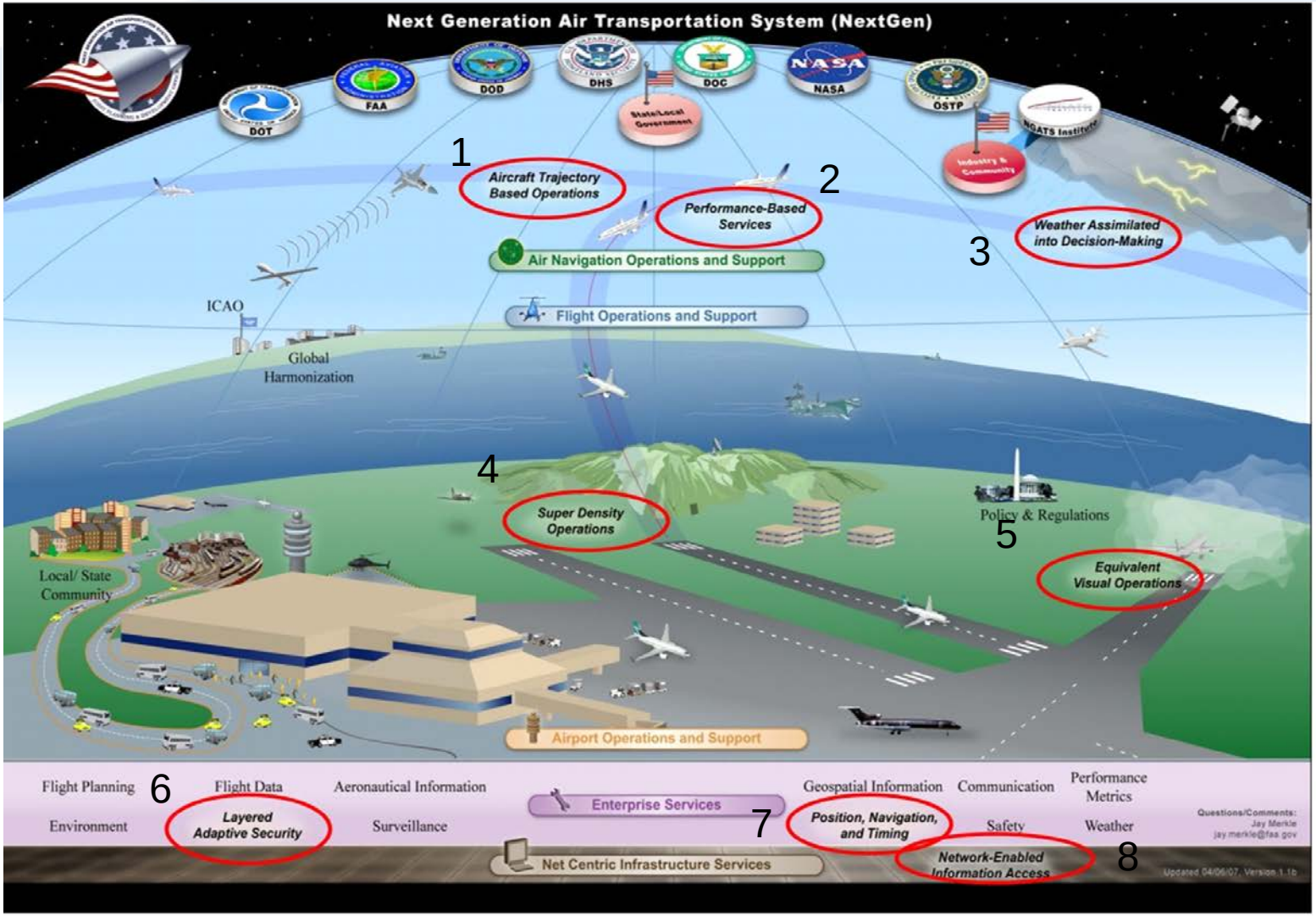
FAA Cybersecurity Test Facility (CyTF)

By: Enterprise Information Security Team ANG-B31
Patrick Hyle, William J Hughes Technical Center

Date: 08 August, 2016




Next Generation Air Transportation System (NextGen)
DOT
FAA
DOD
DHS
DOC
NASA
NASA
OSTP
NGATS Institute
State/Local Government
Industry & Community
1
Aircraft Trajectory Based Operations
2
Performance-Based Services
3
Weather Assimilated into Decision-Making
Air Navigation Operations and Support
ICAO
Global Harmonization
Flight Operations and Support
4
Super Density Operations
Policy & Regulations
5
Local/ State Community
Equivalent Visual Operations
Airport Operations and Support
Flight Planning
6
Flight Data
Aeronautical Information
Enterprise Services
Geospatial Information
Communication
Performance Metrics
Environment
Layered Adaptive Security
Surveillance
7
Position, Navigation, and Timing
Safety
Weather
Questions/Comments:
Jay Merkle
jay.merkle@faa.gov
Net Centric Infrastructure Services
Network-Enabled Information Access
8
Updated 04/06/07, Version 1.1b

FAA

NextGEN

FAA Provides Aviation Portion of Critical Infrastructure





According to a 2005 DHS report:

A successful cyber attack which shuts down aircraft operations, the potential losses to the economy would be in the range of **$2.5 billion per day**.

Additional losses *could* occur due to decreased consumer confidence , and cascading disruptions.

The primary goal of the CyTF is to provide cybersecurity research, test & evaluation services which address the changing threat landscape to the FAA NextGen Air Transportation System.

FAA

NextGEN

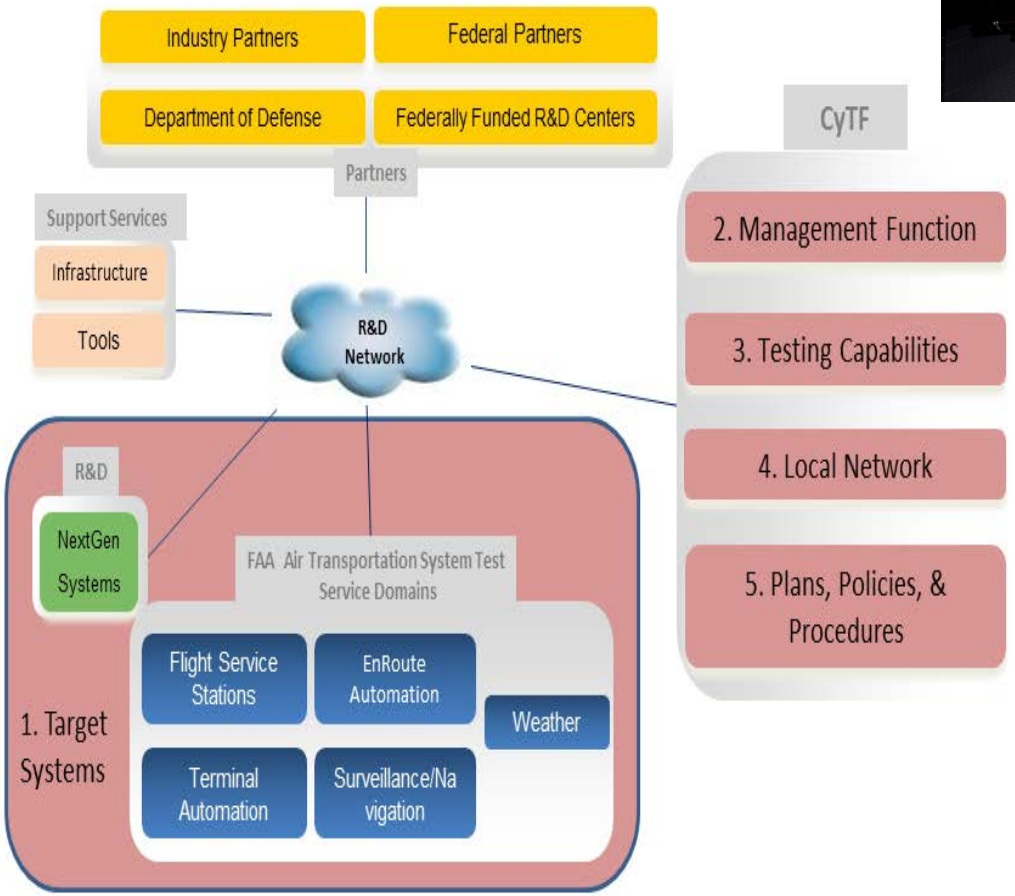
FAA Cybersecurity Test Facility (CyTF)



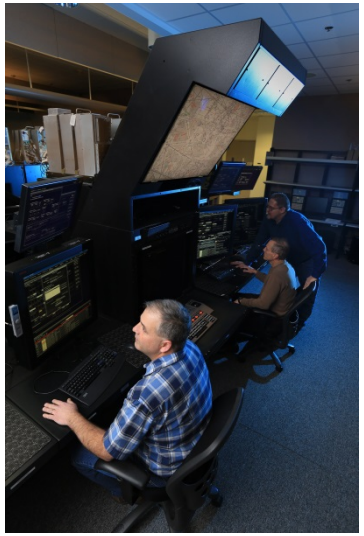
FAA Test and Evaluation Capability for Cybersecurity Interoperability











FAA

NextGEN

FAA Cybersecurity Test Facility (CyTF)

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





- ✓ CyTF combines management support, expert engineers, well defined testing procedures, and appropriate technologies in the development and operation of a cost-effective, state-of-the-art cyber test facility
- ✓ Evaluates, verifies, and validates Information Security Continuous Monitoring (ISCM) capabilities for application to the NAS



- ✓ Provides an environment where cyber testing and training will not interfere with NAS and Mission Support continuous operations
- ✓ Offers a facility to assimilate multiple existing partner capabilities for testing and evaluation of vulnerabilities in the integrated aviation environment

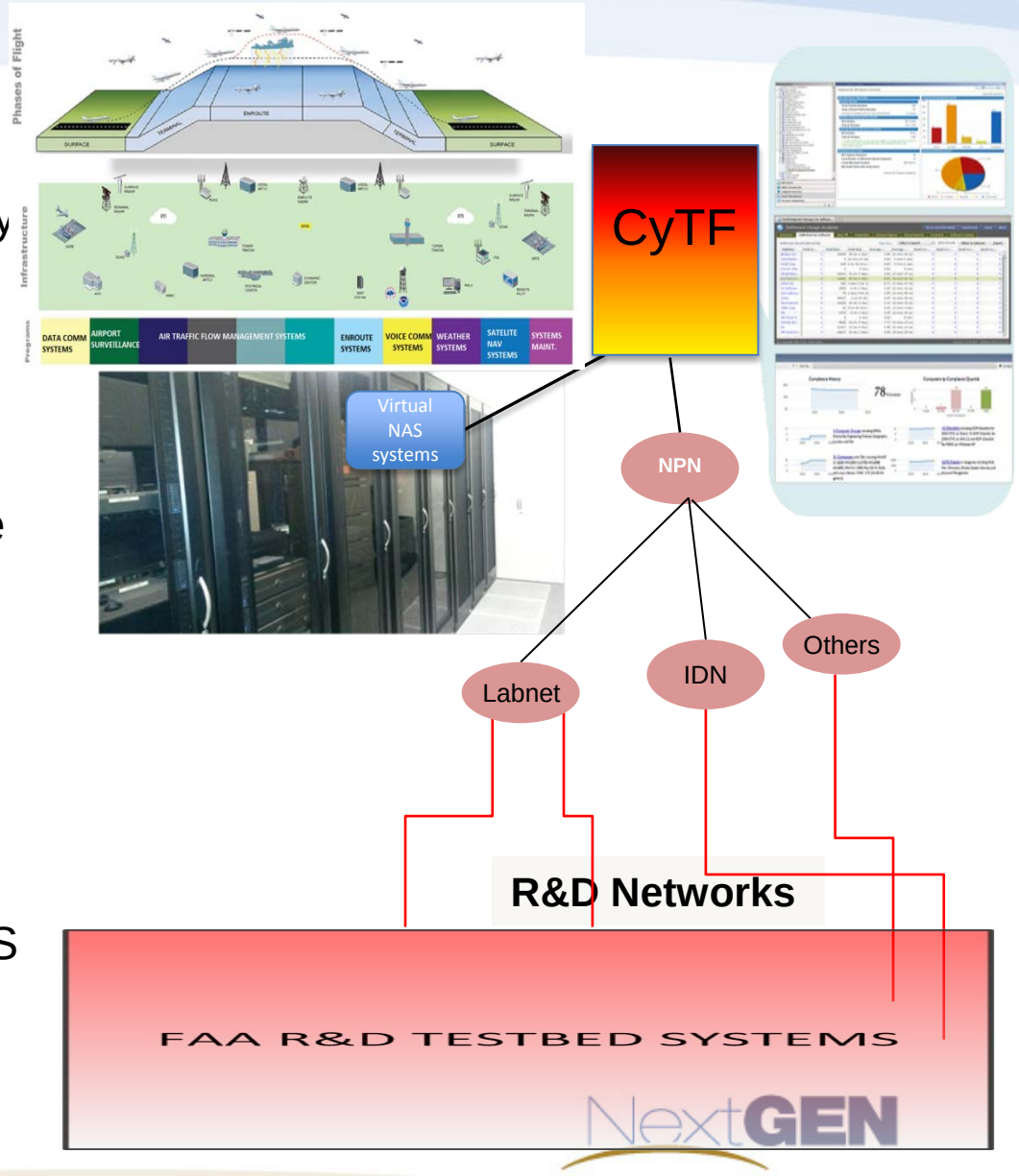
FAA

NextGEN

NAS Enterprise Test Environment

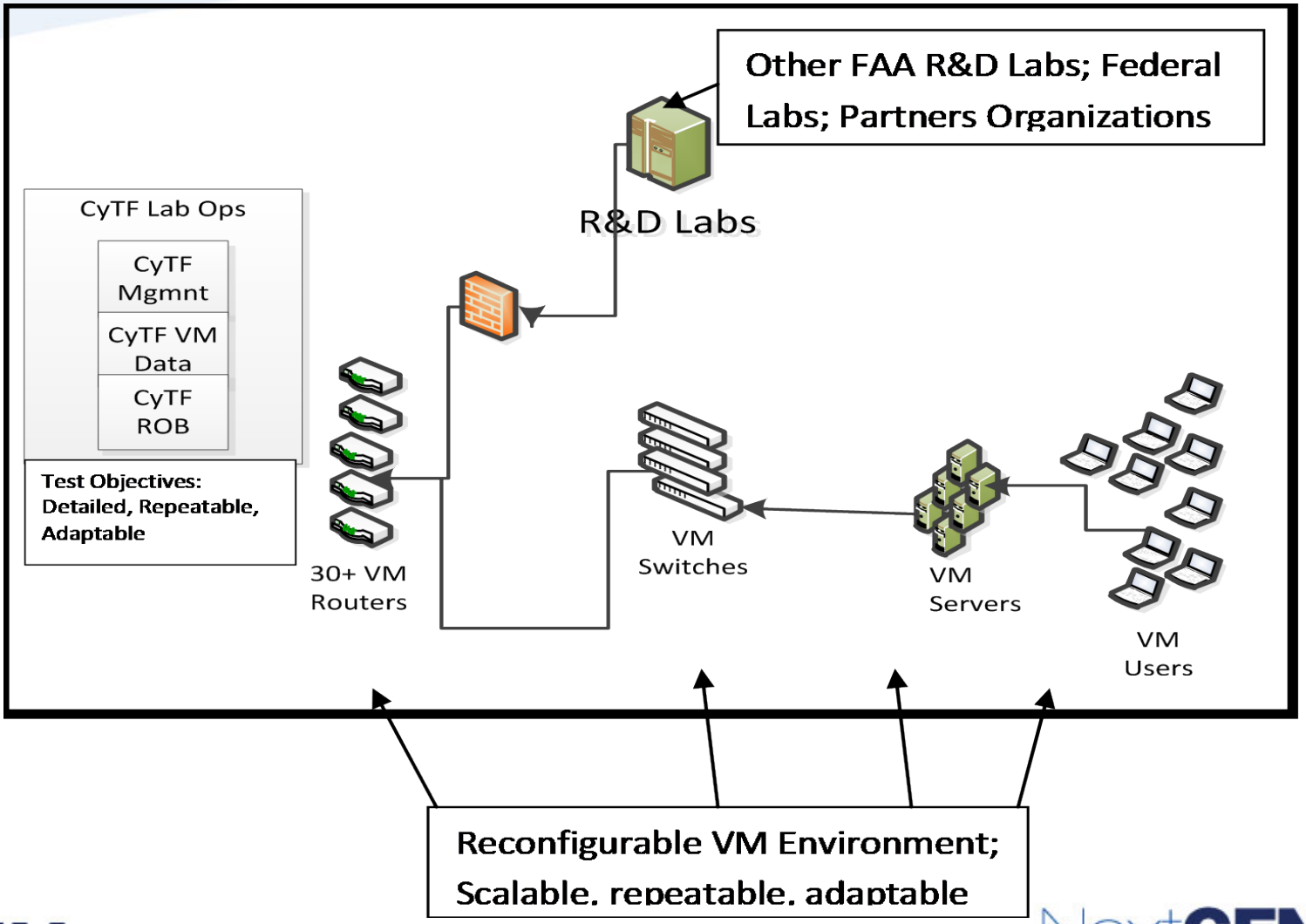
FAA Cybersecurity Test Facility

- State-of-the-art cybersecurity facility providing virtualized and existing NAS laboratories to assess impact of new tools and capabilities on the NAS.
- Robust and resilient laboratory able to provide a virtual NAS environment under simulated cybersecurity attacks to train and evaluate cyber response and recovery procedures for cybersecurity events
- Utilizes existing developmental NAS capabilities and R&D networks



FAA

CyTF Notional Layout



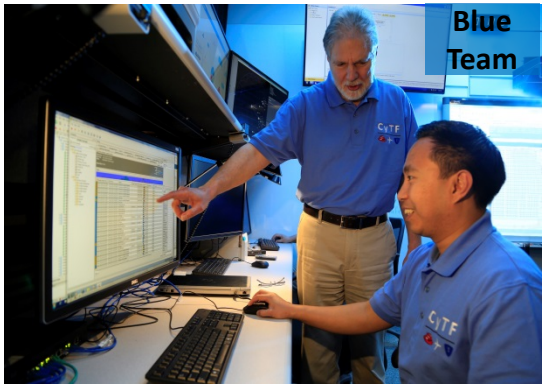
FAA

NextGEN

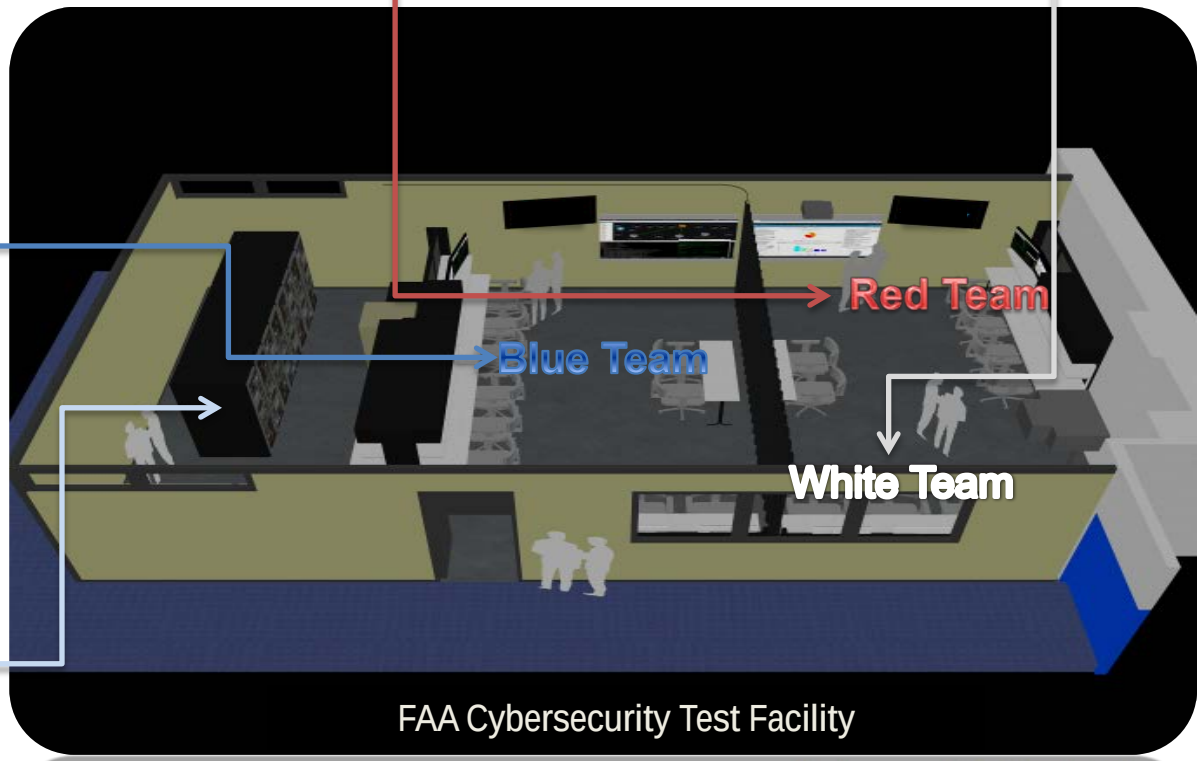
CyTF Physical Layout







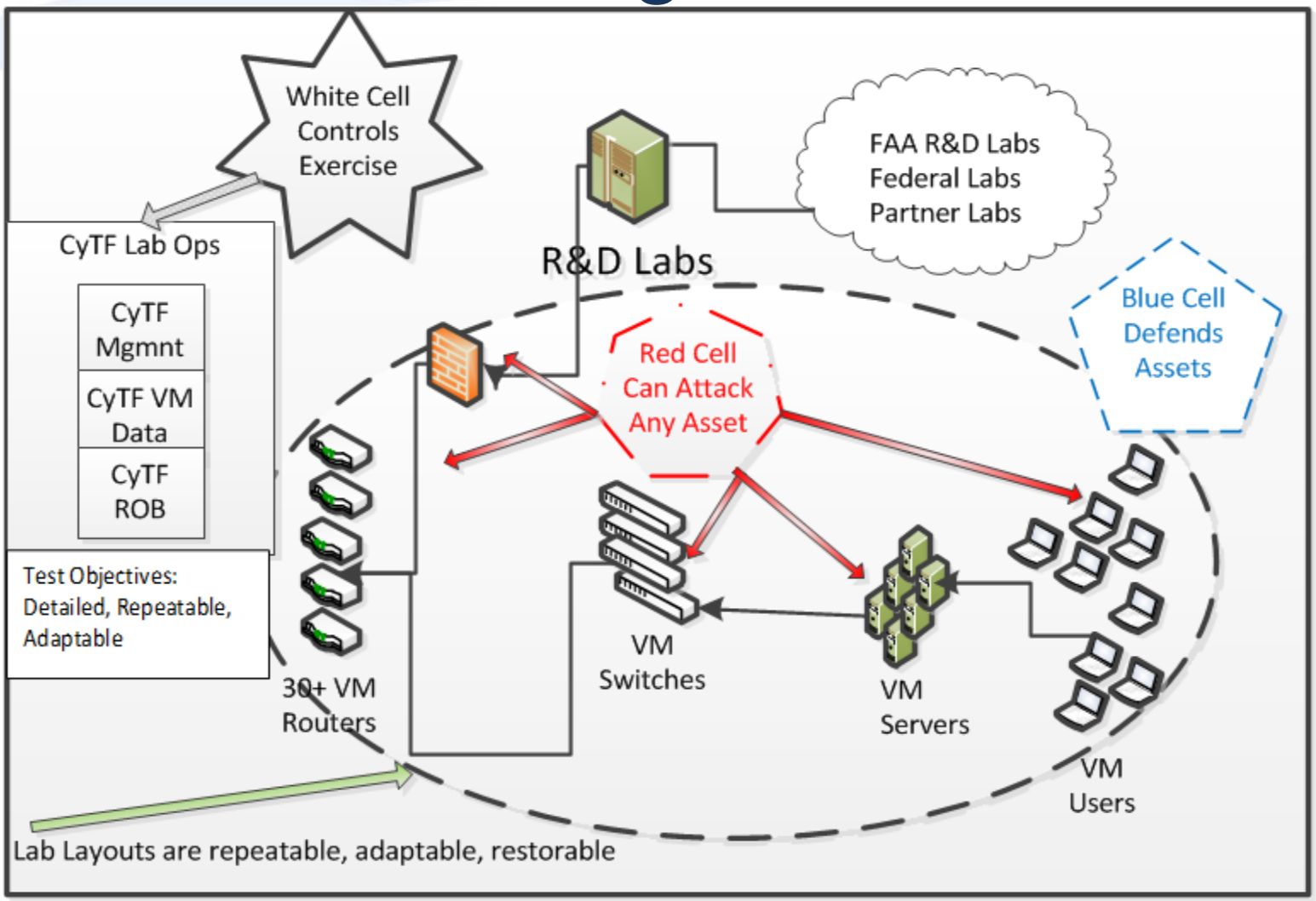




FAA

NextGEN

FAA Exercise High Level Network



FAA

NextGEN

Simulated Cyber Exercise

- Simulated FAA environment enabled hands-on experience vs. previous TTX iterations
- Inaugural exercise involved ~ 50 real time participants utilizing the CyTF VM network
- CyTF provided all network components – routers, switches & over 125 end users (both real and simulated)
- Team oriented exercise with Red, Blue, White, Orange, Green team members:
  - RED TEAM: represent Intruders
  - WHITE TEAM: plans and conducts the exercise
  - BLUE TEAM: represents the defenders
  - GREEN TEAM: provides Network ops support
  - ORANGE TEAM: provides Technical assessment of the exercise – in how it did/did not work; did it meet training needs; note possible improvements for future X ops

FAA

NextGEN

Exercise Roles & Responsibilities

WHITE TEAM

- Before Exercise: Core Planning, Scenario development, Logistics.
- During Exercise: Controls & Manages pace of exercise.

RED TEAM

- Attacks the network environment and its machines.

BLUE TEAM

- Defends against the attack.
- defends the network by executing blocks on firewalls, proxies, etc…

ORANGE TEAM

- Before Exercise: Collects the training objectives / requirements.
- During Exercise: Captures observations & lessons learned, if training objectives were met and generates Blue team assessment reports.

GREEN TEAM

- Ensures the overall virtual environment is available and functional.
- Intercedes in the event of a virtual environment problem.

Product Evaluations

- CyTF enables test/evaluation of Security products & procedures isolated from live Ops
- CyTF has to date evaluated ~ 2 dozen various products;
  - Range from very large (Enterprise level) to individual system components/processes
  - Evaluation assesses operational impacts, induced latency, cyber security improvements, and overall product efficacy – at the system(s) and aggregated Enterprise levels
  - Evaluations support DHS & USCYBERCOM US Govt continuous detection and mitigation efforts

Training Services

- The simulated environment enables hands-on training and testing of training procedures
  - Assessing the efficiency/efficacy
  - Assessing aggregate impacts
  - Identifying areas for improvement
- Adaptive VM environment enables tailored training environment
- Tailorable, adaptive, responsive, contained

Lessons Learned

- There is a growing need for Cyber Labs
- CyTF addresses this need for the FAA
  - This is the 1st step of many on a continuous path
- Collaboration is the BIGGEST key to success
  - Continued collaboration is essential to operations
- Scalability, adaptive components, are essential from the outset
- Leverage current & Emerging Cyber initiatives
  - Maintain Cyber acumen, utilize all available resources
    - Government, Business, Academia
- This is not STATIC and will evolve over time and per force of the changing ***Cyber Landscape***

FAA

NextGEN

In Summary….

The CyTF addresses the need to improve current cybersecurity capabilities commensurate with growing and evolving cybersecurity risks and threats to the FAA

- Proactively manage cybersecurity risks and threats using a mission-oriented enterprise-wide development and prototyping approach
- Establish cybersecurity test and evaluation capabilities that protect FAA essential systems and information
- Tailor continuous monitoring capabilities to efficiently and effectively detect cybersecurity events and attacks
- Provide robust training and simulation capabilities to respond to and recover from sophisticated cybersecurity events
- Establish a robust and resilient environment able to evaluate critical services while under a cybersecurity attack

FAA

NextGEN

Collaboration is Key



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



FAA

NextGEN

Contact Information

FAA Cyber Test Facility :

Via E-Mail:

9-ACT-CYTF