



Federal Aviation
Administration

FENS Program Technical Interchange Meeting (TIM) FISMA High Discussion

June 21, 2018

NAS First

People Always

Scope of Discussion



- FAA will address questions surrounding FENS
Categorized as FISMA High, including:
 - Shared Infrastructure
 - FAA Auditing Requirements
- Questions about the Network, Components, FAA Domains, SWIM or other Technologies will not be addressed

Why FISMA High?



- The FAA NAS Infrastructure was identified as Critical Infrastructure by Presidential Policy Directive 21
- In response to IG and GAO Audits, ATO revalidated NAS systems to ensure appropriate FIPS 199 categorization
- FIPS 199 impact categories are high, moderate and low based on the following:
 - Harm to Individuals
 - Financial Loss
 - Damage to Organizational Assets
 - Degradation or Loss of Mission Capability
- FENS is considered a Safety-Critical system and is High for Integrity and Availability and Moderate for Confidentiality

Shared Infrastructure



- Network infrastructure and services that are dedicated to FAA operations and facilities must meet ATO-Tailored High security controls
- Network infrastructure and services that are not dedicated to only FAA use are considered “shared” and will require tailoring of both the ATO High security controls that must be met and FAA Security Authorization methods
- Dedicated and shared infrastructure will be expected to meet the performance requirements for availability and integrity

FAA Auditing Requirements



- All FAA contracted systems/services that operate at OSI layer 2 and above are considered to be Information Systems for which FAA has FISMA responsibility
- FAA security control requirements are written assuming system/service assets are dedicated to FAA use
- When non-dedicated assets (e.g. shared layer 2 and above transport) are approved for use, an alternative means of Information Assurance is needed to meet the FAA's due diligence requirements
 - The alternate method of assurance will be based on the proposed architecture and services being provided
 - FAA will assess its security control requirements and recommend a set of tailored controls based on the shared infrastructure and services proposed
 - It is assumed that some level of FAA risk assessment of the shared infrastructure will be required to obtain sufficient assurance to support the Authorization to Operate

Summary



- FENS is considered a Safety-Critical system and is High for Integrity and Availability and Moderate for Confidentiality
- Network infrastructure and services that are dedicated to FAA operations and facilities must meet ATO-tailored High security controls
- Non-dedicated network infrastructure and services will have an alternative means of Information Assurance to meet the FAA's due diligence requirements
- The FAA will conduct some level of a risk assessment of the shared infrastructure to obtain sufficient assurance to support the Authorization to Operate
- Dedicated and shared infrastructure will be expected to meet the performance requirements for availability and integrity