PM), Industry Partners, and Decision Makers; and supports risk-based decision making throughout the acquisition life cycle. Primarily focused on automating and standardizing Program Protection Plans, ASM is made up of the ASM assessment, Supply Chain Risk Management (SCRM) survey, WS Cyber 1637 survey, and WS Cyber Health Assessment survey. The ASM assessment is used for RFP development, generation of countermeasure consideration, and risk management for PMs, PEOs, and MDAs. All of the assessments and surveys are on SIPRNet and ready for use. The Program Protection Plan survey is currently in use.

Mission Assurance Risk Management System (MARMS)
MARMS is managed by the Defense Threat Reduction Agency (DTRA) along with the US Army Futures Command as Lead Integrator, in support of the Joint Chiefs of Staff and the DoD-wide Mission Assurance community. MARMS is a federation of systems designed to support the execution of the Mission Assurance process. EPRM officially represents the Assessment module of the federation. The two modules within EPRM designed specifically for the MARMS program are the Antiterrorism (AT) Module, and the Mission Assurance (MA) Module.

Updates:
-There was an MA Workshop at Army HQDA on May 6 to 9.
-The Antiterrorism threats and countermeasures are currently being updated and are projected to be released in July.

EPRM Cyber Module (ECM)
The cyber security module allows:
-Audit AF Local Registration Authorities (LRA) performing aspects of PKI certificate issuance and management at the AF site/installation/base level, in compliance with the DoD PKI Registration Authority/Local Registration Authority (RA/LRA) Certificate and Registration Practice Statements (CPS/RPS);
-Facilitate JFHQ-DODIN Readiness and Security Inspections (DRSI) responsibility to conduct CPS and RPS PKI Audits of Registration Authorities (RA), and Local Registration Authorities (LRA) throughout the DoD, and;
-Allow the Services and Agencies throughout DoD to conduct pre-inspection and scoping, as well as self-assessment and continuous monitoring, within the Command Cyber Readiness

Inspection (CCRI) construct, prior to the official CCRI assessment conducted by JFHQ-DODIN (DRSI).

ECM is broken into two variants, PKI Audit Module (PAM) and CCRI Assessment Module (CAM).
-PAM
--The EPRM Public Key Infrastructure (PKI) Audit Module (PAM) addresses PKI audit requirements and facilitates the PKI audit process for the Air Force at the local site/installation/base level, and the DoD PKI community at the Service/Component/Agency level across the DoD enterprise.
--IAW AFMAN 17-1301, all Air Force Local Registration Authorities (LRA) are required to complete the AFPKI self-assessment and submit to their designated AF Registration Authority (RA), annually. In utilizing ECM for PKI Audits, results will be automatically available to the designated RA. Mandatory use of EPRM is currently being updated as a requirement in AFMAN 17-1301.
--IAW various DoD, National Security Systems (NSS) and Federal PKI guidance, the DoD PKI Audit process provides a level of assurance that each DoD Certificate Management Authority (CMA) site is configured and operated in conformance with the relevant DoD and NSS certificate policy (CP) documents, current policy including (DoDCP), and DOD Key Recovery Policy (DoDKRP).

-CAM
--The EPRM Command Cyber Readiness Inspection (CCRI) Assessment Module (CAM) enables the USAF cyber community, as well as DoD Services and Agencies, to be inspection-ready at all times via access to a self-managed tool that feeds the following processes:
--The online DODIN Inspection Scoping Workbook (ISW) in EPRM will exist as the official tool of record for elements of the CCRI phase 2 pre-inspection and scoping process.
--The assessment capability within EPRM will utilize elements of CCRI phase 3 and present standardized checklists that guide a CCRI team or installation-level POC through a pre-CCRI, self-assessment.
--The continuous monitoring capability within EPRM will utilize elements of CCRI phase 4 and allow installation-level POCs or assessment teams to create a Plan of Action & Milestones (POA&M) following self-inspection.
--Service/Agency senior leadership and CCRI Team leads will have read only visibility into the pre-inspection and scoping process in EPRM, with the potential for visibility into the self-assessment and monitoring processes, as needed.

Interagency Security Committee (ISC)
The Department of Homeland Security (DHS) Interagency Security Committee (ISC) has certified EPRM as the first DoD-sponsored tool for risk assessments and analysis of off-base/non-military site federal facilities throughout the U.S. EPRM administers the ISC Risk Management Process (RMP) and presents results in one simple analysis, identifying areas of wasted resources that can be applied to unmitigated risks.

Operations Security (OPSEC)
The OPSEC Module is designed with the principles of the OPSEC process in mind – to systematically identify, control, and protect critical information. The purpose of the module is to

automate OPSEC assessments and allow senior leaders to receive trend analysis across the enterprise. The module consists of 90 countermeasure questions comprised of several categories, such as communications, critical information, operations, and program management. It is in DoD policy that all DoD missions, functions, programs, and activities be protected by an OPSEC program that implements DoD Manual 5205.02. OPSEC assessments are required to be conducted annually by the end of the fiscal year in accordance with DoD Manual 5205.02.

EPRM HELP
User guides and help videos are available on the EPRM Help page:
https://eprmhelp.countermeasures.com/

To contact the User Support team
Email, NIPR: eprmhelp@hii-tsd.com or raleigh.onks.ctr@us.af.mil
Email, SIPR: raleigh.a.onks.ctr@mail.smil.mil

EPRM User Support Team
CTR – HII