

Next**GEN**

# V & V of Enterprise Safety and Information Security

Presented to 9th Annual Verification & Validation Summit  
September 17-18, 2014

James Daum

Safety and Information Security Division Mgr, ANG-B3  
NAS Systems Engineering



**FAA**

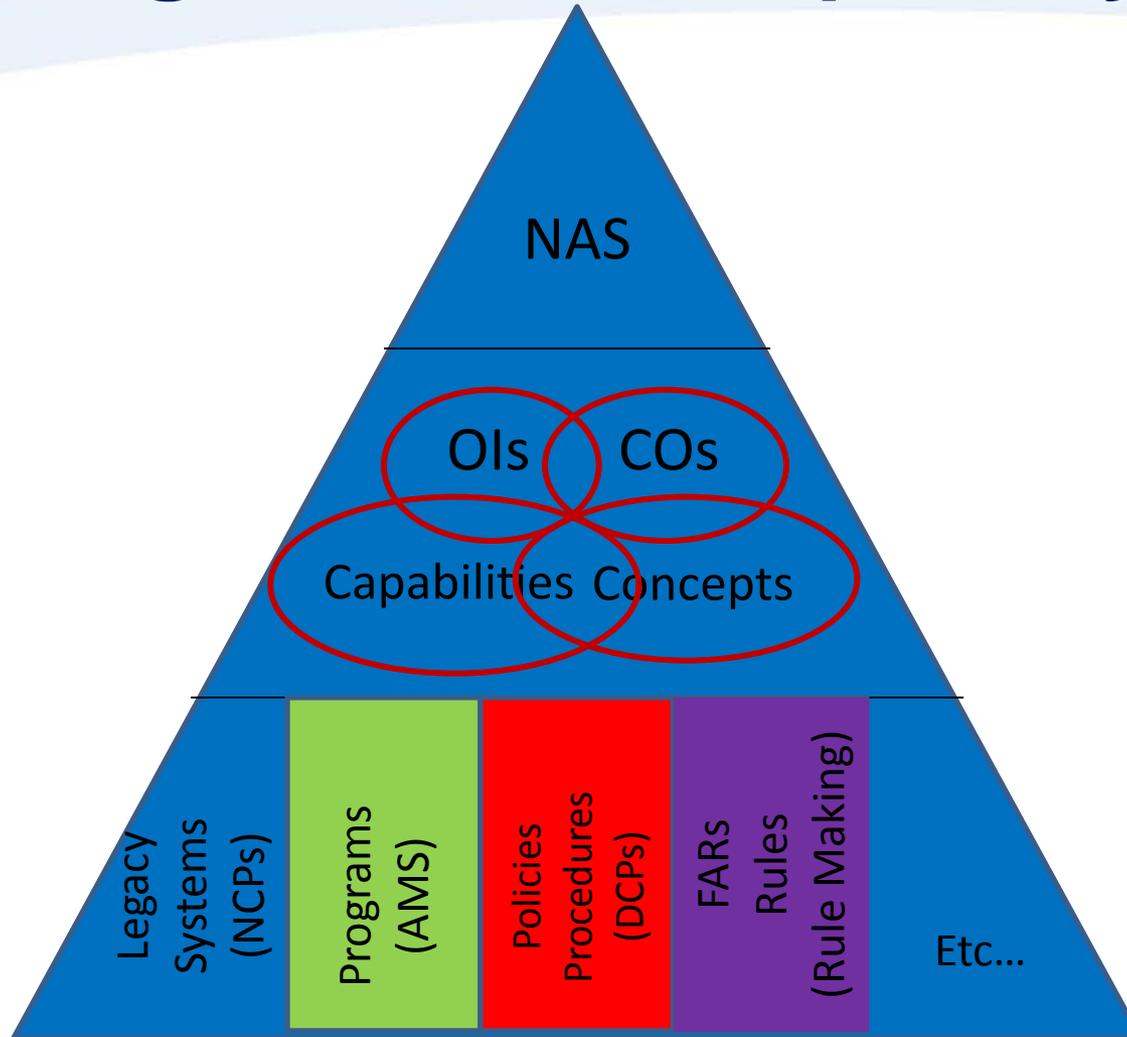
# My Lesson in V&V



# Current State

- Implementation of The Safety Management System has increased the awareness of SRM
- AMS requirements for SRMDs have improved the identification of hazards and the mitigations that have the potential to reduce safety risk
- With few exceptions SRMDs become “shelf ware” that have limited effect on reducing NAS safety risk
- Traceability of safety requirements to SRMDs is required to conduct V&V that results in accurate assessment of system residual risk
- Automation is required to provide associative links and relationships to V&V Enterprise Requirements

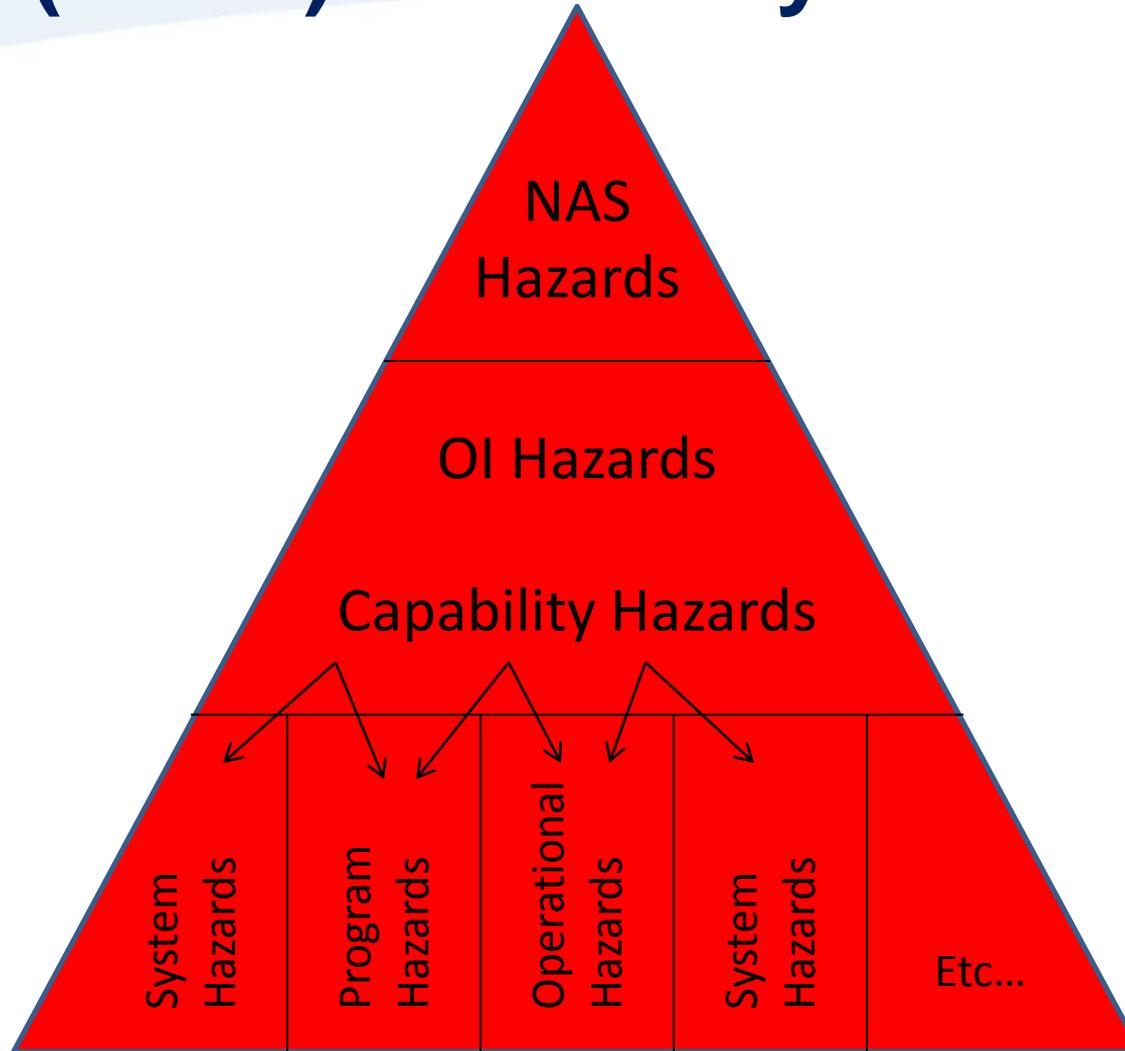
# Integrated NAS Capability



**FAA**

Next**GEN**

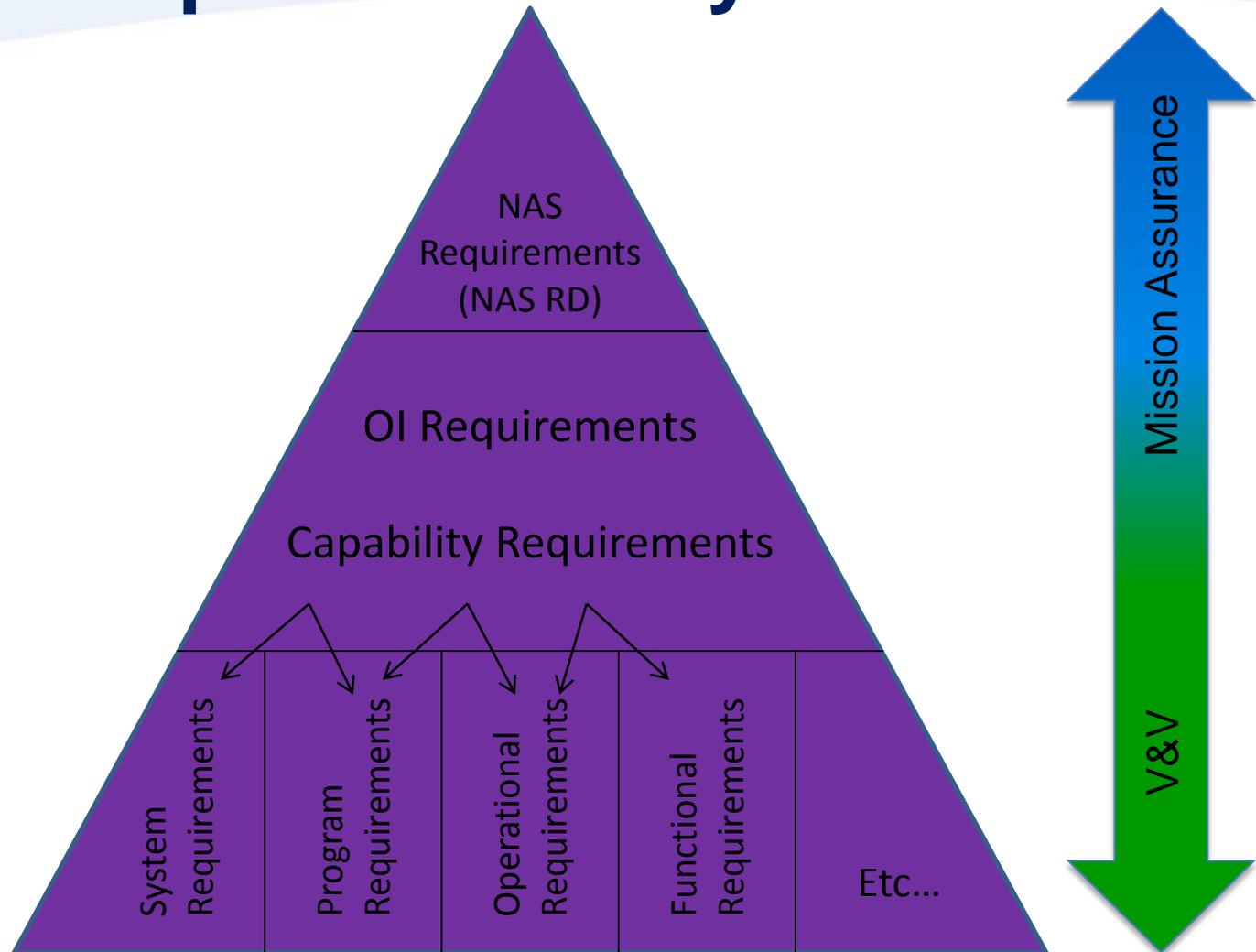
# Integrated Safety Risk Management (ISRM) Hazard Pyramid



**FAA**

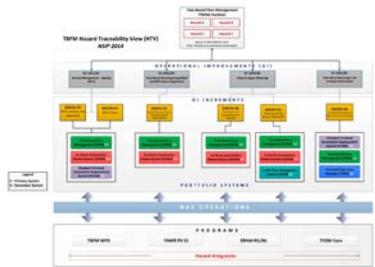
Next**GEN**

# Integrated Safety Risk Management Requirements Pyramid





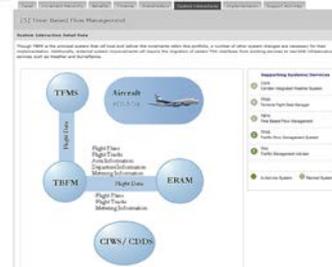
# Integrated Safety in a Complex NAS



Vertical HTVs



EA



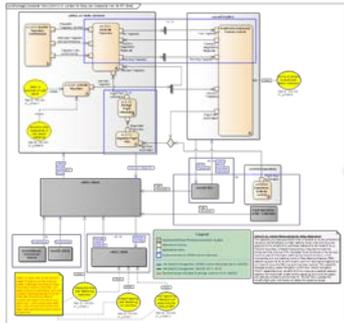
NPE



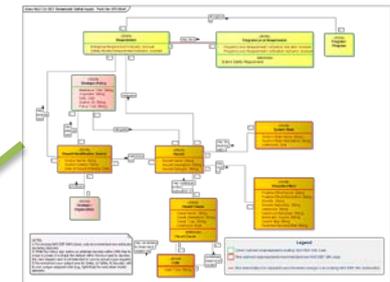
NSIP



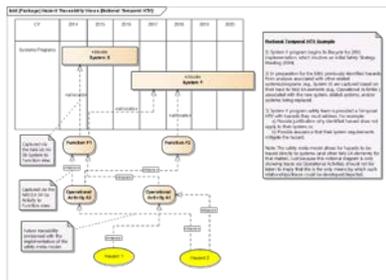
**ISRM**



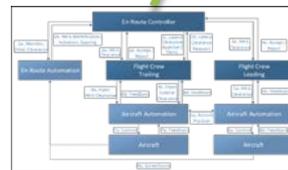
Horizontal HTVs



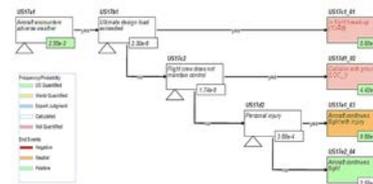
EA Meta-Model



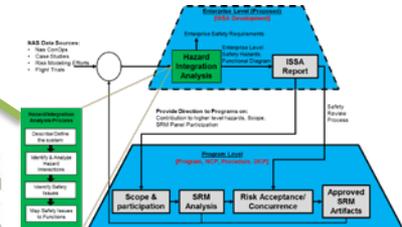
Temporal HTVs



HESRA



ISAM



ISSAs



# Enhanced EA Safety Products

## Safety Meta-Model:

- Establishes needed relationship between NAS EA elements and safety data.
- NAS EA is central to supporting integrated SRM.
- Safety Meta-Model implementation/instantiation is key to developing HTVs.

## Hazard Traceability View (HTV):

- System safety tool to graphically depict hazard information to stakeholders as input to planned safety analysis efforts.
- Conveys identified safety issues across associative, dependent, and/or interacting systems that may eventually be categorized as hazards.

Conveys potential gaps in safety analysis by integrating across three planes:

Vertical – Hierarchical. Enterprise level system-of-systems safety risk and requirements allocated down to programs.

Horizontal – Across organizations, programs, systems, and functions.

Temporal – Across program/system implementation timelines.



# Enhanced EA Safety Products

## Integrated System Safety Assessment (ISSA):

- A broad look at safety issues to ensure Integrated Safety Risk Management (ISRM) accountability within system acquisitions as well as other planned NAS changes
- Early and iterative identification of cross-organizational safety hazards at all implementation levels
- Improves the ability to manage, minimize or eliminate safety risk, strengthening the overall safety process for system acquisitions as well as for other planned NAS changes (e.g. procedural or rule-making)
- Basis for Administrator's Strategic Initiative of Risk Based Decision Making (RBDM) for Planned Changes





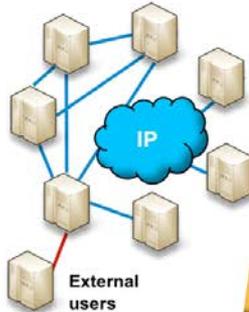
# V&V for Enterprise Safety

- Hazards that effect integrated capabilities must be mitigated via enterprise safety requirements are allocated to multiple systems, services, and operations
- Traceability of allocated requirements is necessary to be able to V&V enterprise requirements (Hazard to Performance)
- Techniques and processes are needed to V & V enterprise requirements and assess the ability of the integrated capabilities to provide **mission assurance**

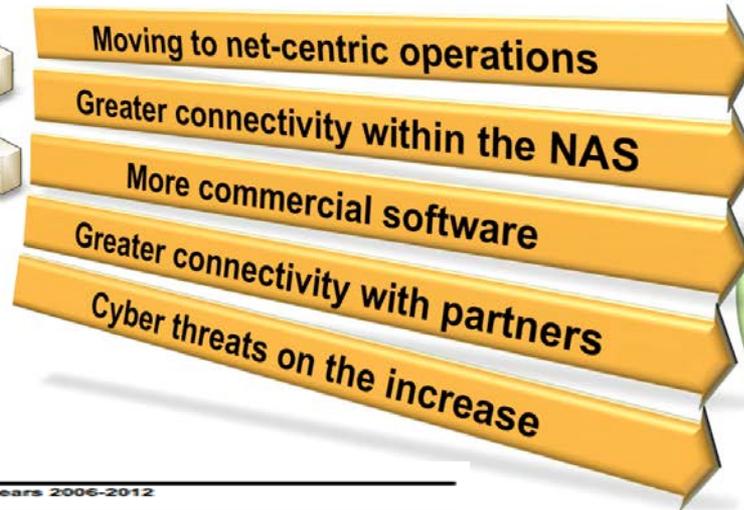
# State of NextGen Security Environment

**NextGen introduces higher cyber security risk environment to NAS**

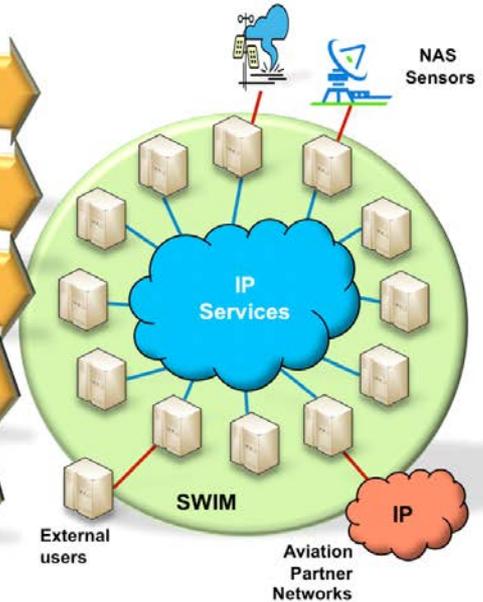
**Today's NAS**  
Limited inter-connectivity



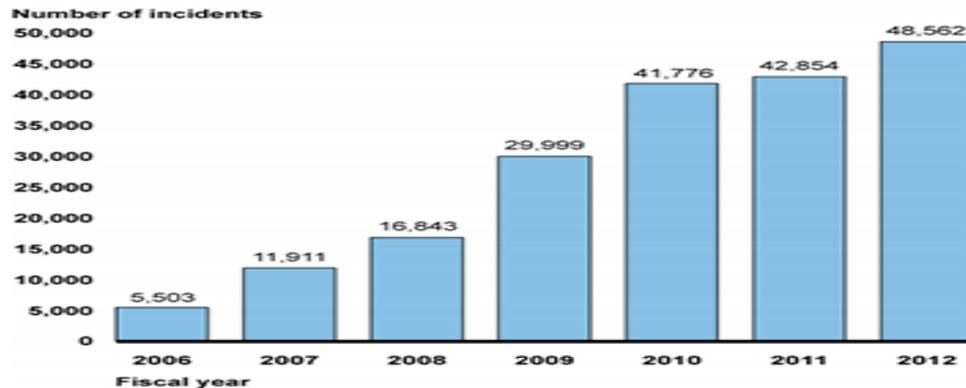
**NAS Environment is Changing**



**Tomorrow's NextGen**  
Significant inter-connectivity



Incidents Reported by Federal Agencies in Fiscal Years 2006-2012



Source: GAO analysis of US-CERT data for fiscal years 2006-2012.

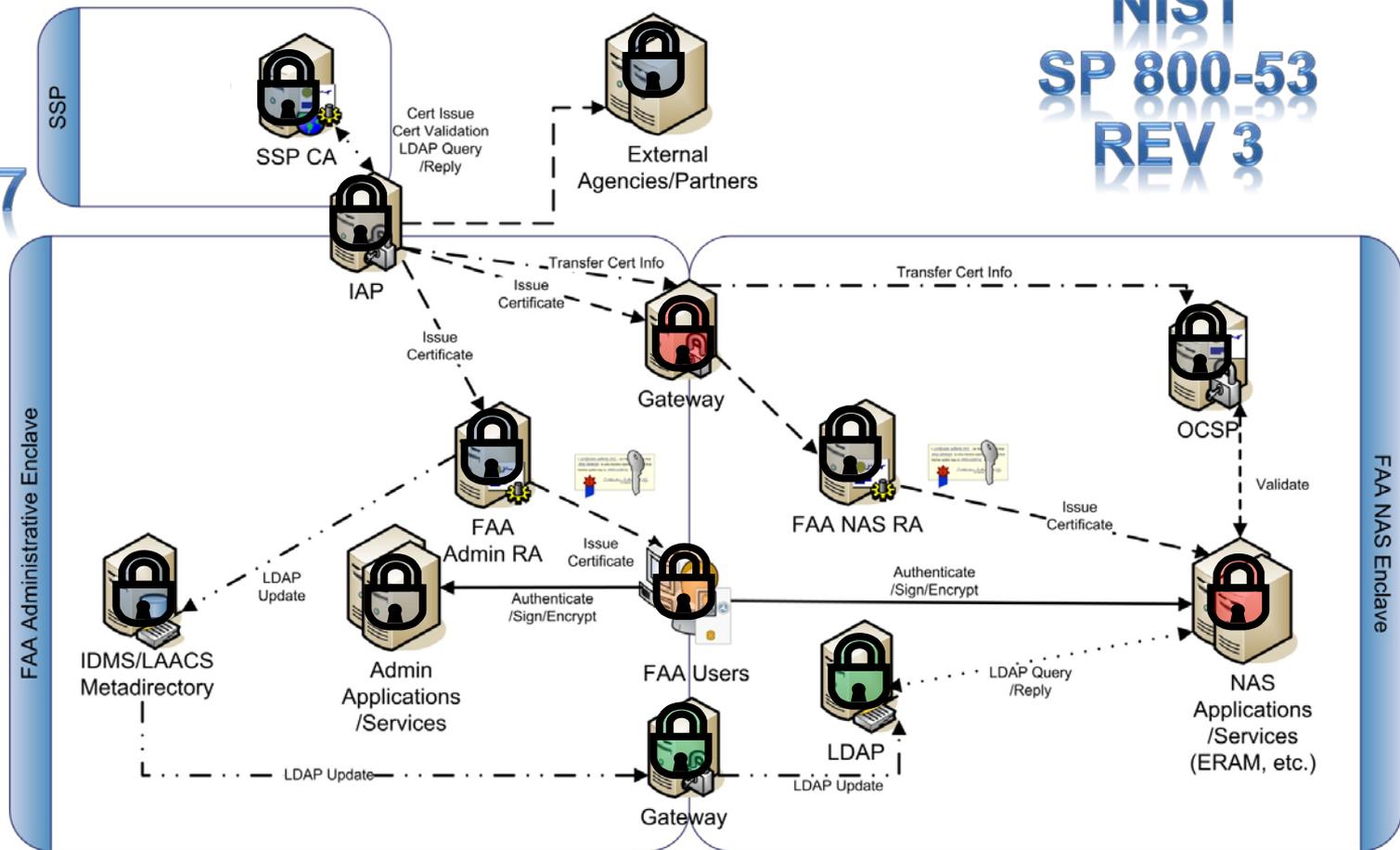
**Incident occurrence is increasing at an alarming rate**



# State of Legacy NAS Information System Security (ISS)

HSPD-7

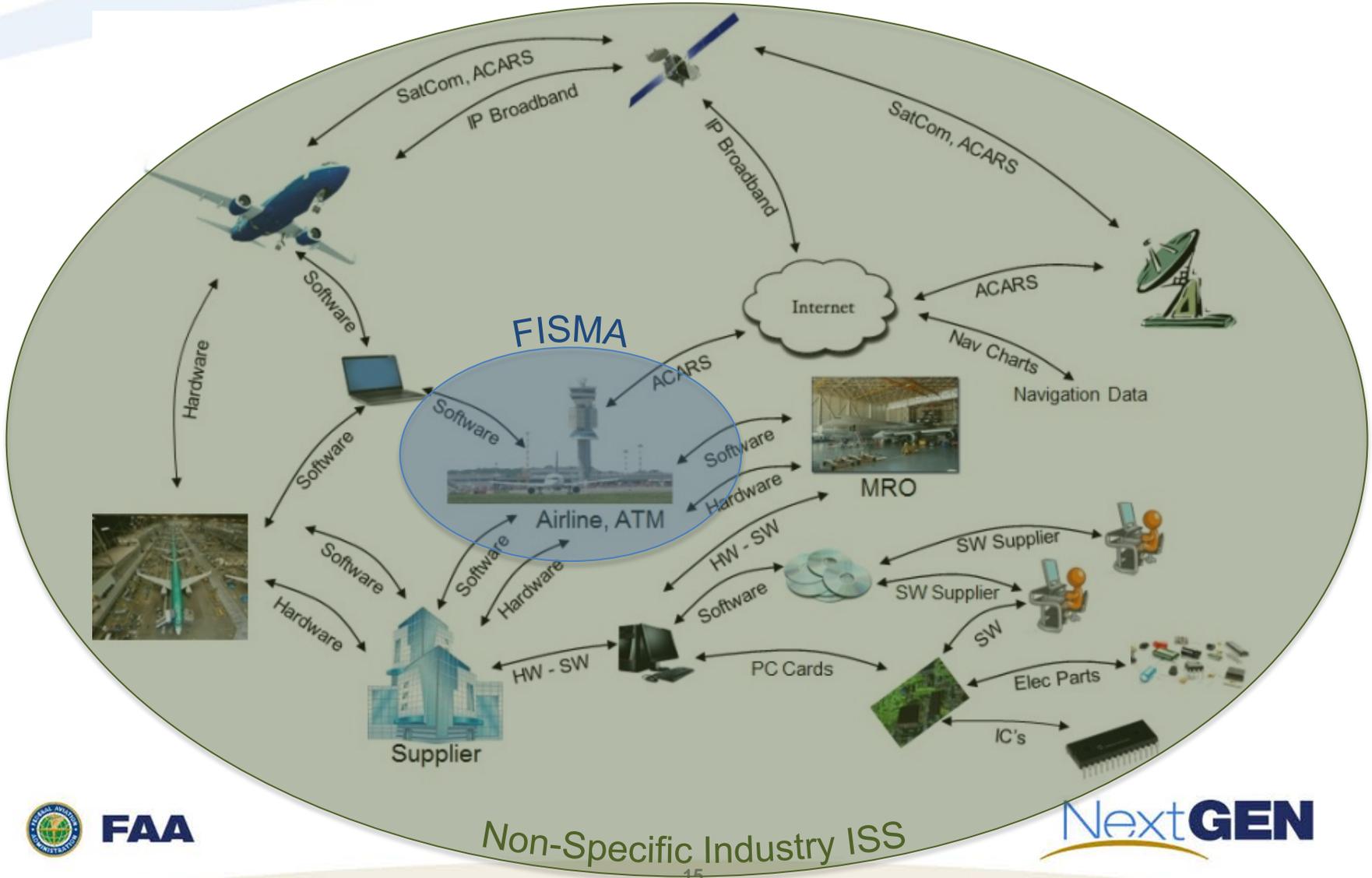
NIST  
SP 800-53  
REV 3



FISMA

NextGEN

# State of Aviation Information System Security (ISS)



# Enterprise Information System Security



FAA

NextGEN

# Enterprise ISS Architecture

IDENTIFY



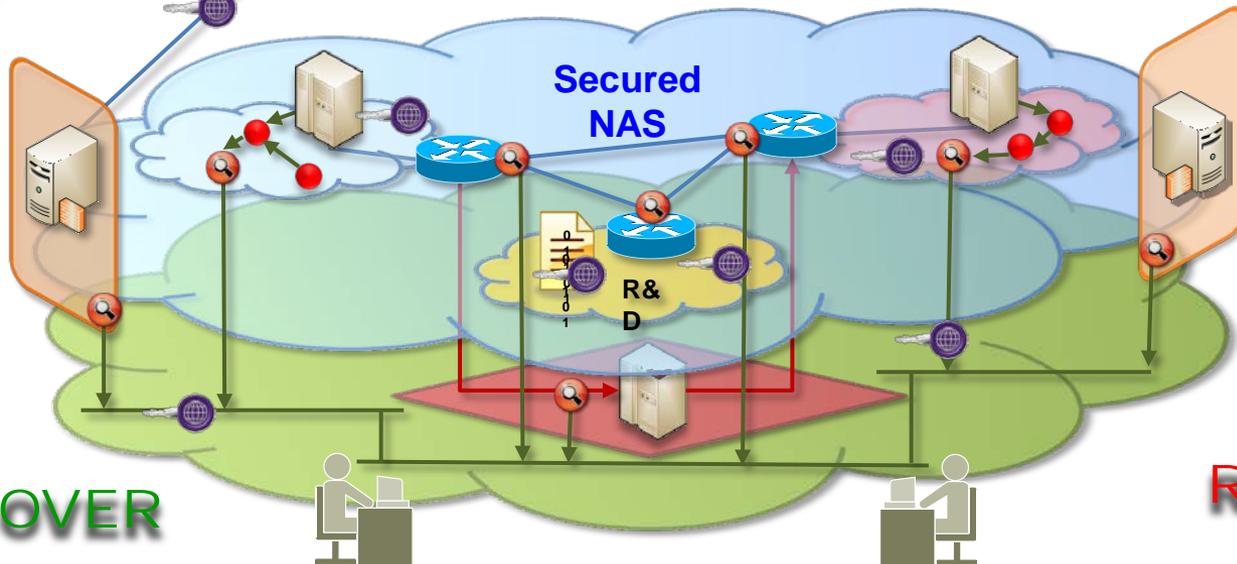
PROTECT



DETECT



(PPD)-21



EO -13636

RECOVER



RESPOND



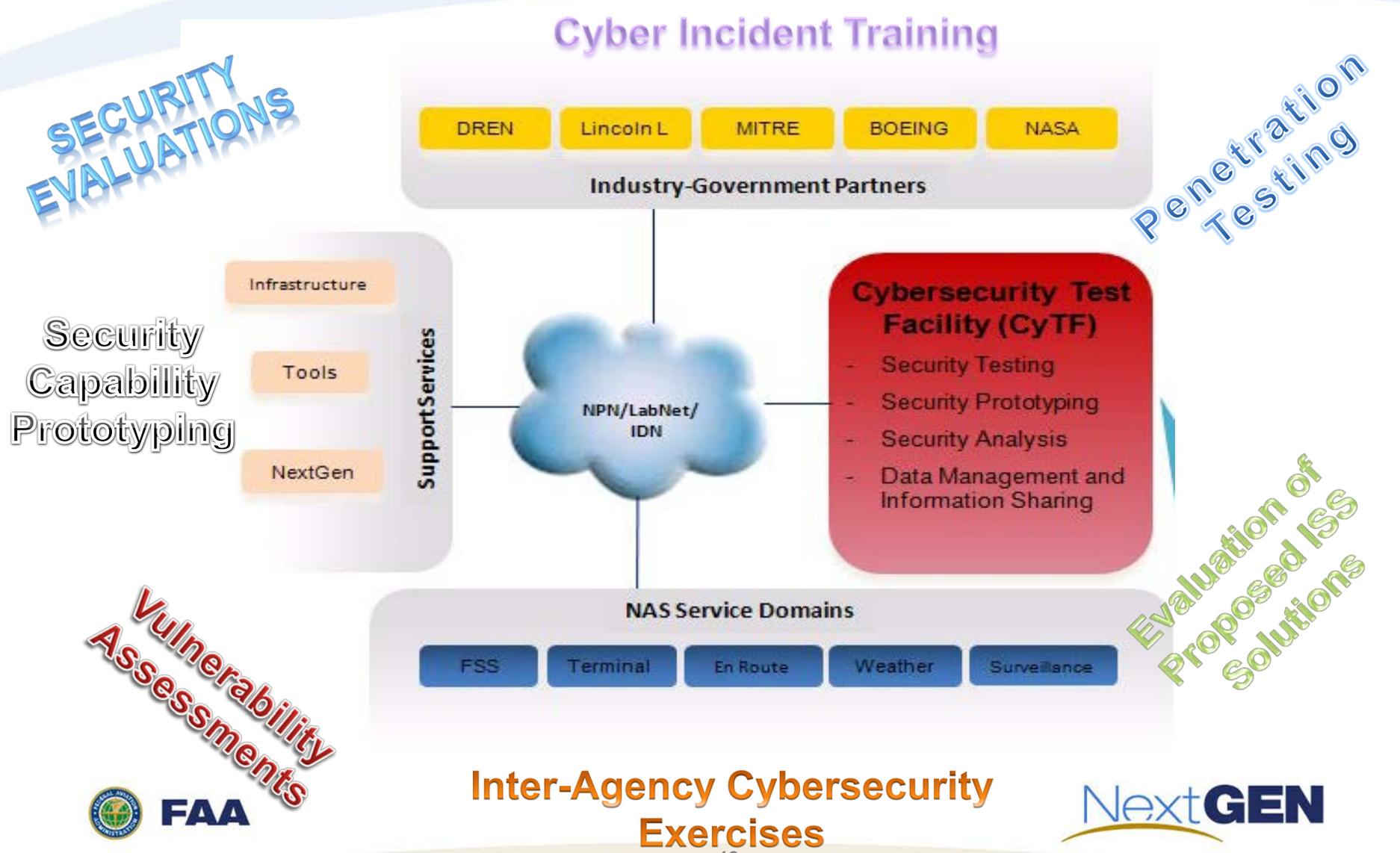
NIST  
SP 800-53  
REV 4



FAA

NextGEN

# NextGen Cyber Test Facility (CyTF)



# CyTF Objectives

- Provide security evaluation and research services strengthening NextGen information security in a Research and Development (R&D) environment
- Provide an extensible and flexible cybersecurity R&D environment to evaluate NAS enhancements
- Establish the cybersecurity test facility without effecting the availability and safety of operating NAS services
- Provide cost-effective, state-of-the-art cyber-test facility

# V&V for Enterprise Security

- Cyber security requirements are implemented as system, hybrid, or common controls
- A descriptive security architecture is needed to identify implementation of security controls and existence of security vulnerabilities
- Techniques and processes are needed to V & V security requirements and assess the resiliency and **mission assurance** of NAS Information Security

# How do we achieve success

- Continue to identify enterprise requirements and develop traceability from source of the requirements to operational performance metrics
- Collaborate to develop techniques and processes to V&V enterprise requirements and assess NAS mission assurance

## Questions:

James Daum

James.Daum@faa.gov

