Request for Information:
Post Quantum Cryptography Support for FAA Information Technology and National Air Space Systems (RFI Number 697DCK-26-RFI-PQC)

10 March 2026
Version 1.1

CONTENTS

1 REQUEST FOR INFORMATION (RFI) PURPOSE AND GOVERNMENTS DISCLAIMERS

1.1 PURPOSE

The Federal Aviation Administration (FAA) is issuing this Request for Information (RFI) to request detailed data, innovative approaches, and strategic insights from industry partners regarding their capabilities and readiness to (1) support the transition of the National Airspace System (NAS) and its supporting Air Traffic Control (ATC) infrastructure to Post-Quantum Cryptography (PQC) and (2) support the transition of FAA business systems to PQC.

The NAS is undergoing a generational transformation to realize a modern, resilient, and globally leading ATC system capable of integrating new entrants (e.g., drones, Advanced Air Mobility (AAM), and commercial space operations). Achieving this vision requires a secure foundation capable of withstanding emerging threats, including those posed by quantum computing. Without quantum-resistant, crypto-agile security, the NAS cannot achieve the reliability, performance, or international leadership required in the decades ahead. FAA therefore views PQC not as a compliance exercise, but as a foundational enabler of modernization—one that must be embedded into every vendor solution, every system upgrade, and every step of the Brand New Air Traffic Control System ("BNATCS")[1].

Specifically, this RFI seeks industry input on the challenging and mandatory transition of both FAA enterprise IT and FAA NAS safety-critical ATC systems to quantum-resistant algorithms to meet federal mandates, while managing the high cost, complex recertification, and potential operational disruption of integrating new cryptography into FAA operations. The Government is also seeking information regarding the most effective architecture for the enterprise-wide transition to PQC. As National Institute of Standard (NIS) standards continue to finalize, the Government is evaluating the feasibility of a "One-Stop Shop" (Integrated Suite) approach versus a "Best-of-Breed" (Modular Component) approach. The goal is to ensure FAA NAS and FAA non-NAS systems remain "crypto-agile" while minimizing implementation risks and interoperability gaps. FAA recognizes that the PQC market is still maturing and that potential vendors may not currently possess the internal capability to execute a fully integrated solution. Specifically, the FAA acknowledges that:

- A single provider may not have validated all necessary cryptographic primitives across all hardware and software layers.

[1] https://www.faa.gov/new-atcs

- A provider's offerings may not support both FAA Information Technology (IT) and FAA Operational Technology (OT) systems.
- Integration of PQC into legacy National Airspace System (NAS) infrastructure or legacy FAA business infrastructure may require specialized expertise that exceeds the scope of a single product suite.

1.2 REQUEST FOR INFORMATION (RFI) ONLY.

This RFI is issued solely for information and planning purposes and does not constitute a Request for Proposal (RFP) or a promise to issue an RFP in the future. Your response will be treated as information only, and it shall not be used as a proposal. This RFI does not commit the Government to contract for any supply or service whatsoever.

The Government is not, at this time, seeking proposals and will not accept unsolicited proposals. Respondents are advised that the Government will not reimburse any costs associated with preparing or submitting a response to this RFI. Submission of a response does not guarantee participation in any future solicitation or resulting contract award. Information obtained through this RFI may be used to inform the FAA's acquisition strategy for PQC modernization. The FAA, at its sole discretion, may contact one, some, all, or none of the respondents to the RFI and ask for additional information.

1.3 GOVERNMENT POINTS OF CONTACT

Jackson LeMay
Contract Specialist
Jackson.T.LeMay@faa.gov

Kristin Frantz
Contracting Officer
Kristin.T.Frantz@faa.gov

1.4 RESPONSE INSTRUCTION

Vendors are requested to respond to the questions in Section 3 in a clear, concise, and thorough manner.

Responses to this RFI must be received electronically by email to the government points of contact in Section 1.3 above no later than 4:00 PM Eastern Time on April 10, 2026 . Responses received after this date and time may not be considered. The email subject line MUST adhere to the following format: RFI Response: [697DCK-26-RFI-PQC– Company Name].

ZIP files, executable files (.exe), or links to external cloud storage drives will NOT be accepted for security reasons.

Responses must use a standard 11-point font (e.g., Times New Roman, Arial, or Aptos) with at least 1-inch margins on all sides. All pages must be sequentially numbered. The total response (excluding the cover page, table of contents, and proprietary legends) should NOT exceed 30 pages in length. The Government reserves the right to disregard any content beyond the 30-page limit. All content responding to RFI questions, diagrams, charts, graphs, and executive summaries ARE included in the page count. The following are excluded from the total page count: Cover Page, Table of Contents, Corporate Background/PQC Expertise, and Glossary/Acronym List.

1.5 PROPRIETARY INFORMATION

Respondents are strongly advised not to include in their responses any (1) information that they consider to be a trade secret (as defined under the Trade Secret Act (18 U.S.C. § 1905)) and (2) commercial or financial information that is privileged or confidential ("Proprietary Information"), unless such information is essential for the Government to evaluate the response. Respondents grant to the Government unlimited rights to use, modify, reproduce, release, perform, display, or disclose the information contained in the responses, except for Proprietary Information. Respondents grant to the Government limited rights to use, modify, reproduce, release, perform, display, or disclose Proprietary Information for government purposes, including competitive procurement. Government purposes do not include public disclosure.

Proprietary Information submitted in response to this RFI must be clearly and conspicuously marked. Proper marking is necessary for the Government to identify Proprietary Information as such, including for exemption from the public disclosure requirements under the Freedom of Information Act (5 U.S.C. § 552) (FOIA), specifically Exemption 4 (which protects against public disclosure of trade secrets and confidential commercial or financial information). The marking should be included in the transmittal page and on each page of the response clearly and with specificity identifying therein the Proprietary Information. Responses without appropriate markings will be treated as having been submitted with unlimited rights. The Government will not be liable for any use, disclosure, release, reproduction, modification, display and/or performance of any Proprietary Information not properly marked by the vendor.

If the submission contains any proprietary information, a second, redacted version suitable for public release MUST also be provided as a separate PDF file. The file name for the redacted version must be clearly marked: RFI_ 697DCK-26-RFI-PQC_[Company Name] _PublicRelease.pdf.

2 POST-QUANTUM CRYPTOGRAPHY (PQC) MIGRATION FOR FAA INFORMATION TECHNOLOGY AND NAS AIR TRAFFIC CONTROL (ATC) SYSTEMS

The migration of Federal Aviation Administration (FAA) systems, encompassing both enterprise Information Technology (IT) and the safety-critical National Air Space (NAS) infrastructure, to Post-Quantum Cryptography (PQC) represents an immediate and foundational security imperative. The transition to enhanced cryptography is paramount due to the nature of FAA operations and the focus on safety, security, data integrity, confidentiality, and system authentication. This transition must be initiated now, given the inherent conflict between the rapid progression toward cryptographically relevant quantum computers (CRQC), which some projections estimate may appear in less than 10 years, and the characteristically slow, multi-year integration timelines required for the deployment of new cryptographic algorithms across large, complex information systems

The industry responses to this RFI will help to inform FAA of the development of cost estimates required by the Office of Management and Budget (OMB) for strategic planning and resource allocation. Introducing PQC, which may necessitate deep structural modifications to both hardware and software across the NAS, could profoundly affect the projected benefits, costs, and timelines of ongoing Air Traffic Control (ATC) System improvements. This RFI explicitly requests vendor analysis on the potential disruption or delay caused by PQC insertion into both NAS ATC as well as FAA Information Technology systems.

Since FAA is currently in the fact-finding phase of its transition to PQC, it is not committed to any specific procurement model and is evaluating the feasibility of both a "One-Stop Shop" (Integrated) approach and an "Individual Component" (Modular) approach.

- Model A: Integrated Enterprise Solution (One-Stop Shop)

In this model, a single lead integrator or vendor provides a comprehensive, pre-validated PQC suite including algorithm implementation, key management, and hardware integration. The Government is interested in understanding the trade-offs regarding vendor lock-in versus the speed of deployment and simplified compliance auditing.

- Model B: Modular Component/Subsystem Approach

In this model, the Government would source individual subsystems—such as NIST-standardized Key Encapsulation Mechanisms (KEMs), Digital Signature algorithms, and PQC-ready Hardware Security Modules (HSMs) from specialized providers. The Government seeks information on how "crypto-agility" is best maintained in this model and the potential challenges regarding multi-vendor interoperability.

The FAA transition to PQC applies to both FAA Information Technology (IT) and Operational Technology (OT) systems. FAA OT systems refer to the hardware and software that directly monitors or controls physical aviation assets. FAA IT systems refer to hardware and software systems that focus on the flow of information, administrative tasks, and "non-real time" aviation data. A more detailed discussion of FAA OT systems may be found in Section 2.1, and a more detailed discussion of FAA IT systems may be found in Section 2.2

2.1 THE NAS OPERATING ENVIRONMENT

The NAS, operated by the FAA Air Traffic Organization (ATO), is the most complex and busiest air traffic system in the world, overseen by the FAA. It is not merely the sky over the United States; it's a vast, integrated network of airspace, navigation facilities, equipment, services, airports, and the human and regulatory infrastructure required to manage civil, commercial, and military aviation safely and efficiently. It refers to the hardware and software that directly monitors or controls physical aviation assets. The core mission of the NAS is to protect persons and property on the ground and to ensure the safe, orderly, and efficient movement of over 45,000 flights and millions of passengers daily across 29 million square miles.

2.1.1 Airspace Operations

The NAS is divided into various classifications of controlled and uncontrolled airspace (Classes A, B, C, D, E, and G), each imposing specific requirements on pilots for communication, equipment, and flight procedures. All operations are governed by either Visual Flight Rules (VFR) for clear weather conditions or Instrument Flight Rules (IFR), which allow for flight in all weather and require strict separation services provided by ATC. Maintaining separation between aircraft, monitoring weather conditions, and providing pilots with essential aeronautical information like Notices to Airman (NOTAMs) are among the most critical daily functions.

2.1.2 Key Infrastructure Components and Function

The NAS operates through a highly distributed and redundant infrastructure composed of both physical facilities and complex electronic systems. The system is geographically segmented, managed by various ATC facilities:

- Air Traffic Control Towers (ATCTs): Manage aircraft on the ground and in the immediate vicinity of an airport (terminal area).
- Terminal Radar Approach Control (TRACON) facilities: Manage arriving and departing aircraft within a 30–50-mile radius of a major airport.

- Air Route Traffic Control Centers (ARTCCs or "Centers"): Manage aircraft at a high altitude, enroute environment (above 18,000 feet MSL). The entire US is divided into 20 contiguous ARTCC sectors.
- Air Traffic Control System Command Center (ATCSCC): The central hub responsible for national traffic flow management, balancing air traffic demand with system capacity in real-time to mitigate delays caused by weather, equipment outages, or congestion.

These facilities rely on an expansive network of technology, including over 400 radar sites, 40,000 ground radios, navigation aids (like Very High Frequency Omnidirectional Range(VOR) / Distance Measuring (DME)), and a dedicated, highly available telecommunications network (the FAA Telecommunications Infrastructure (FTI)) which relies on classical cryptographic standards for link and data confidentiality) to ensure continuous, high-availability operation across thousands of sites, many of which are remote.

To meet the demands of increasing air traffic and replace aging, ground-based radar and analog systems, the FAA has implemented and deployed various system enhancements and has recently contracted for a "BNATCS"[2]. This is a multi-billion-dollar initiative transforming the NAS into a satellite-based system centered on Trajectory Based Operations (TBO). Key elements of the current NAS include:

- Automatic Dependent Surveillance-Broadcast (ADS-B): Uses GPS technology for precise, continuous, satellite-based surveillance, allowing pilots and controllers to see traffic with greater accuracy than traditional radar.
- Data Communications (Data Comm): Supplements voice communication with digital text-based messages between controllers and pilots, which reduces read-back errors and improves radio frequency efficiency.
- System Wide Information Management (SWIM): A vast, secure data network that allows all NAS users (FAA, airlines, pilots) to share real-time flight, weather, and airport information.

While full implementation is projected to continue toward 2030, the enhancements are intended to increase airspace capacity, reduce delays, save fuel, and ensure the NAS can safely integrate new technologies like unmanned aircraft systems (UAS/drones) and commercial space operations.

---

[2] The contract to serve as the Prime Integrator for this ambitious, multibillion-dollar effort was recently awarded to Peraton. Key aspects of the project include replacing core infrastructure, including telecommunications networks, radar, software, and hardware, to create a state-of-the-art, resilient system. The FAA is currently targeting the end of 2028 for the implementation of the new system. Immediate work includes transitioning the system's remaining copper infrastructure to modern fiber and establishing a new digital command center

2.1.3 Core Technologies

The core ATC systems can be categorized by the phase of flight they manage: En Route, Terminal, Surface, and Support

2.1.3.1 Enroute

Enroute Automation Modernization (ERAM) is the main automation platform for high-altitude (enroute) air traffic control. It is responsible for air traffic control across the high-altitude, enroute airspace managed by 20 centers in the Continental United States. It integrates surveillance data (including radar and ADS-B), flight plan data, and weather information to provide controllers with a comprehensive picture of all traffic in their sector. It includes tools to help predict conflicts and manage traffic flow more efficiently, supporting the transition to more flexible routes enabled by GPS-based navigation. The Advanced Technologies & Oceanic Procedures system is used in the oceanic air traffic control centers to manage traffic over the oceans, where traditional radar coverage is unavailable. It uses satellite-based position reports and digital communication to maintain safe separation.

Flight Management Data System (FMDS) is a critical system used in the modern aviation operating environment to modernize the handling of digital flight data. It manages and distributes real-time, comprehensive flight trajectories and associated information necessary for trajectory-based operations, which significantly increases data volume and reliance on the NAS network backbone.

2.1.3.2 Terminal Area Systems

Standard Terminal Automation Replacement System (STARS) is the core system used at Terminal Radar Approach Control (TRACON) facilities and many airport towers, which manage air traffic for the approach and departure phases of flight, typically within about 50 miles of an airport. It integrates surveillance data to track aircraft as they transition between the enroute environment and the airport surface. STARS provides the air traffic controller with a graphical display of aircraft position, altitude, speed, and identification. STARS serves as the common terminal automation platform, supporting TRACON facilities and associated ATCT as well as Department of Defense facilities

2.1.3.3 Airport Surface Systems

Airport Surface Detection Equipment (ASDE), Model X (ASDE-X) and the newer Airport Surface Surveillance Capability (ASSC) are crucial safety tools used by tower controllers to monitor the movement area.

ASDE-X is a runway safety tool that provides controllers with a highly detailed, continuous map of all aircraft and transponder-equipped vehicles moving on runways and taxiways. It fuses data from surface

movement radar, multilateration[3] sensors, and ADS-B to precisely determine position and identification. Its key function is to detect and issue visual/aural alerts for potential runway conflicts (runway incursions), especially helpful in low-visibility conditions.

2.1.3.4 Core Surveillance and Communication Technologies

These systems provide the essential data for the automation platforms listed above. Automatic Dependent Surveillance–Broadcast (ADS-B) is a satellite-based surveillance technology where an equipped aircraft determines its position via GPS and regularly broadcasts this data (identification, position, velocity) to other aircraft and ground stations. While the broadcast data is currently unencrypted, its identity and integrity are protected using classical authentication schemes. It's the foundation of the modern aviation operating environment surveillance, providing more precise and continuous coverage than traditional radar, especially in areas with challenging terrain.

Data Communications (Data Comm) enables controllers and pilots to exchange routine text-based messages (like departure clearances and reroutes) to supplement traditional voice communication. Data Comm uses the Controller-Pilot Data Link Communications (CPDLC) protocol, to ensure message authenticity and confidentiality. This reduces radio frequency congestion, minimizes miscommunication errors from similar-sounding call signs, and allows controllers to manage more tasks efficiently. Any PQC transition plan must include a strategy for migrating the digital signature mechanism for ADS-B Broadcast Authentication (ADS-B-AUTH) to PQC to counter quantum-enabled identity spoofing.

The NAS relies heavily on Global Navigation Satellite Systems (GNSS) like GPS. The integrity and authentication of GNSS correctional signals is paramount. Wide Area Augmentation System (WAAS) is a crucial satellite-based augmentation system that provides GPS signal correction and integrity information to pilots, enabling precision approaches. The system's integrity and authentication data are secured using classical digital signature algorithms to prevent unauthorized modification or spoofing, which is critical for flight safety.

Runway Status Lights (RWSL) RWSL is an advisory safety system that uses automated red lights embedded in the pavement of runways and taxiways. These lights automatically illuminate warning pilots and vehicle operators when it is unsafe to enter, cross, or take off from a runway, based on information from the ASDE-X/ASSC surface surveillance systems.

---

[3] Multilateration sensors are devices used in positioning systems to determine the location of an object by measuring the difference in arrival times of a signal at multiple sensor points. Instead of measuring distance directly, they rely on Time Difference of Arrival (TDOA).

2.1.4 Support Systems

These provide essential, real-time information for safe air travel.

2.1.4.1 Notices to Airman (NOTAMs)

NOTAMs is a vital alert system that provides timely, critical, and time-sensitive information that is not known far enough in advance to be publicized by other means (like aeronautical charts). NOTAMs communicate the real-time and abnormal status of any component (facility, service, procedure, or hazard) within the NAS that impacts flight operations. They cover a vast array of information, including:

- Airport Conditions: Runway closures, taxiway issues, temporary lighting outages, and surface conditions (like snow, ice, or water).
- Airspace Restrictions: Temporary Flight Restrictions (TFRs) for things like presidential movement, natural disasters, or major public events.
- Navigation Aids (NAVAIDs) Status: Outages or unreliability of radio navigation beacons.
- Procedures: Changes to instrument approach procedures.

The FAA is currently modernizing the NOTAM system through the Aeronautical Information Management Modernization (AIMM) program. The new NOTAM Management Service (NMS) is a cloud-based system designed to replace the outdated legacy system, provide near-real-time data exchange and use a modern, streamlined interface to enhance safety and efficiency.

2.1.4.2 Weather Systems

Accurate and current weather information is paramount for aviation safety. The FAA relies heavily on two primary automated systems for weather data at airports The first is Automated Surface Observing System (ASOS) ASOS \provides a comprehensive, continuous, real-time weather observation system, primarily used at larger airports. The data provided includes Wind speed and direction, visibility, cloud height and sky cover, temperature, dew point, altimeter setting, and type and intensity of precipitation (rain, snow, freezing rain). It generates reports hourly, with "special" reports issued for rapidly changing conditions.

The second is Automated Weather Observing System (AWOS). AWOS provides automated weather observations, often used at smaller airports and heliports. It generally focuses on basic parameters like wind speed and direction, temperature, dew point, altimeter setting, and visibility. The weather data is typically broadcast to pilots over a radio frequency via a computer-generated voice message, updated at least once per minute.

2.1.4.3 System Wide Information Management (SWIM)

SWIM is the digital data-sharing backbone infrastructure that connects and shares information between all the disparate systems, including NOTAMs and weather. SWIM provides a secure platform for all aviation stakeholders (pilots, air traffic controllers, airlines, dispatchers, etc.) to access a single, consistent source of real-time information. This secure platform relies on Public Key Infrastructure (PKI) and classic cryptographic protocols to authenticate users and encrypt the massive volume of shared data. It delivers and harmonizes vast amounts of data, including:

- Aeronautical: Digital NOTAMs and airspace status.
- Weather: Specialized weather products and real-time airport weather data.
- Flight/Flow: Flight plans, track data, and air traffic flow information.
- Enhanced Situational Awareness:

By ensuring everyone is operating off the same, current data, SWIM improves decision-making and overall safety and efficiency throughout the NAS.

Currently SWIM is operating over the FAA FTI, FTI will be replaced by the FAA Enterprise Network Services (FENS) with further enchantments FENS, and elements of the "BNATCS", will serves as the consolidated, secure digital network backbone providing voice, data, and video communications across the FAA's entire enterprise and the NAS environment, including ARTCCs, Towers ATCTs, and Technical Centers. As the successor to FTI, FENS must support high-reliability, low-latency, and high-availability standards for mission-critical ATC systems. Migration to PQC must ensure that all FENS and BNATCS-managed connectivity services, including VPNs and transport layer security, transition seamlessly to quantum-safe algorithms to protect the fundamental communication integrity of the NAS.

2.2 THE NON-NAS OPERATING ENVIRONMENT

The FAA non-NAS Information Technology (IT) systems, often referred to as FAA Enterprise IT, is operated by the FAA Office of Information & Technology Services (AIT). This is the critical infrastructure that supports the agency's administrative, business, research/development, and regulatory functions. While the NAS systems handle the real-time, safety-critical mission of air traffic control, Enterprise IT provides the essential foundation for the rest of the agency's operations. FAA Enterprise IT generally comprises the systems necessary for the agency to operate as a large federal organization and a major regulatory body. These functions include:

- Administrative and Business Systems: This covers core agency functions such as human resources (HR), finance, procurement, legal services, and general data management. These systems ensure

the FAA can manage its massive budget, pay its thousands of employees (including controllers and technicians), and manage the acquisition of new systems and services.

- Regulatory and Safety Oversight Systems: These are the systems that support the FAA's role in certifying aircraft, pilots, and maintenance facilities. They manage licenses, records of airmen, track safety data, and administer rulemaking processes (like the proposed rule on drones mentioned in the search snippets). These systems are crucial for maintaining aviation safety standards outside the immediate air traffic control process.
- General IT Infrastructure: This includes the network backbone, email, desktop computing environments, and cybersecurity defenses that protect the entire FAA corporate digital environment. This infrastructure connects employees, supports general office work, and secures the agency's non-operational data.

A defining feature of the FAA's overall IT infrastructure is the strict logical and physical separation between the NAS and Non-NAS environments, primarily for safety and security: The NAS operational network is designed to be highly secure and is typically physically isolated from the public internet and the FAA's general business network (the non-NAS environment). Communication between the two environments is heavily controlled and occurs only through secure, defined pathways and firewalls, often referred to as boundary protection systems. This prevents non-critical systems from introducing risk to life-critical air traffic control systems.

2.3 TECHNICAL REQUIREMENTS AND CONSIDERATIONS

When responding to this RFI, vendors should be aware that FAA must prioritize factors that go beyond baseline technical compliance, focusing on strategic alignment with the NAS's unique safety, complexity, and longevity requirements. This vital national asset is increasingly threatened by its reliance on infrastructure based on outdated technologies that are demonstrably unable to meet modern demands. The complexity is compounded by a rapidly evolving sector, including commercial air travel returning to pre-COVID levels and the rapid growth of new airspace users, such as drones, Advanced Air Mobility (AAM), and commercial space operations.

The FAA strategic goal is to mitigate future, unpredictable risks for both IT and OT systems. Rigid cryptography creates massive technical debt; when a future cryptanalytic breakthrough occurs, the alternative to agility is often a costly, multi-year, multi-billion-dollar system overhaul or replacement. Agility prevents this wasteful spending by making system protection a manageable software/firmware update rather than a catastrophic hardware rebuild, thus protecting the government's investment and extending the operational life of the FAA's mission-critical infrastructure. This capability is vital not only for the current migration to PQC standards but also for addressing future unknown threats, responding quickly to new compliance mandates (e.g., from NIST or CISA), and correcting potential zero-day vulnerabilities in deployed algorithms. The transition to PQC is a concern for both NAS and non-NAS systems.

2.3.1 NAS (Operational) Safety and Real-Time Mission

The immediate concern is the integrity and availability of critical, real-time links (like Data Comm) and the need for cryptographic agility in systems with decades-long lifespans. The systems discussed—ERAM, STARS, ADS-B, SWIM, and NOTAMs—rely on a backbone of digital communications and cryptography to ensure data integrity and confidentiality. Everything from a pilot receiving a clearance via Data Comm to the precise position data broadcast by ADS-B is secured using current non PQC standards. The looming threat of a powerful, fault-tolerant quantum computer would break these classical cryptographic standards, compromising the entire network. Therefore, PQC acts as the necessary, next-generation security layer. Integrating PQC algorithms into the system's infrastructure—particularly within the SWIM data-sharing environment and the physical communication links for ERAM and STARS—is the critical step required to ensure that the aviation data used for air traffic control remains secure and trusted for decades to come, protecting the NAS from future quantum-enabled cyberattacks.

2.3.2 Non-NAS (Enterprise IT) Confidentiality of Long-Lived Data

The concern is the "Harvest Now, Decrypt Later" (HND) threat, which applies strongly to long-term sensitive data, such as personally identifiable information (PII) for employees and regulated personnel, proprietary acquisition data, future budget and planning documents, and long-term safety/regulatory records that must remain confidential for decades. .

Vendors must utilize NIST-standardized PQC algorithms for all new acquisitions and system updates. All cryptographic modules must be validated against FIPS 140-3 to ensure a uniform security posture across the entire FAA infrastructure. For OT systems this means protection of real-time satellite data-link communications and terrestrial/satellite navigation signals (WAAS, LAAS). For IT systems this means protection of sensitive administrative, financial, and personnel data. Systems must be designed to swap or update algorithms with minimal disruption. For OT systems this is essential for avoiding multi-year, multi-billion-dollar replacement cycles in the NAS when a specific cryptographic primitive is compromised. For IT systems this ensures seamless security patches in cloud and enterprise environments without long-term downtime.

2.3.3 Legacy Systems and Cost

A major challenge is the FAA's reliance on decades-old, custom-built systems where cryptographic algorithms are often hard-coded into hardware or firmware. Upgrading these components to support PQC is a significant undertaking, often requiring complete system replacement rather than simple software patching. Unlike a one-time upgrade (like Y2K), the transition to PQC is expected to be a continuous, ongoing process that requires sustained resources for maintenance, updates, and monitoring of new PQC standards. Due to the decades-long lifespan of NAS infrastructure, the FAA requires a complete Software Bill of Materials and rigorous vetting of third-party libraries. Vendors must demonstrate financial health to

support systems for 20+ years. Vendors are also expected to provide hands-on training for FAA engineers and controllers to ensure the internal capacity to sustain both PQC-enabled NAS OT systems and PQC enabled IT systems.

2.3.4 Technical and Performance Constraints

PQC algorithms, while quantum-resistant, often have larger key and signature sizes compared to their classical counterparts with potential impacts of these larger sizes on system performance, memory, and bandwidth critical issues in time-sensitive air traffic control and data-link communications.

2.3.5 Interoperability and Standardization

A crucial challenge for the FAA and its vendors is maintaining seamless global interoperability with international Air Navigation Service Providers (ANSPs) and the global commercial aircraft fleet. PQC migration efforts must be coordinated internationally to ensure aircraft can transition smoothly across national airspace boundaries and communicate securely, which is complicated by varying PQC adoption timelines and different national strategies. Radio Technical Commission for Aeronautics (RTCA) Special Committee 214 (SC-214) European Organization for Civil Aviation Equipment. (EUROCA) Working Group 67 (WG-67) are undertaking efforts in updating current protocols for PQC. These bodies are actively defining the profile of PQC algorithms (e.g., hybrid modes, parameter sets) that will be mandated for aircraft avionics. Compliance will be required not just with the NIST algorithms themselves, but with the aviation community's mandated PQC profiles for specific protocols. While NIST has selected some initial PQC standards, the broader ecosystem-wide adoption of these standards into common communication protocols and production-grade libraries is an ongoing effort that vendors must track and integrate.

2.3.6 Certification and Oversight

The introduction of new, highly sensitive cryptographic systems into the NAS requires vendors to navigate the FAA's rigorous and often lengthy aircraft and system certification processes. Integrating PQC must be proven safe, reliable, and compliant with all relevant safety standards, a process that is critical for mission-critical ATC system. FAA oversight of certification tasks can add complexity and time to the approval of new PQC-enabled systems and software updates. For OT systems integrators must demonstrate deep expertise in the FAA safety assurance process. PQC compliance with RTCA DO-178C (Software) and DO-254 (Hardware). Recertification costs and timelines must be modeled according to the specific Design Assurance Level (DAL) of the system

2.3.7 Integration and External Factors

The implementation and deployment of PQC into the NAS poses a significant risk due to the need to integrate PQC into the long-term, evolving Future NAS architecture centered on Trajectory Based

Operations (TBO) and the yet to be defined replacement Air Traffic Control System. PQC operations must exhibit minimal overhead (ideally <5% increase) compared to classical systems on target NAS hardware. Given the age of legacy NAS hardware, solutions must minimize CPU and memory footprints through assembly-level optimizations or hardware accelerators.

TBO requires sub-millisecond, real-time cryptographic operations for continuous, dynamic trajectory sharing, which conflicts directly with the generally higher computational cost and larger data sizes of PQC algorithms. The PQC solution must be developed and certified before the final architecture and specific hardware for the automation replacement system (Future NAS) are fully finalized and deployed, creating an unstable integration target. Integrating new PQC libraries into the core ATC automation code, which often falls under the highest Design Assurance Levels (DAL A/B), necessitates highly rigorous and costly RTCA DO-178C recertification for every cryptographic change.

The replacement Air Traffic Control system envisioned by the current administration is not a singular project but the critical acceleration and refinement of current and planned initiatives. It is defined by the core operational objective of Trajectory Based Operations (TBO), which replaces tactical vectoring with strategic, optimized 4-D flight path management. This operational paradigm rests atop an information-centered, service-oriented architecture, with a shared digital backbone for secure data exchange. Foundational automation systems such as ERAM and STARS are strategically retained and enhanced to host TBO capabilities.

2.3.8 Phased Deployment

Implementing a PQC transition within the FAA is not merely a software update; it is a massive logistical and budgetary undertaking. Success depends on the availability of three critical resources: Capital Funding, Technical Workforce, and Hardware Lifecycle Synchronization. The FAA's transition to Post-Quantum PQC is currently planned to be executed as a multi-stage modernization effort. By 2027, the agency will launch a Pilot Program (with a system to be determined) to test PQC-integration in a live data environment before scaling to the broader FAA IT and NAS OT systems. The subsequent deployment after the pilot is organized into "waves" grouping systems by their operational criticality and "sustainability" as defined by the Government Accountability Office (GAO's) 2024/2025 assessments.

2.3.8.1 Phase I: The 2027 Pilot

The goal of the pilot is to demonstrate that NIST-standardized PQC algorithms can be integrated into cloud-based safety databases without degrading data retrieval speeds or cross-agency sharing. The 2027 Pilot Program is a "proving ground" designed to de-risk the massive transition of the NAS and FAA Business IT systems. By starting with a pilot system, the FAA aims to meet four primary objectives.

- Validation of Cryptographic Agility

- Mitigation of "Harvest Now, Decrypt Later" Threats
- Performance Benchmarking (Latency Ceilings)
- Safety Certification & "Fail-Safe" Verification

2.3.8.2 Phase II: Wave-Based Rollout (2028–2036)

Following the 2027 pilot, remaining IT and OT systems will be modernized in "Cohorts" based on their risk level and impact on flight safety and business operations

3 VENDOR QUESTIONS FOR PQC TRANSITION

The FAA is embarking on a once-in-a-generation transformation of the NAS and its supporting ATC infrastructure. As outlined by Secretary of Transportation, Sean P. Duffy, the vision is for a modern, resilient, and globally leading ATC system—one that controllers can fully trust, that integrates new entrants such as drones, Advanced Air Mobility (AAM), and commercial space operations, and that positions the United States as the benchmark for aviation safety and efficiency worldwide.

Achieving this vision requires more than incremental upgrades. It demands a secure, future-proof foundation capable of withstanding emerging threats, including those posed by quantum computing. PQC is therefore not simply a technical requirement; it is a strategic enabler of the FAA's modernization priorities. PQC migration must be approached with the same rigor, foresight, and international coordination as Trajectory Based Operations (TBO) initiatives.

Parallel to the evolution of the NAS, the FAA is concurrently modernizing its broader IT systems to provide the enterprise-level backbone necessary for administrative and mission-support functions. These IT systems, while segregated from the mission-critical NAS to maintain operational integrity, provide the essential connectivity, data analytics, and cloud-based environments that allow the agency to function as a unified enterprise. The migration to PQC within the IT domain focuses on safeguarding sensitive personnel data, financial records, and internal communications against future decryption threats.

The segregation of the IT systems from the NAS ensures that enterprise-wide security updates or administrative patches do not interfere with the high-availability requirements of real-time air traffic management. By maintaining these distinct environments, the FAA can implement agile IT solutions—such as zero-trust architecture and automated endpoint protection—without compromising the stringent certification and safety standards of the NAS. This dual-track approach ensures that while the NAS handles the specialized "state" of the airspace, the IT systems handle the global "flow" of agency information with equal resilience.

Accordingly, the FAA requests that vendors provide detailed responses demonstrating how their PQC strategies align with and support the following FAA modernization imperatives: the replacement of legacy systems with modern, crypto-agile architectures; real-time performance to meet TBO and operational demands; and seamless global interoperability with international partners and fleets. Proposals must also address rigorous certification and oversight processes to ensure safety and reliability, secure supply chains with a trained workforce capable of sustaining PQC adoption, and long-term adaptability to evolving standards and emerging threats.

The FAA emphasizes that PQC product readiness will be evaluated not only on technical compliance, but also on strategic alignment with the NAS's unique safety, complexity, and longevity requirements, as well as the IT system's need for enterprise-wide scalability. Vendors are encouraged to provide forward-looking insights, lessons learned, and innovative approaches that will help ensure both the mission-critical NAS and supporting IT systems remain the safest, most efficient, and most resilient in the world.

3.1 TECHNOLOGY TIERS SUPPORTED

The FAA seeks to understand the impact PQC integration across the following architectural tiers. Respondents should identify which tier or tiers their technology supports and if their solution provides a "One-Stop Shop" (Model A) or a "Component" (Model B). (Table 1)

Table 1: Technology Tiers

Tier	Example Devices/Systems	Envisioned Capability
Root of Trust (Hardware)	HSM Servers, TPM 2.0+, Smart Cards	Hardware-based generation of NIST FIPS 203/204 keys; support for "Hybrid Key Wrapping" (PQC + Classical).
Compute and Infrastructure	Web Servers, App Servers, Database Clusters	CPU-optimized PQC libraries (e.g., OpenSSL 3.5+); support for large-packet handshakes without timeout
Networks and Gateways	VPN Concentrators, Firewalls, SD-WAN	Support for "Hybrid IKEv2/IPsec" tunnels; hardware acceleration (FPGA/ASIC) for line-speed PQC encryption.
Cloud Services	KMS, SaaS Platforms, Virtual HSMs	Managed PQC key lifecycles; interoperability with on-premises PQC roots of trust via standardized APIs.
Edge & Endpoints	IoT Sensors, EFB (Electronic Flight Bags), Avionics	Lightweight PQC implementations for resource-constrained hardware; secure remote firmware signing via SLH-DSA.

For each technology tier identified above that your product(s) supports, please address the following core questions as well as NAS Specific and Enterprise specific system questions as applicable. Because the FAA has not yet finalized its acquisition strategy, respondents are encouraged to provide realistic assessments of their current capabilities. Please specify your organization's capability to support FAA

modernization by indicating whether your solution addresses IT (Business Systems), OT (NAS/ATC Systems), or both IT and OT domains:

- For IT-Only Capabilities: please explain how your PQC solutions would integrate with FAA enterprise business logic, cloud-based mission support systems, and administrative data protection standards without disrupting agency-wide data flows.
- For OT-Only Capabilities: please explain how your solutions would integrate in the National Airspace System (NAS) environment, specifically addressing real-time safety constraints, low-latency requirements for ATC operation, and compliance with RTCA DO-178C/DO-254 hardware and software standards.
- For Integrated IT and OT Capabilities: Please explain your comprehensive strategy for securing the convergence of mission support and air traffic operations, ensuring that PQC-enabled gateways maintain strict logical separation while allowing for the secure, cross-domain data exchange required by BNATCS initiatives.

3.2 PQC ALGORITHM AND IMPLEMENTATION DETAILS

3.2.1 Shared Questions (Common Core)

3.2.1.1 Algorithm Spec:

- Which NIST-selected PQC algorithms are implemented? State security levels (e.g., FIPS 140-3) and library versions.

3.2.1.2 Cryptographic Agility:

- Describe the mechanism for switching algorithms or updating parameters via software without a new hardware baseline.

3.2.1.3 FIPS Validation:

- Provide evidence of FIPS 140-3 validation or a detailed timeline and plan for the specific module under validation.

3.2.1.4 Seed Protection:

- Detail how PQC cryptographic seeds are protected from unauthorized access and side-channel leakage during derivation and storage.

3.2.2 NAS-Specific Questions (Safety-Critical/OT)

3.2.2.1 NAS Key Management:

- Detail integration with the NAS Enterprise Hardware Security Modules (HSM). Describe the key lifecycle specifically for high-availability aviation data.

3.2.2.2 OT Performance Optimization:

- Specify if the NAS implementation uses Assembly-level optimizations to meet deterministic real-time requirements.

3.2.3 Enterprise IT Questions (Administrative)

3.2.3.1 IT Key Management:

- Detail integration with Enterprise Key Management Infrastructure (EKMI) for administrative functions like HR and personnel records.

3.2.3.2 Implementation Type:

- Specify if the IT implementation is a "Reference" or "Optimized C" build suited for cloud and standard server environments.

3.3 INTEROPERABILITY AND SYSTEM INTEGRATION DETAILS

3.3.1 Shared Questions (Common Core)

3.3.1.1 Protocol Engineering:

- How does your TLS 1.3/IKEv2 handle hybrid key exchanges? Is there a deterministic fallback to classical crypto if a PQC handshake times out?

3.3.1.2 Connectivity:

- How do you prevent IP fragmentation on legacy links? Do you support Certificate Compression (RFC 8879) to keep handshakes within a single Maximum Transmission Unit (MTU)?

3.3.1.3 Pluggable Crypto:

- Does the system support swapping NIST algorithms for sovereign-approved alternatives without a full software re-build?

3.3.1.4 Asset Inventory:

- What methodology would your firm use to perform a comprehensive inventory of all cryptographic assets within the FAA's Enterprise IT environment, including Commercial off the Shelf (COTS) products, custom applications, and third-party Software as a Service (SaaS) integration to determine an appropriate PQC solution?
- How would you integrate selected PQC solutions with crypto inventory products?

3.3.1.5 Milestone Based Roadmap

- Provide a recommended milestone-based roadmap for the full transition of your product that aligns with the FAA's Acquisition Management System (AMS)[4] process. The roadmap must include a section identifying all "systems unable to support PQC" upgrades and proposing alternative protection mechanisms (e.g., cryptographic proxy layers).

3.3.1.6 HNDL Data Re-encryption

- Detail the recommended strategy required for protecting long-term secure data storage (data with a required confidentiality lifespan greater than 5 years, e.g., archived flight plan data, security logs) generated by your product. This must include a plan for re-encrypting or migrating this sensitive data to PQC protection.
- Do your products or systems provide automated periodic re-encryption, quantum-safe key rotation services, and data minimization audits (HNDL mitigation)?

3.3.1.7 Post Migration Audit Tools

- Describe recommended new operational tools, metrics, and procedures required by FAA cybersecurity analysts to monitor and audit the deployed PQC infrastructure post-migration.

---

[4] The FAA's Acquisition Management System (AMS) is organized into a set of lifecycle phases that guide how the agency plans, analyzes, acquires, deploys, and sustains systems. There are 5 phases (1) Concept and Requirements Definition (2) Investment Analysis (3) Solution Implementation (4) In-Service Management (5) Service Life Extension or Disposal

3.3.1.8 Deployment Plan

- Describe the recommended deployment plan (e.g., phased regional rollout, concurrent shadow mode, specific ATC facility pilot programs) to minimize disruption and ensure smooth transition to the PQC-enabled product.

3.3.2 NAS-Specific Questions (Safety-Critical/OT)

3.3.2.1 NAS Architecture:

- Describe the architecture for safety-critical apps. Specify placement in ground-to-ground links and how it maintains sub-millisecond latency for TBO.

3.3.2.2 ATN/IPS Support:

- Detail how PQC capability supports the protocol ensuring compatibility with future PQC-equipped ground and aircraft avionics.

3.3.2.3 Legacy OT Isolation:

- Describe your solution (e.g., cryptographic gateway) for isolating the PQC domain from non-PQC legacy systems like older radar.

3.3.2.4 International Compliance:

- Confirm adherence to anticipated International Civil Aviation Organization (ICAO)/ European Organization for the Safety of Air Navigation (Eurocontrol) PQC standard**s** to maintain interoperability and seamless transition for international flights interfacing with your product (e.g., over international air traffic routes).

3.3.3 Enterprise IT Questions (Administrative)

3.3.3.1 IT Architecture:

- Describe the architecture for administrative/cloud functions, focusing on segregation from the NAS.

3.3.3.2 External Enforcement:

- Describe the use of proxies to enforce PQC for FAA data leaving the internal network for third-party cloud/partner networks.

3.3.3.3 IAM Migration:

- Provide a specific plan to migrate mission-critical Identity and Access Management (IAM) and Zero Trust Network Architecture (ZTNA) systems to PQC.

3.3.3.4 Legacy IT System Isolation:

- If your product must communicate with non-PQC legacy FAA systems describe your solution (e.g., cryptographic gateway, protocol proxy) to securely isolate) for isolating the PQC domain from non-PQC legacy systems.

3.3.3.5 Interoperability

- Describe how the PQC implementation adheres to adherence to IT industry standards to maintain interoperability and seamless transition for interfacing with your product.

3.4 PERFORMANCE AND REAL-TIME OPERATIONAL IMPACT DETAILS

3.4.1 Shared Questions (Common Core)

3.4.1.1 Resource Consumption:

- Provide peak Central Processing Unit (CPU) and memory utilization metrics for PQC key exchanges under high load and confirm compliance with existing FAA platform resource utilization ceilings

3.4.1.2 PQC Failover:

- Describe the mechanism if a PQC component fails or degrades. How is a safe return to classical (or degraded) mode ensured and logged?

3.4.2 NAS-Specific Questions (Safety-Critical/OT)

3.4.2.1 OT Benchmarks:

- Provide mean/95th percentile latency data for operations benchmarked on embedded platforms (multi-core microcontrollers) for ATC functions.

3.4.2.2 Message Overhead:

- Quantify the increase in message size for control messages or radar returns. Confirm these will not lead to packet fragmentation.

3.4.3 Enterprise IT Questions (Administrative)

3.4.3.1 IT Performance Mitigation:

- How will the solution address performance impacts on administrative network traffic, particularly for high-volume data transfers or internal IPsec/TLS tunnels?

3.4.3.2 HNDL Prioritization:

- How does your migration plan prioritize data based on confidentiality lifespan (e.g., decades-long Human Resource (HR) /financial records) to mitigate "HNDL" threats?

3.5 SOFTWARE AND SUPPLY CHAIN RISK MANAGEMENT DETAILS

3.5.1 Shared Questions (Common Core)

3.5.1.1 Side-Channel Analysis:

- Provide evidence of hardware-layered Data Processing Agreement (DP) resistance and freedom from timing attacks.

3.5.1.2 Emergent Risks:

- Identify all PQC components and the risk mitigation strategy for newly discovered vulnerabilities (rapid patching plan).

3.5.1.3 Root of Trust:

- Detail the roadmap for migrating the System Root of Trust to a PQC digital signature scheme. How are signing keys protected (e.g., offline HSM)?

3.5.1.4 OT Secure Provisioning:

- Detail the process for ensuring embedded chips and Floating Point Gate Arrays (FPGAs) used in equipment are securely provisioned and free of backdoors.

3.5.1.5 Partner Ecosystem:

- Detail your participation in PQC Partner Ecosystems to ensure multi-vendor interoperability for COTS/SaaS enterprise tools.

3.6 COSTS (ROM) DETAILS

3.6.1 Shared Questions (Common Core)

3.6.1.1 Rough Order of Magnitude (ROM) Pricing

The Government requests a ROM estimate for the implementation of your proposed solution or capability segmented by the following federal reporting categories: Cryptographic Inventory, Risk Prioritization Assessment, Remediation (Hardware/Software Replacement), Re-encryption of Data Archives, and Testing/Certification (including DAL compliance). Respondents should categorize costs according to the following structure to assist the FAA in comparing Model A and Model B financial impacts:

- Non-Recurring Engineering (NRE): Initial costs for system design, cryptographic inventory/discovery, and custom integration with legacy FAA National Airspace System (NAS) interfaces.
- Hardware Acquisition: Unit costs for PQC-validated HSMs, upgraded gateways, and specialized crypto-accelerator cards.
- Licensing & Software: Per-seat, per-device, or enterprise-wide licensing fees for PQC cryptographic libraries and management consoles.
- Implementation & Deployment: Estimated labor hours for installation, testing, and validation within a high-availability aviation environment.

3.6.1.2 TCO Drivers:

- Model A (Integrated) Efficiency: If proposing/providing an integrated suite, identify the projected cost savings associated with reduced "integration labor" and simplified vendor management.
- Model B (Modular) Lifecycle: If proposing/providing a modular component, estimate the "integration tax" the cost for the FAA to ensure your component interoperates with third-party Certificate Authorities (CAs) or Key Management Systems.
- The "Crypto Agility" Premium: What is the estimated cost difference between a "static" PQC implementation (fixed algorithms) and a "crypto-agile" implementation (capable of rapid algorithm swaps)?
- Parallel Operation Costs: Estimate the cost of maintaining "Hybrid Mode" (Classical + PQC) during the transition period (e.g., dual-licensing or increased compute requirements).

3.6.1.3 Scaling Metrics

- What is the primary cost driver for your solution(s) (e.g., number of endpoints, volume of encrypted traffic, or number of cryptographic keys)?

3.6.1.4 Testing Resources

- Detail the recommended testing and validation resources that FAA should make available including a Non-Operational Test Environment (NOTE) or equivalent, where the FAA can perform stress testing, performance benchmarking, and system-of-systems integration of the PQC implementation

3.6.1.5 Training Costs:

- Is specialized PQC training for FAA staff included in the ROM? If not, what are the training costs for the specialized cryptographic training?
- What specific PQC-focused training and documentation will or should be provided for FAA personnel, including system operators, maintenance technicians, and cybersecurity analysts, to ensure workforce readiness for the new cryptographic primitives

3.6.1.6 Modularity Incentives:

- Do you offer standardized APIs (e.g. PKCS#11, KMIP) at no additional integration fee?

3.6.2 NAS-Specific Questions (Safety-Critical/OT)

3.6.2.1 NAS Remediation Costs:

- What ae the drivers of segment costs for custom integration with NAS interfaces (E-RAM, DataComm) and specialized ATC hardware replacement?

3.6.2.2 Certification Costs:

- What are the drivers of segment costs for achieving Design Assurance Level (DAL) compliance for aviation safety?

3.6.3 Enterprise IT Questions (Administrative)

3.6.3.1 Remediation Costs

- What are the segment costs for enterprise licensing, SaaS integration, and the re-encryption of large-scale administrative archives (HNDL mitigation)?

3.7 VENDOR INSIGHTS

3.7.1 Shared Questions (Common Core)

3.7.1.1 Inter vendor Coordination

- What are the biggest non-technical challenges (e.g., proprietary interface disputes, differing development timelines, conflicting intellectual property) you foresee in coordinating PQC upgrades across the multiple, existing NAS vendors (e.g., vendors for E-RAM, DataComm, etc.) to achieve seamless, end-to-end PQC compatibility?

3.7.2 Certification Challenges

- Beyond FIPS 140-3, what specific Design Assurance Level (DAL) or FAA certification challenges (e.g., RTCA DO-178C, DO-254 for airborne PQC components) do you anticipate will slow the adoption of PQC in safety-critical NAS ground systems or next-generation avionics?

3.7.1.2 Quantum Resistance:

- Describe your defenses against future threats like Quantum Random Access Memory (QRAM) attacks. or other potential future advances in quantum computing that could degrade the security of currently standardized PQC algorithms? Conversely, what non-quantum cryptanalytic

resistance (e.g., specific defenses against known PQC side-channel and timing attacks) is built into your PQC implementation?

3.7.1.3 Joint Acceleration:

- Suggest areas where FAA and industry can jointly accelerate PQC transition readiness.

3.7.2 NAS-Specific Questions (Safety-Critical/OT)

3.7.2.1 NAS Strategy:

- What strategy is recommended to coordinate the PQC upgrade cycle to ensure NAS system operability?

3.7.2.2 NAS-OT Experience:

- Describe previous experience integrating PQC into safety-critical OT environments.

3.7.3 Enterprise IT Questions (Administrative)

3.7.3.1 IT-Enterprise Experience:

- Describe previous experience adapting PQC into large-scale administrative IT enterprise systems.