A Cybersecurity Test and Evaluation Facility for the Next Generation Air Transportation System (NextGen)

David Ingegneri, *CyTF Engineer* Dominic Timoteo, *CyTF Engineer* Patrick Hyle, *CyTF Engineer*
Fidel Parraga, *Support CyTF Engineer* Alex Reyes, *Support CyTF Engineer*

Abstract

The Federal Aviation Administration (FAA) is developing the Cybersecurity Test and Evaluation Facility (CyTF) for the FAA Air Transportation System as it transitions to the Next Generation Air Transportation System (NextGen). This paper describes the goals, capabilities, architecture, current implementation, initial experience, lessons learned and future implementation of the CyTF. The FAA Air Transportation System is an attractive cybersecurity threat target and the FAA must proactively and continually adjust its cybersecurity capabilities to match the changing cybersecurity threat landscape. The CyTF is providing an adaptable cybersecurity research and development environment independent of the operational system to satisfy research, test and evaluation needs. The CyTF has a number of complex requirements: testing cybersecurity tools and technologies prior to their integration into the Air Transportation System, the evaluation of individual FAA Air Transportation subsystems security, security of end-to-end services involving multiple subsystems, procedures to respond and recover from a cybersecurity event and cybersecurity training of the FAA workforce. One of the major lessons learned, described in the paper, has been how to address some aspects of the CyTF's complex requirements.

1. Introduction

As the cybersecurity threat landscape continues to evolve, the FAA must proactively and continually adjust the cybersecurity capabilities of the Nation's Air Transportation System in order to maintain a safe and resilient information systems environment. The CyTF is providing a state-of-the-art independent, adaptable and scalable cybersecurity environment to satisfy research, test and evaluation needs without impacting performance and availability of the FAA Air Transportation System. Cybersecurity threat actors, including criminal organizations and nation-state adversaries, have become very sophisticated; they are usually well funded, use advanced and persistent methods of attack, and pose the greatest security risk to organizations with critical missions such as the FAA Air Transportation System.

The FAA Air Transportation System is a large and complex system of systems based on legacy and state-of-the-art technology. Like other industrial control systems, the Air Transportation System has unique performance, reliability and safety requirements. The Air Transportation System interfaces with Department of Defense system components to provide aviation security and defense. The key characteristics of the Air Transportation System and its critical mission make it a very attractive target for a cybersecurity attack.

The FAA Next Generation Air Transportation System, (NextGen), depicted in Figure 1, is part of the Nation's critical infrastructure. NextGen includes components shared with various international, national, state, local, and private entities to improve the overall air transportation system. NextGen will improve the air transportation system capacity and safety through the use of high performance and cost effective technologies including satellite based surveillance, air-ground data communications, and a state of the art communications system. Figure 1 represents an operational concept of NextGen [6] that defines the various components and systems that make up the FAA Air Transportation System with a focus on NextGen improvements. The goal of NextGen is to improve the overall air transportation system with a focus on NextGen capabilities that provide the greatest results. Some of these NextGen capabilities are circled in red in Figure 1 and include: aircraft trajectory based operations, performance-based services, weather assimilated into decision-making, super density operations, equivalent visual operations, layered adaptive security, position, navigation, and timing, and network-enabled information access. Progress is moving forward to meet the NextGen goals but the FAA Air Transportation system is a complex and unique system that requires the correct blend of technical, policy, and operational improvements to succeed.

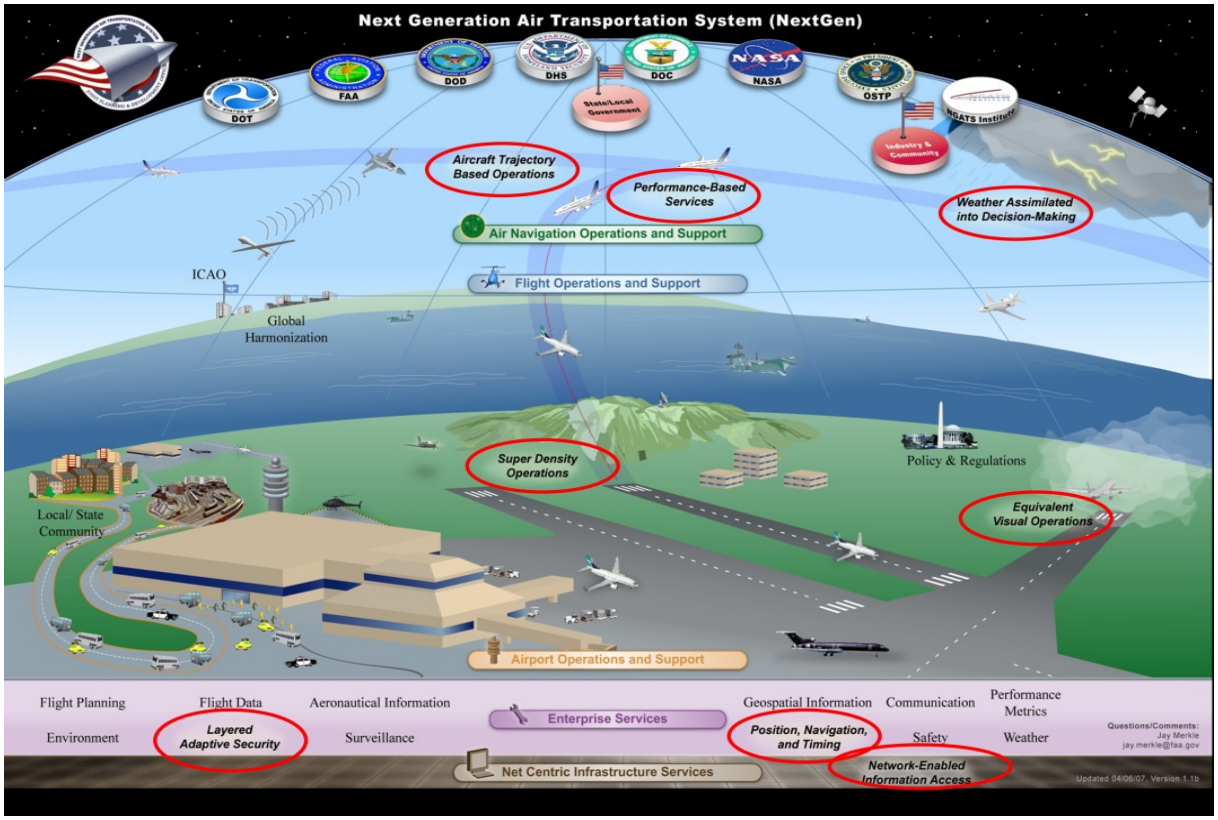

Figure 1 - NextGen Capabilities

The unique characteristics of the FAA NextGen Air Transportation System require cybersecurity capabilities, tools and technologies that are adjusted and adapted to satisfy those unique characteristics. However, these cybersecurity safeguards must be thoroughly evaluated, tailored, and tested before making decisions to deploy them in the Air Transportation System to ensure their effectiveness and that their integration will not impact performance, reliability and safety.

The disruption of the FAA NextGen Air Transportation System would have a debilitating safety, security, and economic impact and may prevent the FAA from performing its mission. The value of the CyTF resides in the ability to integrate required cybersecurity capabilities, tools and technologies while continuing to maintain a safe, secure and resilient Air Transportation System. The CyTF is working to become the state-of-the-art information system environment to perform cybersecurity research, test and evaluation that supports and enables the mission of the FAA.

2. Goals

The primary goal of the CyTF is to provide cybersecurity research; test and evaluation services that improve the cybersecurity posture of and address the changing threat landscape to the FAA NextGen Air Transportation System. To achieve the primary goal, the CyTF is providing a scalable and adaptable environment to support:

1. The identification and validation of cybersecurity threats and risks by simulating the FAA Air Transportation System to determine impact to the FAA's mission.

2. The integration of cybersecurity capabilities, tools and technologies to protect information systems, data and infrastructure, while satisfying the strict needs for safety, security and availability.

3. The transition to a continuous monitoring of the information system environment to effectively and efficiently detect and prevent cybersecurity events.

4. The process improvement to respond and recover from cybersecurity events and attacks including advanced and persistent attacks from criminal groups and nation-state adversaries.

5. The process to assess and improve the resilience of information systems ability to operate and perform the FAA's mission even when affected by a cybersecurity event or attack.

There are many in-progress and planned FAA cybersecurity initiatives, studies and assessments to address the evolving threat landscape. The CyTF is providing the Research and Development test and evaluation environment to support those efforts and validate results.

3. Key Characteristics

To achieve its goals CyTF must incorporate the following key requirements and characteristics:

1. The CyTF must replicate with high fidelity systems, services, and capabilities of the FAA operational Air Transportation System.

2. The CyTF systems must be independent of the operational environment they replicate so that CyTF experiments can be conducted without affecting the performance of the operational systems.

3. The CyTF systems and subsystems must be extensible to allow the addition and testing of new security approaches and security prototypes.

4. The CyTF must be highly adaptable but have a number of stable core baselines.

a. The CyTF can be used to conduct experiments that utilize individual systems, systems of systems, or represent an enterprise architecture that supports a variety of scenarios.

b. The CyTF can be reset to a stable core baseline at the conclusion of experiments.

5. The CyTF must be able to evaluate, verify, and validate information security controls in the FAA Air Transportation System.

6. The CyTF must facilitate cooperation with industry, academia, and government to maintain and improve the security posture of the FAA NextGen Air Transportation System.

7. The CyTF must be able to utilize existing developmental FAA air traffic capabilities and R&D networks.

8. The CyTF must have asset discovery and vulnerability identification capabilities.

4. High-level Architecture

The Architecture of the CyTF, as depicted in Figure 2, includes five major components: the target systems to be tested, the CyTF management function, the CyTF testing capabilities, the CyTF local network, and the CyTF plans, policies, and procedures (the applicable Rules of Behavior related to exercise/experiment processes).

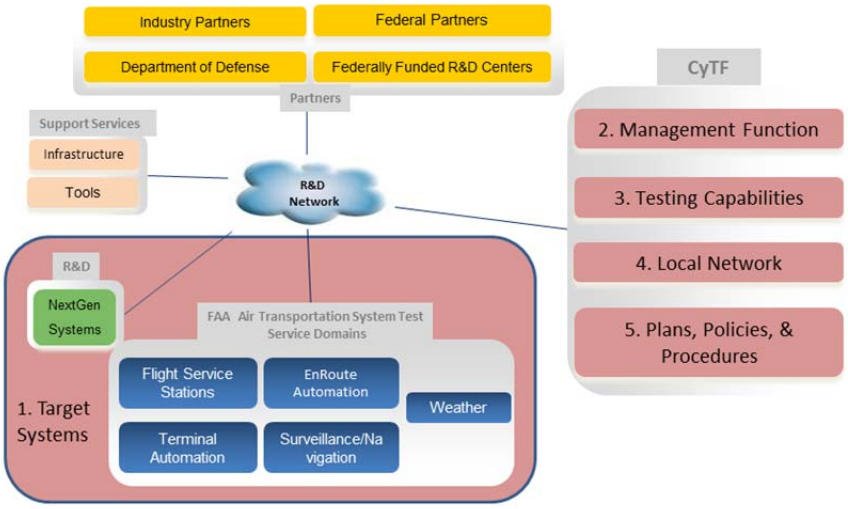

Figure 2 - High Level CyTF Architecture

The target systems to be tested are select operational components of the FAA Air Transportation System that are either virtualized in CyTF or that exist in other FAA test beds accessible to CyTF via existing connections to external facilities/networks. This element of the architecture fulfills the first two CyTF requirements: reflecting the FAA Air Transportation System with high fidelity, and not impacting real-world operational performance and availability.

The CyTF management function provides the capability to configure the CyTF environment, enables capturing experimental data, and assists in the preparation of follow-up reports. The CyTF testing capabilities range from single component to enterprise testing and are an evolving set of capabilities as described in the next section. The CyTF hosts the virtualized systems, platforms used to manage CyTF capabilities, and interfaces to other FAA test beds and partners' R&D networks. The CyTF plans, policies, and procedures include a plan for overall configuration management and agreements to document connectivity and testing level permissions regarding systems to be tested and/or simulated in the conduct of testing.

5. Capabilities

The CyTF capabilities were initially developed exclusively with FAA resources, however some other

capabilities are being developed with the support of the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. CyTF includes capabilities to test and evaluate:

1. Select cybersecurity tools and technologies, either to be deployed in the FAA or under consideration for such deployment.

2. Cybersecurity solutions to help determine their feasibility, effectiveness, and impact to the operational FAA Air Transportation System.

3. The security posture of individual FAA Air Transportation System systems;

4. Enterprise security functions, e.g. enterprise level incident response, boundary protection, and backbone protection within an operational framework.

In addition to test and evaluation CyTF also includes the following capabilities to:

5. Train designated cybersecurity staff in the use of new and existing cybersecurity tools and processes, vetted through the T&E process.

6. Identify vulnerabilities and select applicable fixes and/or cybersecurity defenses.

7. Assess the associated risk via penetration testing in a virtual environment for those vulnerabilities that cannot be readily fixed or easily mitigated.

The implementation of CyTF requirements and characteristics listed in Section 3 enable CyTF capabilities. In particular, these capabilities require an independent environment that can replicate the operational FAA Air Transportation System without impacting its operations, a highly extensible and adaptable CyTF to accommodate different test scenarios, tools and solutions, a CyTF environment that facilitates internal and external cooperation, and methods for asset discovery and vulnerability identification.

6. Planning, Implementation, Utilization

Planning of CyTF took about a year. Initial planning involved visits by the FAA CyTF planning team to the DOT/FAA Security Operations Center to understand their operations and to discuss their training processes. The team also visited FAA partner cyber-laboratory facilities to discuss their capabilities and learn about their cybersecurity exercises. The team observed a large scale military cyber-exercise hosted by MIT Lincoln Laboratory at their cybersecurity facility in Lexington, MA and subsequently entered into an agreement with MIT LL to support the expansion of CyTF into a cyber-range. These experiences helped solidify CyTF planning which followed the FAA Systems Engineering procedures and produced the following CyTF internal documents: a Concept of Operations [1], a Functional Architecture [2], and Functional and Performance Requirements [3].

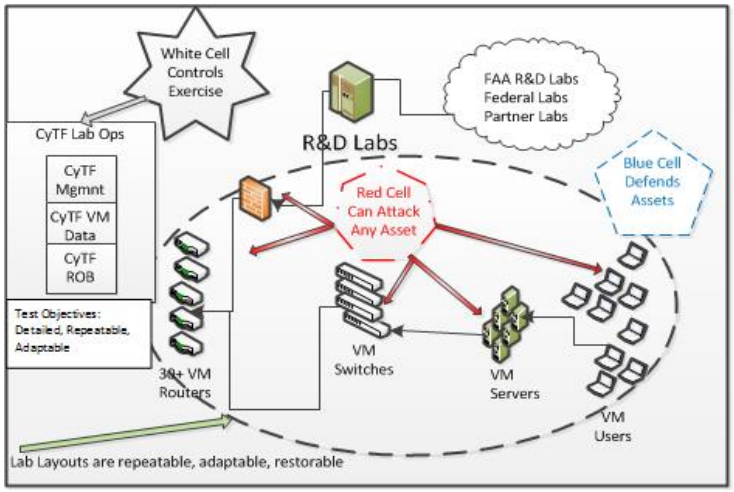

Figure 3 - CyTF Conceptual Layout

The current CyTF implementation was dedicated in October 2015 and includes: (1) The CyTF local laboratory and network hosting the CyTF management function, virtualized systems, and gateways to other FAA testbeds and CyTF partners' in the FAA R&D network; (2) a virtual environment that contains over 30 routers and 120 virtual servers and workstations that simulates parts of the FAA Air Transportation System; (3) connectivity to FAA Air Transportation System replica systems within the CyTF and in other FAA test beds; and (4) the CyTF testing teams that include defensive (blue), offensive (red), and orchestration (white) cybersecurity testing teams. Figure 3 illustrates the CyTF conceptual layout described above.

The CyTF implementation is congruent with CyTF goals. CyTF network connectivity enables the transition of FAA's R&D information system

environment from sporadic and manual to automatic and continuous monitoring; this connectivity also enables CyTF integration with Air Transportation System component-system replicas for cybersecurity testing. The CyTF virtual environment facilitates identification of cybersecurity threats and risks in a high-fidelity network environment that is similar to, but isolated from, FAA operations. Process improvement of FAA's response to cybersecurity events is also facilitated via the CyTF implementation's physical infrastructure augmented by the expertise of its staff of security subject matter experts.

The implementation of CyTF can go through substantial changes to meet the needs of an experiment. The CyTF configuration changes are governed by the CyTF Configuration Management (CM) plan [4] which identifies two levels of changes: (1) transitory changes to accommodate experiments; these changes are removed at the conclusion of the experiment, and (2) evolutionary changes that affect the CyTF core configuration; evolutionary changes are more permanent, less frequent, and respond to the need to improve the CyTF core capabilities. CyTF CM prescribes the process for making changes to the CyTF and it also identifies CM roles and responsibilities.

To date CyTF has facilitated information security testing, training, and evaluation activities. The three tasks described in this section illustrate four of the seven CyTF capabilities identified in Section 5 of this paper.

ERAM Security Tool Evaluation

A task that illustrates CyTF capability #1 conducted a functional and performance evaluation of a complex commercial network vulnerability and asset management tool integrated with the FAA's En Route Automation Modernization (ERAM) [5] system. ERAM primarily supports high-altitude Air Traffic Control (ATC) and is considered the backbone of the nation's airspace system with processors for flight data, surveillance data, communications and display data to air traffic service providers. CyTF leveraged the FAA R&D Network to access the Interoperability and Integration Facility (I2F), an FAA laboratory that has a hardware and software instantiation of ERAM. A software agent for the security tool-under-test was installed on each of the 38 ERAM processors at the I2F; the agents communicated with a relay at the I2F that aggregated the data and sent it to the asset management tool server hosted at CyTF. The evaluation measured the tool's impact on the ATC system by comparing metrics of processor utilization with and without the agents installed to the requirements for these metrics imposed by FAA on ERAM. A typical load of flight and surveillance data consisting of 211 simultaneous aircraft tracks recorded at the FAA's Washington, DC Air Route Traffic Control Center, was used to feed ERAM and a scenario was built to exercise the tool-under-test in the way it would be expected to function in the FAA environment. This functionality is primarily endpoint asset scanning of ERAM hardware & software that provides detailed information on operating system, applications and utilities for each ERAM processor. Additionally the tool-under-test was used to install software updates on certain ERAM processors. The results confirmed that there was no impact to ERAM functionality and performance under expected tool-under-test use cases; however, an atypical use case involving an initial software scan during ERAM peak aircraft processing did demonstrate moderate impact. From these results CyTF staff generated a report with recommendations for the use of the security tool on ERAM.

This task revealed that the use of a partner laboratory, albeit necessary, can have a complicating effect on estimating task schedule and cost. Indeed, all aspects of the project were impacted from planning (agreements between the laboratory organizations were required that specified funding), to conduct (logistics & scheduling, connectivity issues), to analysis (data delivery & format issues).

IPE Evaluation

A task that exemplifies CyTF capability #2 conducted a feasibility study of one aspect of a proposed FAA security solution called Internal Protection Enforcement (IPE). IPE is based on the idea that the FAA Air Transportation System conforms to the characteristics of an industrial control system (ICS) with a finite set of data and command message formats. With this characteristic it may be practical to conduct low-level message whitelisting; i.e., block all traffic coming from non-FAA networks into the FAA Air Transportation System network and only allow the data and command messages that conform to specific profiles. This is in contrast to the more common method that allows all traffic and blocks only malware with known signatures. Whitelisting is very effective in blocking advanced threats and zero-day attacks but it can be computationally intensive when applied to large flows of data messages and it is not feasible for certain data formats such as binary data. An early CyTF configuration was used to whitelist FAA incoming data containing International Civil Aviation Organization (ICAO) flight plan messages. A whitelisting prototype was constructed using a programmable network device that is being used by FAA in the NextGen timeframe. The use of an existing device for IPE can be a significant benefit since it is expensive in both time and

money to add and maintain a new device in the Air Transportation System. Using the flight data sample the prototype established that 100% of flight plan messages conforming to the test profile were successfully accepted and only 0.02% of non-compliant flight plan messages were accepted. This study examined the ability to whitelist entire messages via regular expressions. CyTF staff generated a report that concluded this level of whitelisting was technically feasible using the FAA device but more testing in a more realistic FAA network traffic environment is needed to examine performance and scope issues. This additional testing is not currently planned but CyTF, supplemented with other FAA system laboratories, has the capability to conduct it.

The IPE task revealed the value of software engineers that also have knowledge of FAA networking and messaging. This knowledge base was critical to completing the study in an acceptable amount of time.

Incident Response Planning Exercise

An example that spans CyTF Capabilities #4 and #5 is the FAA Incident Response Plan (IRP) Exercise. This is a human-in-the-loop (HITL) exercise conducted over five days to examine the FAA's cyber-incident response processes and to train FAA IT and cyber analysts on the use of the procedures to detect and respond to intrusions. Expected results include improvements in stakeholder information sharing, strengthening SOPs and identifying criteria and processes for incident response escalation and reporting. CyTF hosted the 2016 IRP exercise which had been a table-top; i.e., events on paper only, exercise in previous years. The exercise is designed to be carried by three teams: Red, Blue, and White teams. The Red Team is the intrusion team; it has partial or full knowledge of the targeted system (usually virtual) and is armed with offensive network tools. The Blue Team is the incident detection and response team; they operate the CyTF defensive tools to block and contain the intrusion. The White Team directs, observes, and collects data during the exercise. CyTF, as shown in Figure 4, is designed to accommodate cyber exercises and has the means to configure and isolate physical space for the needs of each team. CyTF's design was planned from the start to be extensible via the use of other spaces (specific conference rooms with direct CyTF connectivity and reconfigurable walls, and other local laboratories) to handle exercises that are too large for the CyTF physical footprint. The 2016 IRP Exercise, with 45 players, required the use of CyTF plus two of the specialized conference rooms.

The IRP participant's feedback indicates that the addition of the virtual machine environment adds significantly to the realism of the exercise when compared with previous years' tabletop exercises. Each player was assigned his/her own virtual workstation and the security center detection and response analysts used most of the same security tools as they use at their security center workstations. Unfortunately, given the newness of the CyTF environment and the necessary time constraints of pre-exercise player support, not all tools the analysts use were put into the exercise environment and some that were there weren't configured exactly as the players preferred them to be. Even with these limitations overall player feedback regarding the realism of the environment was positive. In addition to security analysts there were FAA Information Technology SMEs that were provided access to virtual routers, firewalls and security gateways that mimicked their everyday environment.

Figure 4 - CyTF Cybersecurity Exercise Layout

Some elaboration is in order concerning the complexity and effort inherent when first introducing a virtual

machine environment to what was formerly a table top exercise. Since this was also the first exercise for CyTF, both the physical and virtual environments were created from scratch. Logistical issues are to be expected when hosting an exercise for the first time. The physical environment required workable lighting and HVAC tuning as well as arrangements for player access and seating to accommodate the 50 plus players and observers. The virtual environment required not only virtual machines and network devices but also commercial and FAA software applications that were installed and configured according to current FAA standards to have the same look and feel as in the player's own environment. The large number of software applications required the coordination of the CyTF with FAA partners and commercial vendors. This presented a scheduling problem in that partner SMEs were only available when they could take time away from their normal duties. The completion of many pieces was just-in-time and some couldn't be included in the exercise due to these SME dependencies. Commercial product licensing was also a major hurdle. The number of temporary licenses and their various expiry dates became a significant CM issue. The amount of time to install, configure, test and verify the pieces and then test the overall environment meant that many temporary licenses were expired prior to exercise conduct. Reuse of much of the virtual environment for future exercises should alleviate some of the above issues; however, licensing and support will remain an issue so long as temporary licenses are used. Technical issues were myriad with the most salient being the understanding by the virtual environment architects of how the attack scenarios would operate so that the devices that were being targeted would be affected as the scenario team intended. A device that wasn't affected according to plan meant device logs wouldn't provide the evidence that may be needed by analysts to properly diagnose the security event or to even detect the event. Getting this right meant many meetings that consumed a significant amount of the planning, scenario, and technical team members' time (maybe 30%).

CyTF capability # 6 has not yet been formally applied, but CyTF will be evaluating the current FAA processes that apply security updates to Air Transportation System custom, open source and commercial software in a more unified and systematic approach. Changing and increasing cybersecurity threats may have the potential to exploit vulnerabilities in data flows, servers, networks and security processes so it is increasingly important to discover, assess and, as necessary, either fix or mitigate security vulnerabilities.

7. Lessons Learned

The initial design and implementation of the CyTF has been a rich learning process and experience. One key lesson learned was the need to connect goals and capabilities to the mission of the organization. A research and development, test, and evaluation environment like the CyTF requires cross-organization collaboration and adequate funding (e.g., CyTF realized a 25% differential in budgeting costs) to succeed that can be achieved only with executive-level sponsorship. While primarily a technical environment, CyTF management elevated their technical perspective and connected the value of the CyTF to the FAA's mission, to address cybersecurity concerns from executives accountable and responsible for the FAA's mission and strategy.

Another key lesson was that it is critical to design for scalability and adaptability from the outset. CyTF management identified a strong need for a cybersecurity research, test and evaluation environment. Once the initial CyTF environment was up and running, there were multiple stakeholder organizations interested in learning more about and using the CyTF. A robust system engineering approach was employed (described in Section 6) to design an environment with initial limited capabilities and connections, but designed to evolve, scale and adapt as necessary. From a technology perspective, great benefit is being realized in the use of virtualization technologies that provide the flexibility to scale, re-configure and adapt the CyTF to satisfy multiple stakeholder needs.

It is important to leverage current cybersecurity initiatives, research and development. As the cybersecurity threat continues to evolve, industry and government institutions have responded with significant research and initiatives that can be leveraged. CyTF is collaborating with academia, government partners, and other government agencies.

Finally, it is useful to plan for the on-going management, operations and maintenance of the environment. It is easy and rewarding to focus on the technical aspects of the environment, but the on-going management, operations and maintenance of the environment consume a significant amount of time and resources. Managing the environment includes real estate, acquisition, procurement, funding, vendor management, and visitor management activities, among others.

Conclusion

The initial and current CyTF implementation lays a solid foundation to address the cybersecurity threat. CyTF implementation includes the local laboratory and network, a virtual environment simulating parts of the Air Transportation System, connectivity to replicated

systems of the Air Transportation System, connectivity to other FAA test beds, and the defensive (blue), offensive (red), and orchestration (white) CyTF testing teams.

The initial CyTF implementation is incrementally evolving to replicate FAA NextGen Air Transportation System services in an independent and secure research and development environment. The CyTF evolution is being driven and prioritized by the need to address the cybersecurity threat to the Air Transportation System.

In the future CyTF will provide the ability to validate the existence and magnitude of cybersecurity risks. As the FAA develops models to identify threats and risks, CyTF provides the independent environment to validate the findings without compromising performance and availability.

CyTF will continue and expand the testing and evaluation of cybersecurity capabilities, tools and technologies to secure access, applications and services, data, networks, servers and end-points without compromising performance and availability.

CyTF will be used to evaluate the security posture of an integrated portfolio of FAA Air Transportation System systems. These assessments include existing and planned cyber-profiles of the subject/selected systems, as well as aggregated "systems of systems" within the FAA construct;

CyTF will continue to train the FAA and partner cybersecurity workforce. CyTF provides the environment to conduct adequate training including processes, tools and technologies to match the cybersecurity threat landscape.

CyTF will provide the ability to conduct penetration testing in a realistic environment without compromising performance and availability. CyTF provides the independent environment to conduct penetration testing that faithfully resembles and evaluates the posture of the operational environment.

CyTF plans to continue and expand cybersecurity exercises to test, evaluate and improve detection, response, and recovery processes, tools and technologies. CyTF provides the environment to expand and mature detection, response and recovery activities to consider advanced and persistent attacks from adversaries.

CyTF will provide the ability to assess and improve the resilience of information systems. CyTF provides the environment where resilience can be assessed, and new capabilities can be tested and evaluated without compromising the performance and availability of the FAA Air Transportation System.

CyTF will continue to expand the portfolio of virtualized systems in the CyTF laboratory and network, as more components of the FAA NextGen Air Transportation System adopt virtualized implementations.

In the future, CyTF will include a Sensitive Compartmented Information Facility (SCIF) to process sensitive classified information that would include storage, discussion on, and/or processing of interconnected data feeds. Development of a SCIF would allow for the handling and sharing of classified information and information connections with other federal partners.

CyTF provides the cybersecurity research, test and evaluation environment to address the continuing cybersecurity threat and to maintain a safe, secure and resilient FAA Air Transportation System.

References

[1] Federal Aviation Administration, January 30, 2015, NextGen Cybersecurity Test Facility (CyTF) Concept of Operations, Version 1.0, FAA ANG-B31 WJHTC, NJ.

[2] Federal Aviation Administration, January 30, 2015, NextGen Cybersecurity Test Facility (CyTF) Functional Analysis, Version 1.0, FAA ANG-B31 WJHTC, NJ.

[3] Federal Aviation Administration, January 30, 2015, NextGen Cybersecurity Test Facility (CyTF) Requirements, Version 1.0, FAA ANG-B31 WJHTC, NJ.

[4] Federal Aviation Administration, July 29, 2015, NextGen Cybersecurity Test Facility (CyTF) Configuration Management Plan, Version 1.3, FAA ANG-B31 WJHTC, NJ.

[5] Fact Sheet - En Route Automation Modernization (ERAM), April 29, 2015, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=7714

[6] Concept of Operations for the Next Generation Air Transportation System, Version 3.2, 2011, http://www.dtic.mil/dtic/tr/fulltext/u2/a535795.pdf.