

2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | “Cyber Hygiene”

PMO Information System Security Working Group ISSWG

Date: October 20, 2020



Federal Aviation
Administration



PMO ISSWG

- **Mission statement defined in the Charter:**

Purpose of the ISSWG

- *Create a collaborative environment to discuss security-related Risk, Issues and Opportunities (RIO).*
- *Collectively update the members on changes in Cybersecurity Federal Requirements and FAA requirements.*
- *Communicate and foster best practices among the AJM programs by sharing lessons learned.*
- *Develop guidelines for reviewing program requirement specifications to ensure consistency and completeness in contracts regarding Information System security matters.*
- *Provide a joint consistent liaison to the Authorizing Official's Designated Representative (AODR) for enhanced communication.*
- *Provide continuous input and feedback to the ISSE framework development process.*
- *Provide System Owners with consistent up to date security information for their respective programs.*
- *Provide a focal point for the AODR to prioritize funding*

***Formed in Dec. 2019 by the PMO Leadership and Directors,
acknowledged by the Signing of the Charter***



PMO ISSWG Functional Area of Responsibility

- Information System Security Engineering Working Group
- Presentation on the KSN – Working Group Starter Kit

Information Systems Security Engineering (ISSE) Starter Kit (January 2020)

Purpose: *The ISSE Starter Kit is a resource that consolidates many of the tools, training, Orders, and templates for quick reference to facilitate streamlined consistent processes in the PMO. The Starter Kit will be of use to PMO ISSE's as well as System Owners. It will assist PMO Program Managers in understanding the ISS requirements applicable to their programs and the processes and funding needed to fulfill those requirements. The ISSE Starter Kit is a single document containing material and links to key material.*

ISSE Framework

System Security Engineering Work in the PMO crosses all AMS stages. Establishment of the ISSE Framework ensures facilitation of a consistent and efficient method to perform this work.

The PMO ISSE Framework is a set of processes, products, and clearly defined ISSE responsibilities designed to achieve a targeted set of security outcomes for the PMO and the ATO.

History of the ISSE Framework:

The ISSE Working Group Charter outlines the objectives, scope and key characteristics of the PMO ISSE Framework.

[ISSWG Charter](#)

[IT Briefing Dec 12 5 2019](#)

[Roles and Responsibilities:](#)

[ISSE Roles & Responsibilities](#)

[ISSE Recommended Training Orientation](#)

[Communication Plan](#)

[FAA Lifecycle Management Process Flowchart](#)

Standard Operating Procedures:

System acquisitions require ISSE analyses in order to meet JRC milestones in the AMS lifecycle. Requirements for ISSE analysis depend on the particular type of program. FISMA, FIPS-199, FIPS-200 and NIST SP800-53 establish the key security requirements. The SOP provides an AMS phase-by-phase overview of best practices.

Link: SOP

The SOP contains specific templates and "How to" for the following ISSE activities:

- How to Process and document an NCO alert
- How to document a program that is Not Applicable (NA) for the JRC
- How to Request Funding for POAM mitigation and document results
- How to review guidelines for reviewing PRD's and Specifications.
- How to review Contract SOWs and ensure standardized contract language is incorporated.
- How to for ISS assessment guidelines for FIP's 199 categorization
- How to dispute a FIPS 199 categorization
- How to for Supply Chain Risk Security guidelines contract language
- How to review a Configuration Change Request for Security impacts via Web CM.
- How to integrate a security issue into the PMO RIO process
- How to utilize the AODR templates for Security Documents



1

PMO ISSWG Functional Area of Responsibility

- Review the key deliverables and share their value.
 - Charter
 - Communication Plan
 - Roles and Responsibilities
 - Training Orientation (lists of many free courses in Cyber Security)
 - Review of general “How to’s”

