FAA Cybersecurity Threat Model: Status, Results and Model Composition

NextGEN

ANG The Future of the NAS Starts Here

Presented at REDAC
Presented by Kelly Mesveskas
ANG-B31

FAA

November 14, 2018

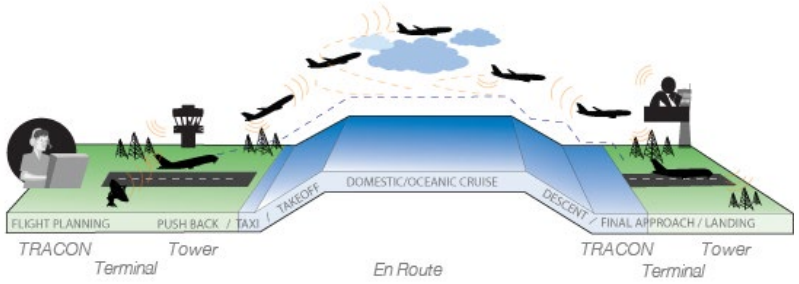
The FAA Cybersecurity Risk Model (CyRM)

- **What is the FAA Cybersecurity Risk Model?**
  - The CyRM identifies a framework for assessing cyber risk that will be integrated into the FAA through the use of end-to-end analysis. This analysis provides a more realistic and holistic understanding of cyber threats, risks, and vulnerabilities to the FAA. The analysis will also help the FAA to identify the potential impact in meeting mission objectives.
  - The FAA CyRM Builds upon the existing system level security certifications information and processes (i.e., formerly the SCAP process) fuses information together and performs a holistic review of what it takes for the FAA to continue to deliver services.
    - End-to-end review of all systems involved in providing a service
    - Creates a better understanding of risk and potential impacts
  - The CyRM does not replace the existing Security Authorization Process which will remain as the cornerstone to ensure system level compliance with NIST 800.53
  - Add use of the FAA Cybersecurity Risk Model
    - Identifies the potential of new threats, vulnerabilities, impacts and identifies any changes to the likelihood of impacts brought by the changes to the underlying service can be assessed quickly
    - Provides a consistent methodology

Improved Decision-Making
Using the Cybersecurity Risk Model (CyRM)

- **Helps prioritize future planning and investments based on risk to service vs system compliance.**
  - Authorization to Operate cybersecurity compliance process continues
  - CyRM enhances and builds upon the current system compliance structure but focuses on evaluating end-to-end critical resources required to deliver the service
- **Enables a common framework to be applied across the three FAA network domains (NAS, Mission Support, and R&D)**
  - Flexible to be tailored to meet the unique requirements within each domain
  - Repeatable process
  - Enables Enterprise integration
- **Provides a way to prioritize cybersecurity testing**
  - Testing provides quantifiable results that confirm the threat and risk.
  - Use cases or scenarios recreate a portion or the entire service thread to test the effectiveness of pertinent security controls
  - Can help measure the effectiveness of security controls

FAA Mission
Safety and Efficiency
Mission supported by five Mission Essential Functions:



Operational Capabilities

MEF 1: Provide Air Navigation Service (ANS)

MEF 2: Use ANS for National Defense

MEF 3: Provide Certification of Airports

MEF 4: Provide Aviation Regulatory Oversight

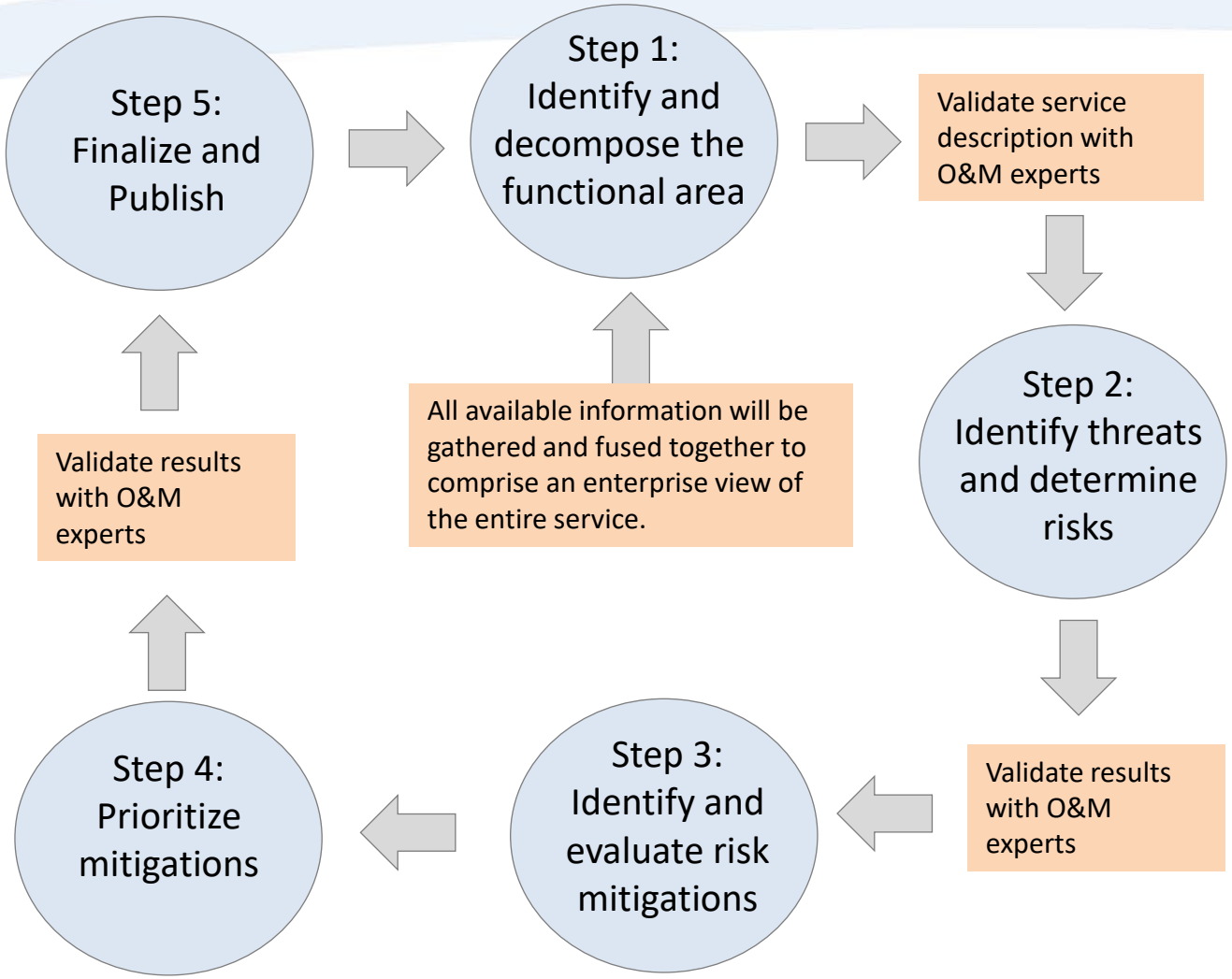
MEF 5: Facilitate Civil Reserve Air Fleet (CRAF)

FAA

NextGEN

ANG The Future of the NAS Starts Here

Five Basic Step in the Service Thread Evaluation.

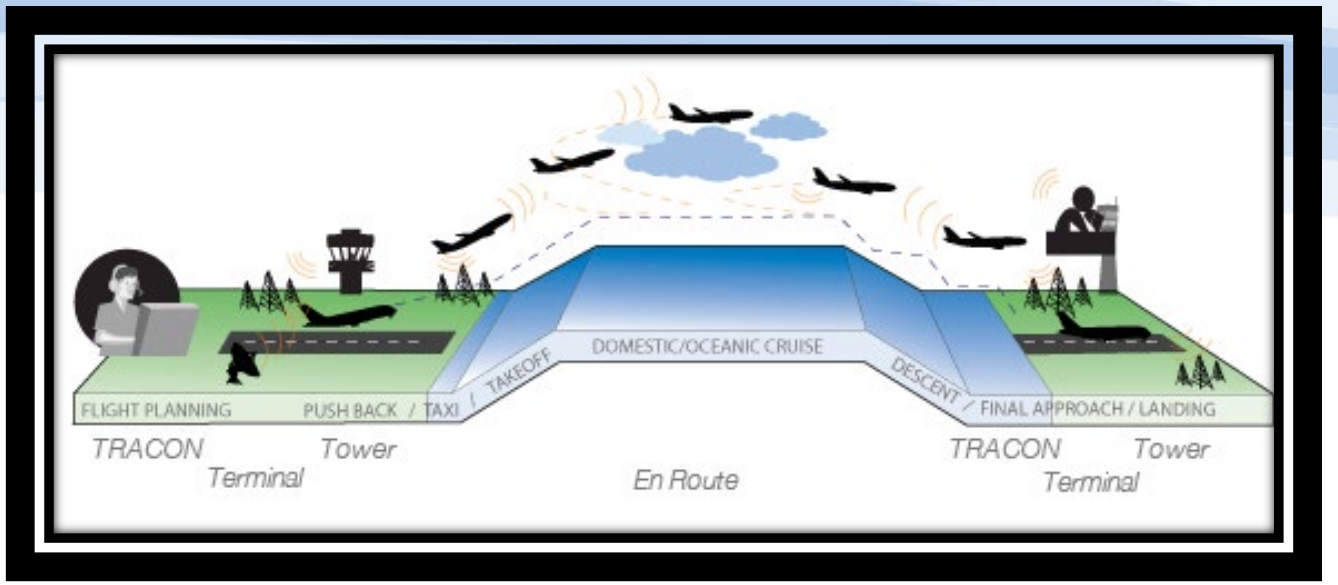


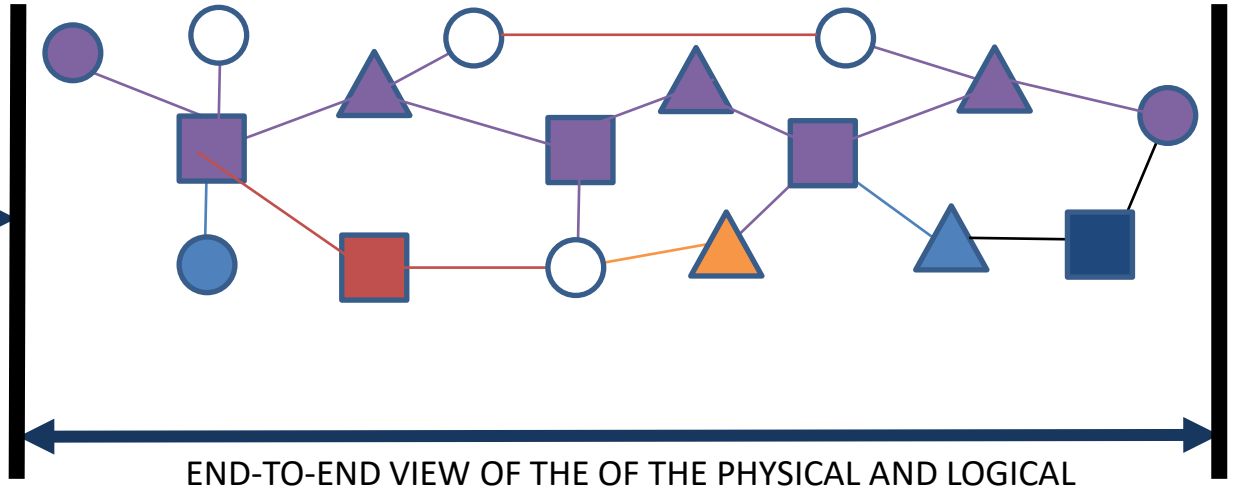
FAA Mission Essential Function 1

Mission Essential Functions

- Separation Assurance
- Traffic Management Synchronization
- Navigation
- Traffic Management Strategic Flow
- **Flight Planning**
- **Airspace Management**
- **Air Traffic Control Advisory Services**
- **Emergency and Alerting**
- **Government Agency Support**

Mission Level Service Thread (MLST)





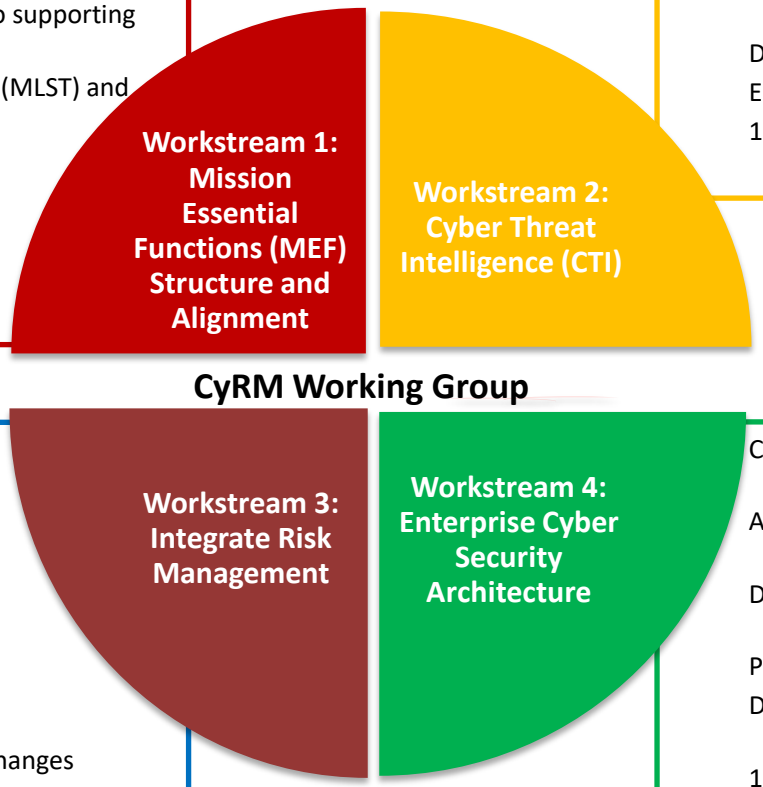
END-TO-END VIEW OF THE OF THE PHYSICAL AND LOGICAL INTERDEPENDENCIES OF RESOURCES (LEASED SERVICES, SYSTEMS, COMPONENTS) REQUIRED TO MEET THE MISSION OBJECTIVES

- INFRASTRUCTURE
- SYSTEMS & LEASED SERVICES
- COMPONENTS

NextGEN ANG The Future of the NAS Starts Here

CyRM Focus Areas

Support Order 1910.1 COOP update by providing business function decompositions to supporting systems
Diagram Mission Level Service Threads (MLST) and Cybersecurity protection
Analyze threats and provide risk models for selected MLSTs
Recommend common controls
18S24D1-T1, 18S24D1-T2
18S.24A50-T1, 18S.24A50-T2



Develop FAA-wide Cyber Threat Intelligence (CTI) process description
Develop CTI analyst role descriptions
Ensure CTI process and product sustainment
18S24D2-T1, 18S24D2-T2

Identify FAA policies & guidance affected by CyRM, CTI or ECA or cybersecurity requirements
Provide change requests to policy & guidance owners to embed cybersecurity, CyRM, CTI or ECA appropriately
Ensure change requests include how to maintain changes as cybersecurity changes
- 18S24D3-T1

Complete definition of attributes of current state ECA
Add metadata to meet EA and FISMA requirements
Define Target state of ECA from Cybersecurity Strategy, 2016-2021 and investments
Populate ECA with cybersecurity assets
Develop ECA Repository & Visualization toolset requirements
18S24D4-T1
18S24C20-T3

Questions?