Appendix A

Provide 2020-2025 Cyber Security Strategy Overview

FAA Cybersecurity Strategy 2020-2025 Overview

September 2019

Goal 1 Refine and maintain a Cybersecurity governance structure to enhance cross-domain synergy

- **Objective 1.1:** Maintain cross-organization processes for Cybersecurity strategic planning and budget development
- **Objective 1.2:** Codify and maintain FAA-wide Cybersecurity Roles & Responsibilities
- **Objective 1.3:** Improve understanding of Cybersecurity risk for FAA-owned, contracted and regulated systems
- **Objective 1.4:** Increase integration of Cybersecurity activities across Domains
- **Objective 1.5:** Update and maintain FAA-wide information security policies
- **Objective 1.6:** Implement the NIST Cybersecurity Framework to Manage Risk

Goal 2 Protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery

- **Objective 2.1:** Improve cyber threat intelligence collection, processing, dissemination, and reporting
- **Objective 2.2:** Improve FAA cyber monitoring, detection and response capabilities
- **Objective 2.3:** Improve privileged user control, monitoring and visibility
- **Objective 2.4:** Improve capabilities for detection and mitigation of threats, internal and external
- **Objective 2.5:** Leverage cybersecurity research and development across FAA domains and systems
- **Objective 2.6:** Ensure FAA Information Security Controls, Policies and Processes are aligned with current NIST Standards and Guidelines

Goal 3 Enhance data-driven risk management decision capabilities

- **Objective 3.1:** Continue development and enhancement of an enterprise cyber threat modeling capability
- **Objective 3.2:** Expand Information Security Continuous Monitoring capabilities for NAS and non-NAS IP systems
- **Objective 3.3:** Integrate threat, attack and vulnerability data with mission focus to prioritize risks
- **Objective 3.4:** Reduce the time required to address high value threats and vulnerabilities

Goal 4 Build and maintain workforce capabilities for Cybersecurity

- **Objective 4.1:** Enhance FAA-wide cybersecurity training, education and awareness program
- **Objective 4.2:** Support cyber workforce training through participation in exercises
- **Objective 4.3:** Ensure personnel having cybersecurity responsibilities receive appropriate role-based training
- **Objective 4.4:** Enhance FAA competitiveness in cybersecurity hiring and retention through adoption of current Federal IT Job Series

Goal 5 Build and maintain relationships with, and provide guidance to, external partners in Government and industry to sustain and improve cybersecurity in the Aviation Ecosystem

- **Objective 5.1:** Expand participation in cyber exercises with external partners
- **Objective 5.2:** Increase collaboration with other Government, industry and private sector cybersecurity teams
- **Objective 5.3:** Ensure cybersecurity requirements are addressed in the AMS and all FAA contract vehicles (ACQ)
- **Objective 5.4:** Expand information sharing with appropriate external partners including through automated cyber threat indicator sharing
- **Objective 5.5:** Leverage regulatory role to identify and address cybersecurity risks in aircraft systems as well automation of aircraft, equipment and technology
- **Objective 5.6:** Represent the United States in global engagement on aviation cybersecurity through partnership and engagement with international partners

Appendix B

Provide Definition / Clarity:

Diversity	Cyber Workforce
Align with MD-715 (EEO Program Status Update Report FY18) • Gender • National Origin • Disability	Align with previously defined OPM cyber work roles (regardless of Job Series):

FAA Cybersecurity Personnel Work Role	OPM Code
Mission Assessment Specialist	112
Exploitation Analyst	121
Threat/Warning Analyst	141
Cyber Defense Forensics Analyst	212
Cyber Crime Investigator	221
Database Administrator	421
Data Analyst	422
Network Operations Specialist	441
System Administrator	451
Systems Security Analyst	461

FAA Cybersecurity Personnel Work Role	OPM Code
Cyber Defense Analyst	511
Cyber Defense Infrastructure Support Specialist	521
Cyber Defense Incident Responder	531
Vulnerability Assessment Analyst	541
Authorizing Official/Designating Representative	611
Security Control Assessor	612
Secure Software Assessor	622
Information Systems Security Developer	631

FAA Cybersecurity Personnel Work Role	OPM Code
Security Architect	652
Research & Development Specialist	661
System Testing and Evaluation Specialist	671
Cyber Instructional Curriculum Developer	711
Cyber Instructor	712
Information Systems Security Manager	722
Communications Security (COMSEC) Manager	723

FAA Cybersecurity Personnel Work Role	OPM Code
Privacy Officer/Privacy Compliance Manager	732
Cyber Workforce Developer and Manager	751
Cyber Policy and Strategy Planner	752
Program Manager	801
IT Project Manager	802
Executive Cyber Leadership	901

Appendix C

Prioritize Bullet 2 of SOW

Bullet 2 of NAS Statement of Work reads:

Management and human resources approaches and strategies to achieve current and future desired outcomes that meet cybersecurity workforce needs, including recruitment and flexibilities, selection, retention, training, education, certification, and compensation considerations;

Proposed Prioritized Order
1. Recruitment and Flexibilities / Selection
2. Retention
3. Compensation Considerations
4. Training / Certification (specific skillsets)
5. Education (formal education)

Approved