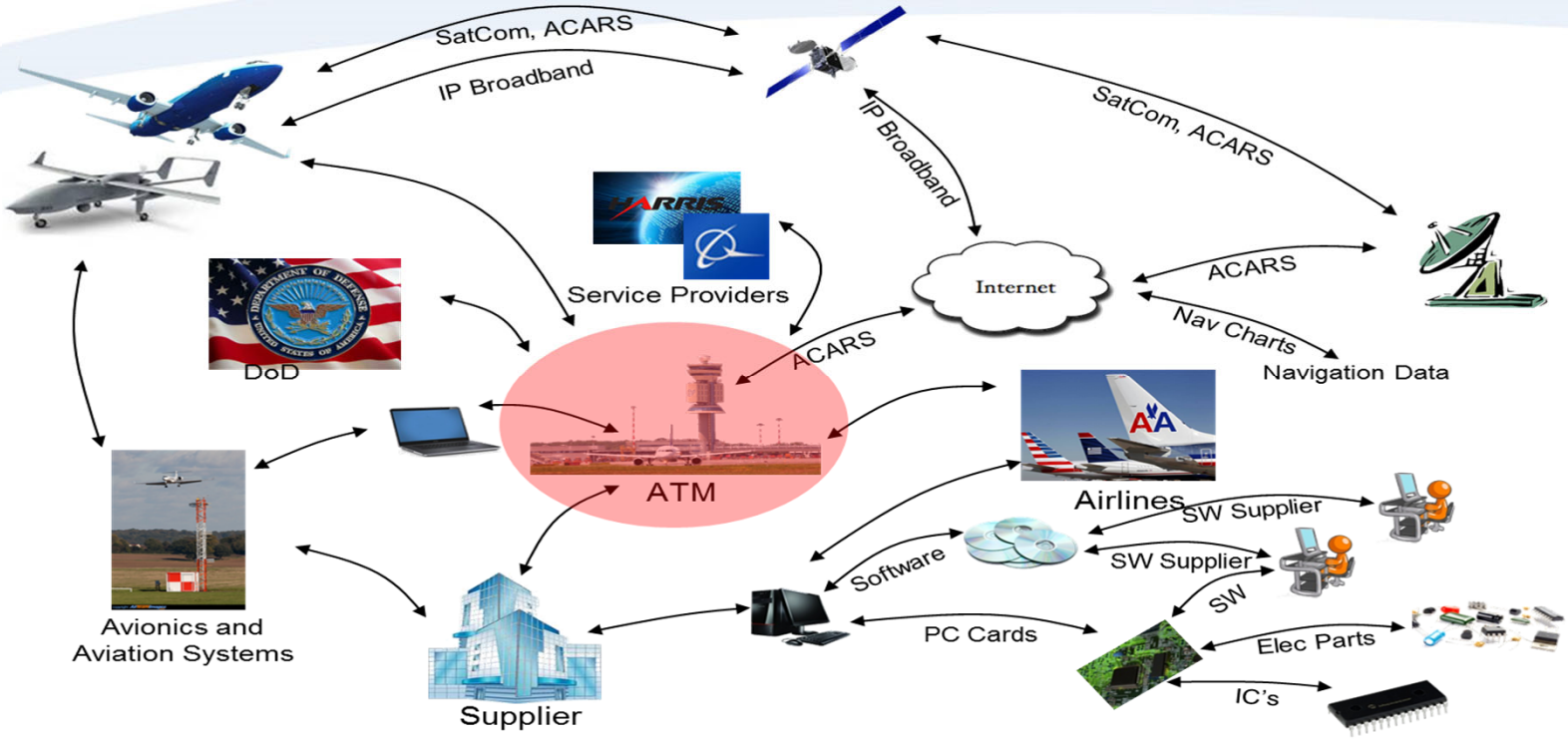

NextGEN
V&V Processes in Cybersecurity
Presented to: Validation and Verification Summit
By: Enterprise Information Security Team ANG-B31
Date: September 2016
FAA

Cyber Security and V&V

- Cybersecurity Test Facility (CyTF)
- V&V Processes for testing threats in the FAA Threat Model

Aviation Cybersecurity Environment



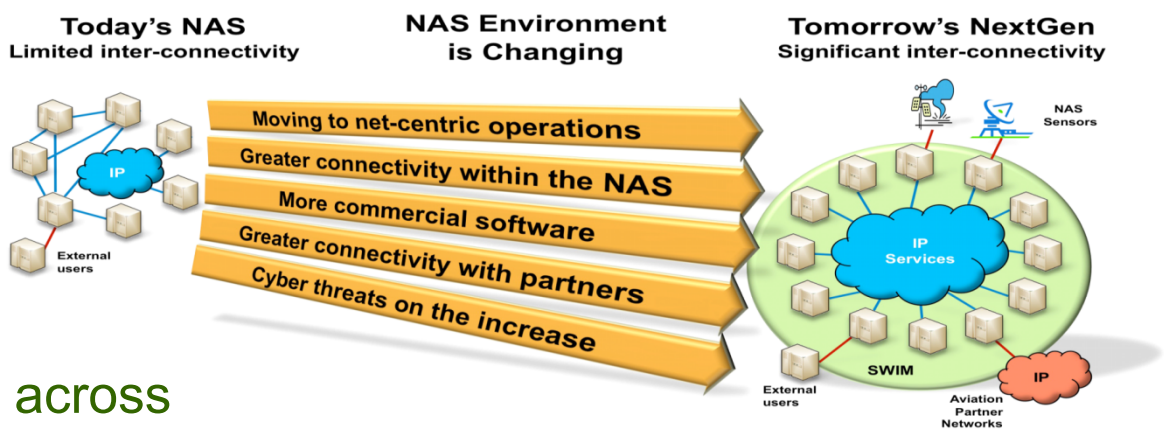
Threat includes a broad spectrum of vectors. Mitigations are not tailored for the Air Domain.

FAA

NextGEN

IT Enhancements Move NAS into a Higher Cybersecurity Risk Environment

Information sharing efficiencies increase the risk of cybersecurity vulnerabilities



Vulnerabilities can spread across internal and external partner boundaries

FAA

NextGEN

FAA Cybersecurity Test Facility (CyTF)

<u>Mission</u>: Provide cybersecurity Evaluation and research services to strengthen FAA information security in a Research and Development (R&D) environment.

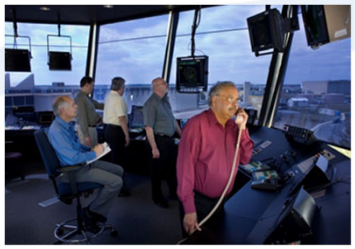
Established as a centralized agency asset utilized by all FAA domains providing a unified environment promoting the development of cybersecurity research and development , testing and training without impacting the operational networks.

- ✓ Research & Development (developing future concepts or requirements)
- ✓ Operations Support (test and prototyping solutions, organizational training)
- ✓ Programs and systems support and testing (validating security controls and solutions)
- ✓ Integrated Aviation Partner Research and Development

FAA

NextGEN

FAA Cybersecurity Test Facility (CyTF)



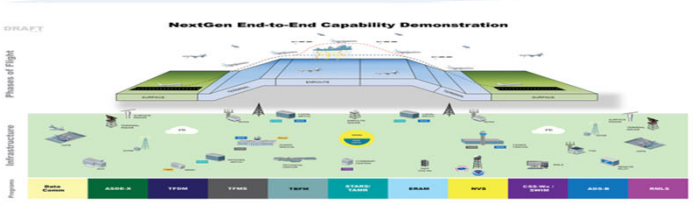
CyTF Capabilities

- Product Evaluations
- Security Capability Prototyping
- Cyber Incident Training
- Cybersecurity Exercises
- Vulnerability Assessments
- Penetration Testing
- Evaluation of Enterprise Security Solutions

FAA

NextGEN

NAS Enterprise Test Environment



Virtual NAS system

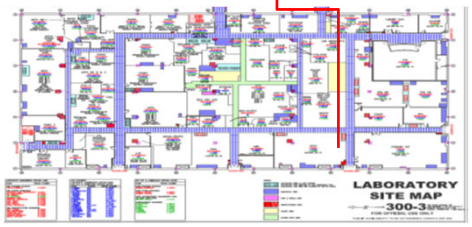
CyTF

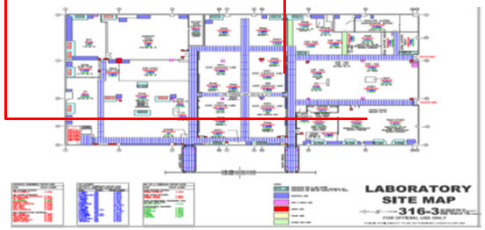
Net A

Net B

Others

R&D Networks





FAA

NextGEN

CyTF Physical Layout

MIT Lincoln Laboratory

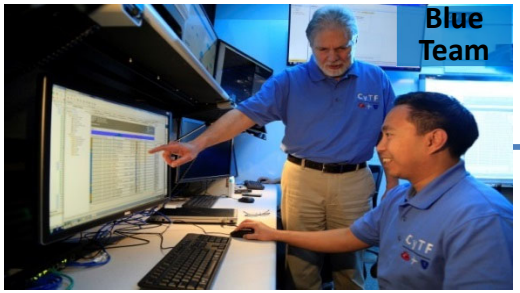
APL The Johns Hopkins University Applied Physics Laboratory

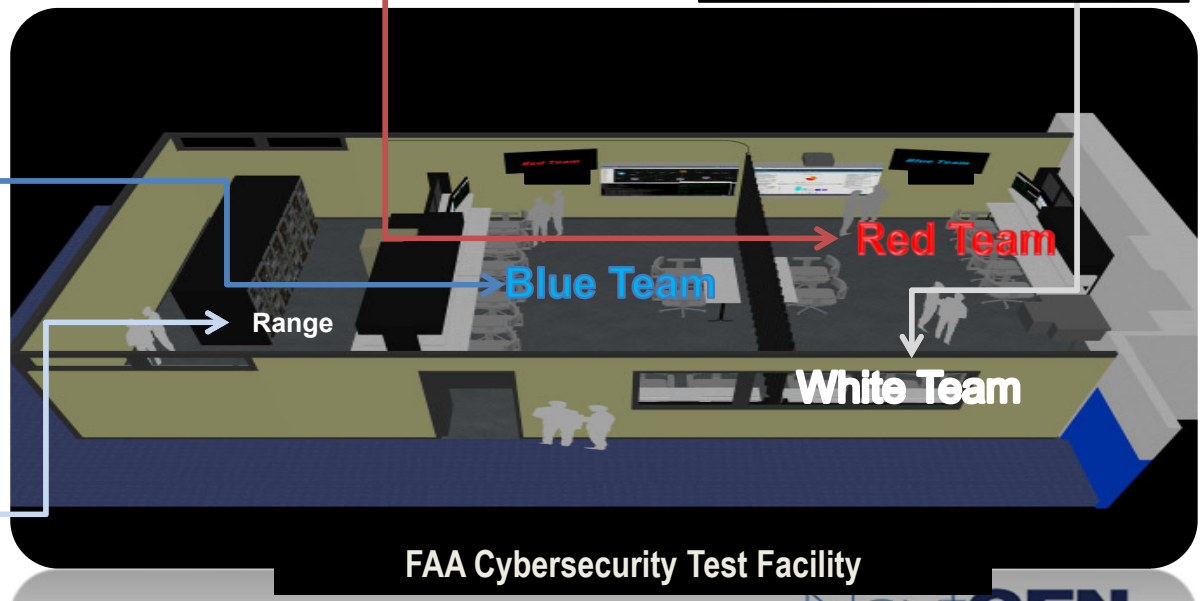
MITRE

Department of Transportation United States of America

BOEING

U.S. Department of Homeland Security





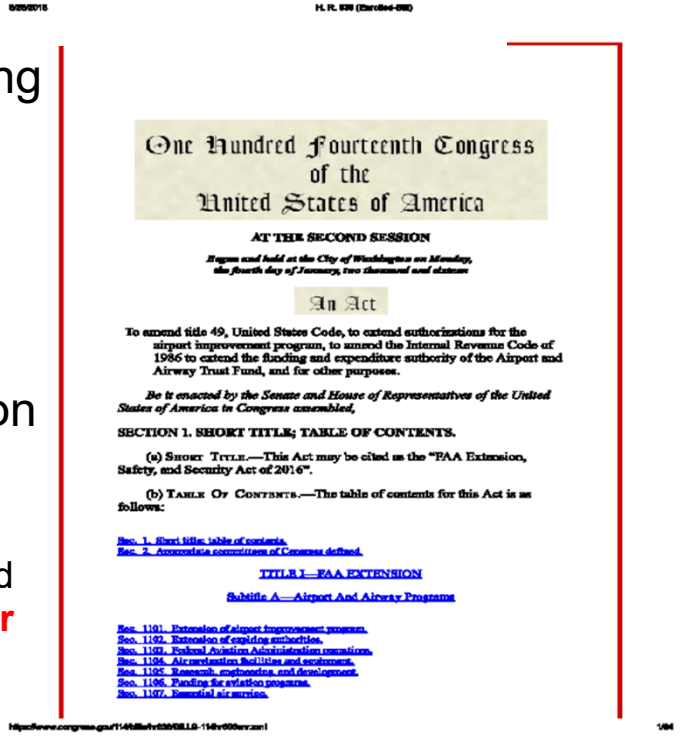
FAA

NextGEN

FAA Cybersecurity Threat Model

Threat Modeling is a structured approach for analyzing the security of an application to identify, quantify, and address the security risks associated with such application.

- July 15, 2016: President Obama signed into law H.R.636, a 14-month extension of FAA authorization
- H.R.636 mandates a Cyber Threat Model (CyTM):
  - Within 1 year, FAA must implement the 2015 GAO recommendation to assess and research the potential cost and timetable of developing and maintaining an agency-wide **cyber threat model**



One Hundred Fourteenth Congress
of the
United States of America

AT THE SECOND SESSION

An Act

To amend title 49, United States Code, to extend authorizations for the airport improvement program, to amend the Internal Revenue Code of 1986 to extend the funding and expenditure authority of the Airport and Airway Trust Fund, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "FAA Extension, Safety, and Security Act of 2016".

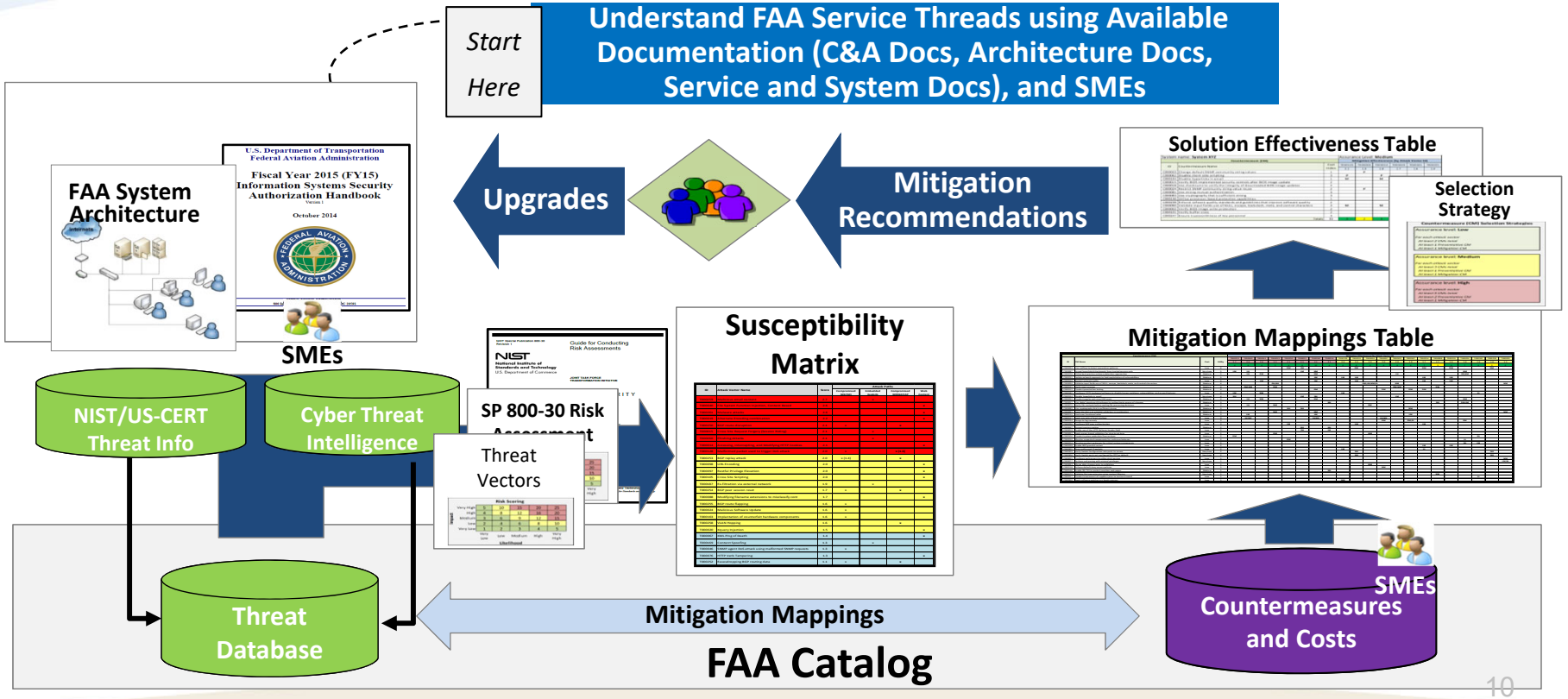
(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—FAA EXTENSION

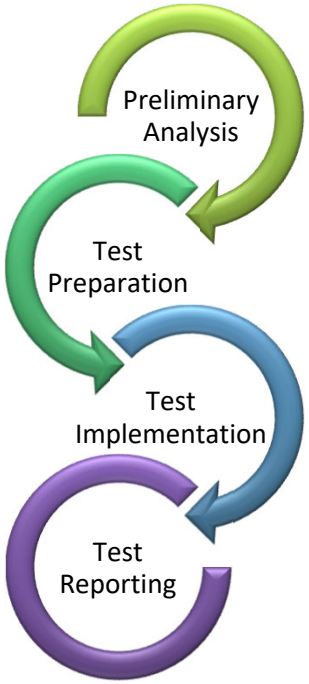
Subtitle A—Airport And Airway Programs

FAA Cybersecurity Threat Model Framework

Cyber attacks employ a wide variety of methods and seek to exploit any and all possible attack vectors



V&V Processes to Testing threats in the FAA Threat Model



- Test Objectives for service threats
- Type of Access to system(s)
- Types of threat actors
- Rules of test engagement

- Test Environment
- System resources needed
- Interface/connectivity testing
- Test plan/procedures

- Conduct test
- Provide test "Status" report

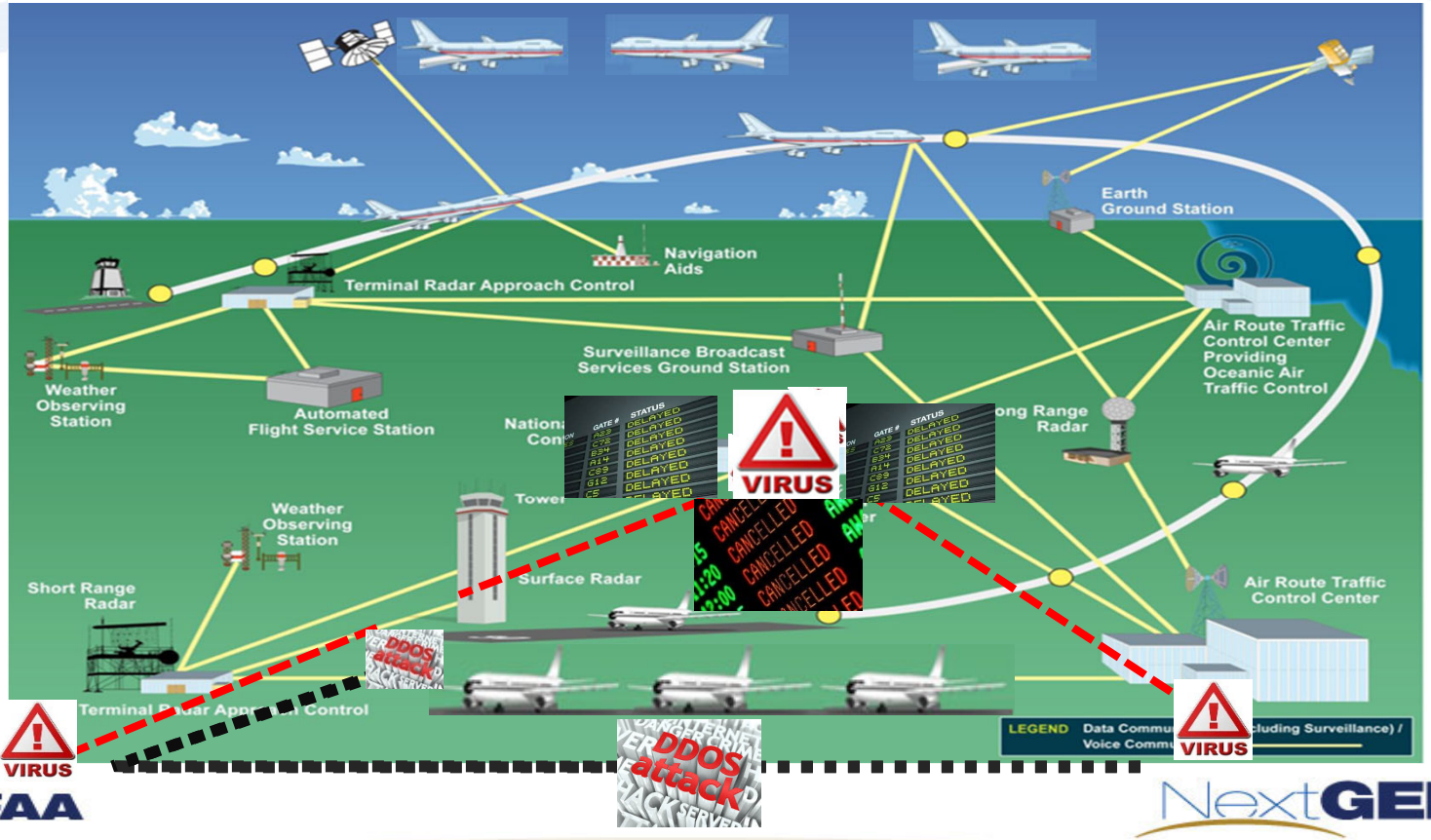
- Final test report
- Findings and recommendations

*"Communication and timely collaboration with stakeholders is **CRITICAL** for the success of Threat Modeling testing"*

FAA

NextGEN

Threat Model scenario example



Collaboration is Key

We need to continue to collaborate internally/externally to reduce FAA vulnerabilities and understand security risks accepted by our partner stakeholders