Replacement of Telecommunications Systems

Federal Aviation Administration

Report Number: FI-2001-076
Date Issued: August 21, 2001

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: **ACTION**: Report on Replacement of Telecommunications Systems, FAA
FI-2001-076

Date: August 21, 2001

From: Alexis M. Stefani
Assistant Inspector General for Auditing

Reply To Attn Of: Meche:x61496

To: Federal Aviation Administrator

This report presents our initial assessment of the Federal Aviation Administration (FAA) plan to replace its telecommunications systems, which is referred to as the FAA Telecommunication Infrastructure (FTI) project. The FTI project was established to replace six owned and leased communications networks because current networks are approaching the end of their contract or service life cycles. The National Airspace System Architecture also requires an upgrade from analog to digital communications to support modernization efforts. The initial life cycle cost for FTI was estimated at $1.9 billion over 10 years.

In 1997, the President's Commission on Critical Infrastructure Protection identified the National Airspace System as a critical national infrastructure. The Commission concluded that the planned modernization effort, including the planned network integration, would increase system vulnerabilities and recommended enhanced security measures.

In 1998, FAA conducted an investment analysis by comparing three alternatives to current telecommunications operations, and concluded that the preferred FTI solution was to replace separate telecommunication networks with an integrated digital network. The integrated network would be used to transmit data and voice for both air traffic control and administrative services with connections to the Internet.

Our audit objectives were to determine whether: (1) security requirements are adequately addressed to secure air traffic control and administrative data on the same network, and (2) key acquisition documents reflect user requirements, adequately assess alternatives, and provide a reasonable baseline for future performance measurement.

RESULTS

The FTI project team has addressed many telecommunication needs that will enable FAA to better support modernization of the National Airspace System with more efficient digital communications and to improve management of telecommunications operations. However, FAA faces significant challenges and risks with the proposed FTI project.

The major risk factor is that air traffic control systems, which now operate on dedicated networks,[1] would share the same network with administrative systems which have direct connections to the Internet, thereby making air traffic control systems more vulnerable to unauthorized intrusion. In our opinion, FAA should not go forward with the network integration until it can give sufficient assurance that combining the National Airspace System with administrative systems on one integrated network will not compromise security of the National Airspace System.

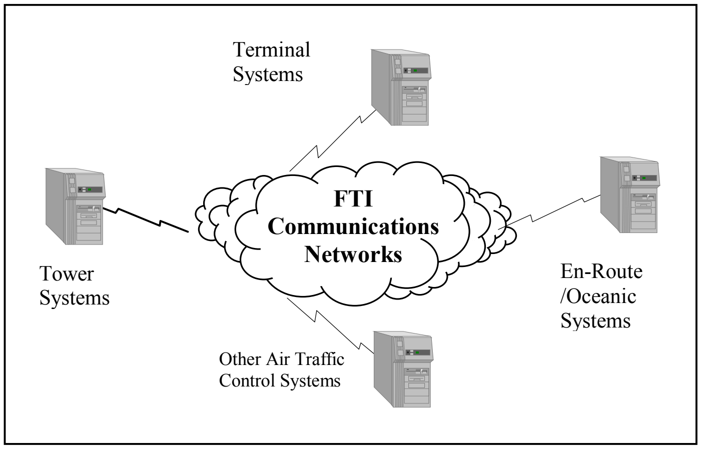
We believe the solution is to combine all air traffic control networks into one network, but leave FAA's administrative systems on separate networks. We are recommending that FAA resolve the issues in this report before the FTI contract award which is scheduled for October 2001. Specifically:

➢ **National Airspace System security needs to be fully assessed before moving to an integrated network environment**. One of FAA's first and foremost priorities must be to protect the National Airspace System from unauthorized intrusion. The National Airspace System is composed of more than 400 systems that support air traffic control operations.

  As indicated on the next page in Figure 1, National Airspace System Interconnections, these systems are located in towers, terminals, en-route/oceanic centers, and other air traffic control sites, which are connected by communication networks such as the one proposed by the FTI project.

[1] The current air traffic control networks may share the same transmission lines with administrative systems. However, FAA uses dedicated and separate network equipment to route air traffic control transmissions.

Figure 1
National Airspace System Interconnections


Terminal Systems
FTI Communications Networks
Tower Systems
En-Route /Oceanic Systems
Other Air Traffic Control Systems

Currently, FAA transmits air traffic control data and voice on dedicated networks with no direct connections to administrative systems or the Internet. By combining air traffic control and administrative systems into an integrated network, National Airspace System exposure will be increased because intruders will have more avenues and opportunities to access and disrupt air traffic control services. In September 2000,[2] we recommended that FAA should not proceed to integrate its networks until it could give assurance that network integration would not compromise National Airspace System security.

To provide sufficient security in an integrated network environment, both the FTI network and all air traffic control systems connected to the network need to be evaluated together as one system for security purposes. We found that FAA acquisition documents specified that securing FTI transmissions is a critical requirement, and vendors were directed to propose network security measures with state-of-the-art technologies for FTI. However, security requirements for individual air traffic control systems that would be connected to the integrated network have not been adequately evaluated by FAA.

FAA has more than 600 user systems, including about 400 systems supporting air traffic control operations such as the Host Replacement System for high altitude traffic. FAA is focusing on securing only about 100 systems[3] and plans to have only 40 of these systems certified as adequately secured prior to awarding the FTI contract.

[2] Statement of Inspector General Kenneth M. Mead before the Committee on Science, U.S. House of Representatives, Computer Security within DOT, September 27, 2000.

[3] These systems are identified as "essential to the Nation's defense, economic security, or public confidence" and need to be secured by May 2003 in accordance with Presidential Decision Directive 63.

The interconnectivity of all 600 systems makes FAA's plan inadequate. More important, FAA's vulnerability assessments for key air traffic control systems were based on the current dedicated network environment, not the proposed integrated network. Consequently, enhancements needed to secure these systems in an integrated network environment are not being addressed or included in the FTI cost estimate.

Maintaining separate networks to support mission-critical operations is not unique to FAA. In 1998, the National Aeronautics and Space Administration (NASA) considered consolidating all its networks. However, the final decision was to consolidate only administrative-support networks, and leave the mission-support network separate. NASA did consolidate all network support and management functions, and reported a reduction of demand for contract support services[4] by eliminating duplicate support functions and streamlining customer support.

FAA has tasked an assessment team to perform an in-depth review of FTI security requirements and the solutions proposed by vendors[5]. We support this initiative and have provided suggestions for the team's consideration. However, the focus of the team's review will not address our main concern for security of the air traffic control systems.

- **FAA could save millions of dollars and better manage National Airspace System security by integrating only the networks supporting air traffic control operations.** Among the six networks to be replaced by FTI, four support air traffic control and two support administrative functions. FAA's investment analysis showed that, by integrating the four air traffic control networks, it could save about $210 million over 10 years. FAA estimated that it could save an additional $250 million if the remaining two administrative networks also are integrated into FTI. We recommend that FAA integrate only the four air traffic control networks to help better manage National Airspace System security.

[4] According to NASA, the reduction ranged from 35 to 40 percent.

[5] Three groups submitted proposals for FAA evaluation: AT&T partnering with Lockheed-Martin, Sprint partnering with the Harris Group, and MCI Worldcom. We have not reviewed any vendor proposals and are not involved in FAA's evaluation process.

- **Future Air-to-Ground communications requirements need to be included in the FTI cost estimate**. One of the major National Airspace System modernization initiatives is to "digitize" Air-to-Ground communications—the Next Generation Air/Ground Communications (NEXCOM) project. NEXCOM will provide digital transmissions critical to other modernization projects such as Free Flight. FAA is working with the industry to evaluate NEXCOM and other alternatives, and has not yet finalized its strategy for NEXCOM.

  Supporting NEXCOM is a stated requirement for FTI. FAA asked contractors to make technical and cost proposals for FTI based on 50 millisecond latency[6] requirements. However, FAA estimated that NEXCOM would impose a stringent latency requirement of 15 to 25 milliseconds on FTI. Currently, this transmission speed could be met only with dedicated transmission lines, not shared transmission lines planned for FTI. FAA addressed this technology gap by only asking perspective FTI vendors to demonstrate that they have the technical capability to provide faster transmission speeds when needed by FAA.

  Since FTI is an all-inclusive contract, FAA will have to order services needed to support future Air-to-Ground transmissions from the FTI vendor, but it has not included the funding requirements in the FTI cost estimate. To avoid possible delays in supporting modernization projects, we recommend that FAA estimate the funding requirements to support NEXCOM and include those needs in the FTI cost estimate.

- **The FTI cost estimate needs to be better supported**. The initial approved FTI cost baseline was $1.9 billion over 10 years. The revised cost (re-baseline) is to be submitted for approval 90 days after contract award. We found that the initial cost estimate for FTI was based on discussions with industry representatives, other Government agencies, and internal support groups. However, there were no field studies or surveys to support the estimate.

  During the audit, we identified that costs were materially underestimated, and the FTI project team confirmed our results. However, the team identified cost offset opportunities such as reducing estimated installation sites by 60 percent. To finalize its cost estimate, FAA ordered an independent Government cost estimate which was completed in April 2001.[7] However, we found that the

[6] Latency is defined as the total time required to successfully transmit a unit of information across two network connection points. A millisecond equals one thousandth of a second.

[7] Due to procurement sensitivity, the outcome of the independent Government estimate is not discussed in this report.

cost estimate focused on contractor costs, which account for only about half of the total estimated FTI costs, and did not update the Government's costs. We recommend that FAA update the Government's portion of FTI costs when revising its cost baseline.

- **Labor union concerns could affect FTI implementation**. Three networks currently managed by FAA employees will be replaced by FTI, thus affecting work for these employees. Most employees are members of the Professional Airways Systems Specialists (PASS) labor union. FAA requested that PASS be part of the FTI Integrated Product Team, but the union has been reluctant to participate.

  We also found a large disparity between FAA and PASS in estimating the jobs impacted by FTI. While PASS estimated that potentially 2,000 jobs could be impacted, FAA's analysis indicated only about 150 jobs are involved. To avoid delays in implementation, we recommend that FAA work with PASS to identify specific positions that will be impacted and develop a plan for reassigning these employees.

BACKGROUND

FAA operates a combination of owned and leased networks to support data and voice communications for air traffic control operations and other administrative-support functions such as accounting for fund obligations, processing payments, and managing human resources. These networks support communications among FAA facilities (Ground-to-Ground) and between air traffic controllers and airline pilots (Air-to-Ground).

The FTI project was established to replace Ground-to-Ground communications networks because existing networks are approaching the end of their contract or service life cycles. For example, the contract for the Leased Interfacility National Airspace System Communications System (LINCS) is expiring in Fiscal Year (FY) 2002.[8] The Data Multiplexing Network (DMN) has been in service since 1990 and is experiencing an increase in failures. Among the nine Ground-to-Ground communications networks, six are land-based and the others are satellite or radio-based. FAA plans to replace land-based systems with FTI first (see Exhibit A).

[8] FAA currently is negotiating a contract with MCI Worldcom to extend LINCS contract services.

In 1998, FAA conducted an investment analysis by comparing three alternatives to current operations:

1. Reference Case: This alternative assumes keeping the six networks intact without any technical upgrades. However, it was priced based on current (lower) marketplace pricing.
2. Interfacility Services Network (ISN): This alternative assumes upgrading the six networks with technical improvements such as converting from analog to digital transmissions. However, these networks would remain separate.
3. Integrated Interfacility Services Network (IISN): This alternative assumes not only technical upgrades but also an integration of the six networks into one system.

In July 1999, FAA completed the FTI investment analysis and concluded that IISN was the preferred replacement solution. The total cost for this integrated network infrastructure was estimated at $1.9 billion. FAA currently is evaluating proposals submitted by three groups, and plans to award the FTI contract in October 2001 and start transitioning to the new network infrastructure during FY 2002.

SCOPE AND METHODOLOGY

We reviewed key FTI acquisition documents including the investment analysis, system requirements, acquisition strategy, integrated program plan, economic analysis, capacity models and the Screening Information Request. We also reviewed National Airspace System Architecture, FAA Information Systems Security Architectures, and existing network manuals and maintenance records.

We interviewed FAA technical and user representatives at both Headquarters and selected field offices; industry representatives including telecommunications providers and system integrators; and FAA labor union representatives. We also met with officials from NASA and the National Institute of Standards and Technology to discuss their network experience.

The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Audit work was performed between November 1999 and July 2001 at FAA Headquarters and selected air traffic control facilities located in Washington, D.C.

FINDINGS AND RECOMMENDATIONS

A. National Airspace System Security Needs to be Fully Assessed Before Moving to an Integrated Network Environment.

The National Airspace System Architecture proposes consolidation of Ground-to-Ground communications systems with a common network infrastructure to support both air traffic control and administrative functions. However, in 1997, the President's Commission on Critical Infrastructure Protection concluded that the combined use of open system architecture[9] and shared networks would result in a major threat to the National Airspace System. The Commission recommended that FAA keep the interconnections between the administrative networks and National Airspace System operational networks to an absolute minimum for better security.

Computer security is getting increased attention due to Presidential Decision Directive 63 which calls for protecting the Nation's critical infrastructure in today's highly connected network environment. Telecommunication networks supporting National Airspace System operations are deemed infrastructure-critical.

The Office of Management and Budget (OMB) also issued guidance (M-00-07) in recent years requiring agencies to demonstrate adequate computer security protection when requesting funding for operations.

Integrating air traffic control and administrative networks increases National Airspace System exposure.

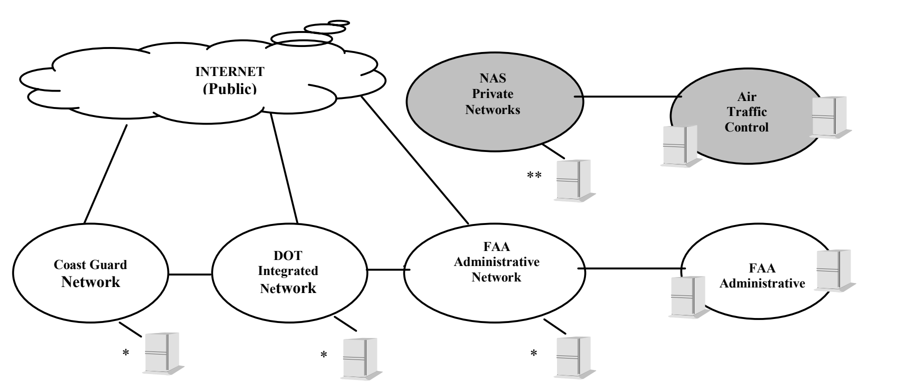
The FTI investment analysis concluded that an integrated network supporting both National Airspace System and administrative functions provides more savings than any other network alternatives. Currently, six land-based network systems are used to support Ground-to-Ground communications—four supporting National Airspace System and two supporting administrative functions. These physically separated administrative and National Airspace System networks are configured independently from each other to maintain security and performance. The proposed replacement with an integrated network having Internet connections will significantly increase the exposure of the National Airspace System because:

- Intruders will have more avenues to access the National Airspace System. As depicted on the next page in Figure 2, Existing Network Environment, the National Airspace System private networks, which support air traffic control systems, have no direct connections to the FAA administrative networks, the

[9] Open system architecture requires using hardware and software compliant with industry standards.

Department of Transportation (DOT) integrated network, the Coast Guard network, or the Internet.

Figure 2
Existing Network Environment

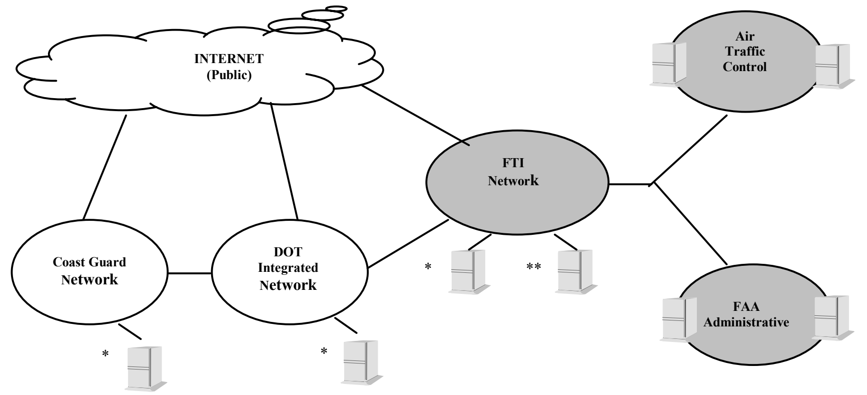


*Third party connections to contractors, grantees, trade associations, and other Government agencies.

**Connected to authorized contractors, airlines and other aviation support agencies.

As shown in Figure 3, Proposed Network Environment, FTI will connect air traffic control, FAA administrative, DOT and Coast Guard systems to each other and to the Internet. Under the proposed FTI integrated network environment, FAA will transmit air traffic control, administrative data, and voice on the same network.

Figure 3
Proposed Network Environment



*Third party connections to contractors, grantees, trade associations, and other Government agencies.

**Connected to authorized contractors, airlines and other aviation support agencies.

DOT, including FAA, has at least 15 authorized connections to the Internet and more than 100,000 users, including employees, contractors, grantees, trade associations, and other governmental agencies, accessing information on DOT networks. With the proposed integration of air traffic control and administrative networks, sophisticated network access security has to be implemented to prevent unauthorized entry into the National Airspace System through these added avenues.

- Intruders will have more opportunities to disrupt National Airspace System services. In an interconnected environment, intruders could gain unauthorized access on less secured systems, take over system administrator privileges, and gain access to other air traffic control systems as "trusted" parties. In addition, if intruders were able to launch denial-of-service attacks on network equipment shared by air traffic control and administrative operations, the National Airspace System also would be impacted.

Due to the increased threat with an integrated network, we recommended in September 2000 that until FAA could give assurance that network integration would not compromise National Airspace System security, FAA should not proceed to integrate the National Airspace System with its administrative network systems. We also pointed out that to provide such assurance, FAA would need sophisticated network controls and enhanced security in user systems connected to the integrated network.

While FAA specified securing FTI transmissions as a critical requirement for vendors, security requirements for individual air traffic control systems that would be connected to the integrated network have not been adequately evaluated by FAA.

FAA proposed a three-layered approach[10] in addressing National Airspace System security—the FTI network; facility infrastructure;[11] and user system. An FAA-wide coordination effort is called for to implement this three-layered security approach. For example, the FTI project is responsible for securing data transmission on the integrated network. Facility management is responsible for securing the interface between FTI and Local Area Networks in each facility. System owners are responsible for securing the user systems connected to Local Area Networks within each facility.

[10] Security in Depth--A Strategy for Meeting the FAA's End-to-End Security Requirements, June 6, 2000.

[11] Facility infrastructure includes various communications equipment used to connect networks.

FAA plans to use state-of-the-art technologies to secure transmissions on the FTI network, such as firewall security, enhanced user identification and authentication, cryptographic protection, and Virtual Private Networks to provide logical separation between administrative and National Airspace System transmissions. However, security for user systems and facility infrastructure has not been adequately evaluated.

- Vulnerabilities in Most Air Traffic Control Systems Were Not Examined. As indicated in Table 1, FAA Systems to Be Examined, FAA has 628 user systems, 402[12] of which are used to support air traffic control operations.

Table 1
FAA Systems to Be Examined

	Total Systems	Infrastructure-critical Systems to be Examined
National Airspace System	402	80
Non-National Airspace System	226	22
FAA Total	628	102

However, FAA has allocated resources and established timetables to examine only 102[13] systems for adequate security. FAA identified 102 information systems as its critical cyber infrastructure because they are essential to the Nation's defense, economic security, or public confidence; and need to be secured by May 2003 as required by Presidential Decision Directive 63. FAA plans to award the FTI contract in October 2001 and start transitioning to the integrated network during FY 2002. However, FAA plans to have only 40 of the 102 systems certified as adequately secured before the planned FTI contract award in October 2001 (see Exhibit B).

The interconnectivity of all systems makes FAA's plan inadequate. For example, there are about 50 mission-critical air traffic control systems that were developed and maintained by FAA regional offices. None of these regional systems is considered as critical to the Nation's infrastructure and, therefore, are not being evaluated. However, they are connected to the infrastructure-critical systems as part of the National Airspace System.

[12] This is calculated by combining the number of systems reported by two FAA lines-of-business: Air Traffic Services which is responsible for maintaining operational air traffic control systems, and Research and Acquisitions which is responsible for developing new air traffic control systems.

[13] The total number of "infrastructure-critical systems" is still evolving. For this report, we used 102 systems, which were defined in the final draft FAA Critical Infrastructure Protection Remediation Plan, June 23, 1999.

Controls and security over these regional systems are questionable, as evidenced by the recent incident where a disgruntled employee stole the production source code of a mission-critical regional system. If intruders take control of these regional systems, they could gain privileged access to other air traffic control systems because the system would consider the intruder as a "trusted source."

- Vulnerabilities Associated with the Integrated Network Environment were not Addressed. FAA's Chief Information Officer has issued well-structured guidance[14] for system owners to follow in conducting vulnerability and risk assessments. The guidance made proper references to the future National Airspace System, which encourages use of open system architecture and an integrated network environment. However, the risks associated with this direction were not addressed in the completed security evaluation for air traffic control systems.

  To promote use of hardware and software compliant with industry standards (open systems), FAA has replaced proprietary systems with commercial off-the-shelf (COTS) products. However, this strategy has made the National Airspace System more susceptive to attack because of common knowledge of the vulnerabilities in COTS products and availability of hacking tools. With the current separate networks, this exposure is limited to insiders such as disgruntled air traffic control employees or contractors. However, with the planned integration of networks, outsiders, including people connected through the Internet, could take advantage of these vulnerabilities.

  As stated earlier, the President's Commission warned in 1997 that the combined use of open system architecture and integrated network environment would result in a major threat to the National Airspace System. Despite the warning and security evaluation guidance, system owners did not evaluate security enhancements and the associated costs to protect their systems in an integrated open-system network environment.

  For example, the Host Replacement System uses the same hardware and operating system software as the DOT accounting system. However, the Host Replacement System does not have enhanced security protection[15] as the DOT accounting system. FAA recently certified the Host Replacement System as adequately secured for the Nation's infrastructure protection based on a

[14] Draft FAA Information Systems Security Architecture, Version 1.1, September 30, 1999; and FAA Information Systems Security Enhancement Program Handbook, Version 2, March 2001.

[15] For security reasons, specifics concerning this enhanced security protection are not discussed in this report, but were discussed with FAA management during the audit.

security review conducted 2 years ago. While the Host Replacement System may not need enhanced security protection on the dedicated networks, it should have the same protection, if not more, as the DOT accounting system on the integrated network.

- Plans to Review Facility-Level Security are Too Limited. As part of the infrastructure-critical systems protection plan, the FAA Chief Information Officer is sponsoring an Integrated Facility Certifications Program. The purpose of this certification program is to ensure that system security, physical security, and personnel security is properly integrated at the facility level. For example, one of the goals for the certification program is to ensure all information systems in the facility are protected against complex cyber-attacks coming from either inside or outside the "electronic" perimeter of the facility. This is a good initiative and could be used to help enhance the National Airspace System security on an integrated network. However, FAA faces two challenges:

  - **The Integrated Facility Certification Program still is in the development stage.** The FAA Chief Information Officer plans to test the program at the Leesburg en-route facility later this year, followed by Atlanta and Salt Lake facilities. There is no schedule to have all facilities certified before the planned FTI implementation.

  - **Facility management is not tasked to perform these certifications.** As stated repeatedly by OMB and DOT officials, agency program officials, not security officers or Chief Information Officers, are ultimately responsible for the security of programs under their control. This includes determining the acceptable level of risk and adequate level of security. Facility management has not been tasked to perform the facility-level certification.

While we agree that network integration provides cost-saving potential, we believe protecting the National Airspace System from unauthorized intrusion should be one of FAA's first and foremost priorities. Maintaining separate networks to support mission-critical operations is not unique to FAA. In 1998, NASA considered consolidating all its networks. However, the final decision was to consolidate only administrative-support networks, and leave the mission-support network separate.

In July 2001, FAA tasked an assessment team to perform an in-depth review of the FTI security requirements and the solutions proposed by vendors. While the focus of the team's review will not address air traffic control systems security (our main concern), we support this initiative because the review will be valuable to overall

National Airspace System security. We provide the following suggestions for consideration by the assessment team.

- Cost-benefits of enhancing FTI network security. FAA projected that, by combining the air traffic control and administrative networks, it could save an additional $250 million over 10 years. The assessment team needs to consider the cost to enhance security for FTI and air traffic control systems on an integrated network as an offset to this projected benefit.

- FAA's ability to support network security over the life of FTI. Network security requires not only installation of proper technologies and equipment but also support for ongoing maintenance. For example, firewall security is becoming a standard network security mechanism. However, firewall security cannot provide expected benefits unless it is properly managed and updated. This requires properly trained technical staff and well-developed management procedures.

Recommendations:

We recommend that the Federal Aviation Administrator:

1. Resolve the issues in this report before awarding the FTI contract. Do not go forward with network integration between air traffic control and administrative systems until FAA can provide sufficient assurance that combining the National Airspace System with administrative systems on one integrated network will not compromise security of the National Airspace System.

2. Require that the assessment team consider cost-benefits and FAA's capability of supporting network security over the life of FTI in making recommendations for FAA consideration.

B. FAA Could Save Millions of Dollars and Better Manage National Airspace System Security by Integrating Only the Networks Supporting Air Traffic Control Operations.

As stated earlier, the FAA investment analysis considered two digital network alternatives for FTI implementation--ISN and IISN. Table 2 is a comparison between the two digital network alternatives.

Table 2
Comparison between Two Digital Network Alternatives

	10-year Cost Estimate (in millions)	Network Infrastructure	Network Support and Management
ISN	$2,399	6 separate networks ■ 4 supporting air traffic control operations ■ 2 supporting administrative functions	Decentralized
IISN	$1,939	1 integrated network	Centralized

Both alternatives were rated high for supporting National Airspace System modernization. However, under ISN, FAA would continue maintaining six separate network systems, each of which would have separate network support and management functions. Under IISN, FAA not only integrates all six network systems but also consolidates all network management and support functions. IISN was determined to be more cost-beneficial (with $460 million of savings over ISN) and was recommended and approved by FAA as the preferred solution for FTI implementation.

Our analyses indicated that FAA could benefit by considering another solution, which would integrate only the four networks supporting air traffic control operations, but consolidate the support and management function for all six networks. This different solution could help FAA better manage National Airspace System security and still realize almost half of the $460 million of anticipated cost savings.

The FTI investment analysis indicated that FAA expected to achieve about $210 million of cost saving by replacing the four stand-alone air traffic control networks—LINCS, DMN, National Airspace Data Interchange (NADIN), and Bandwith Manager (BWM)—with FTI. This was primarily due to reduced system maintenance cost as a result of eliminating duplicate network equipment. Also, our review of the FTI investment analysis indicated that FAA could achieve additional savings by consolidating the support and management functions for the two administrative networks—ADTN and FTS.

In 1998, NASA investigated the possibility of integrating five networks to reduce operating costs. The final decision was to integrate only the four administrative-support networks and leave the mission-support network alone. However, NASA consolidated all network management functions under a single organization for both administrative-support and mission-support networks.

NASA stated that it has experienced a significant decrease in demand for contract support services (35 to 40 percent) since consolidation. NASA attributed this decreased demand to elimination of duplicate support functions, better coordination, and streamlined customer support. FAA could experience similar cost reductions.

Recommendation:

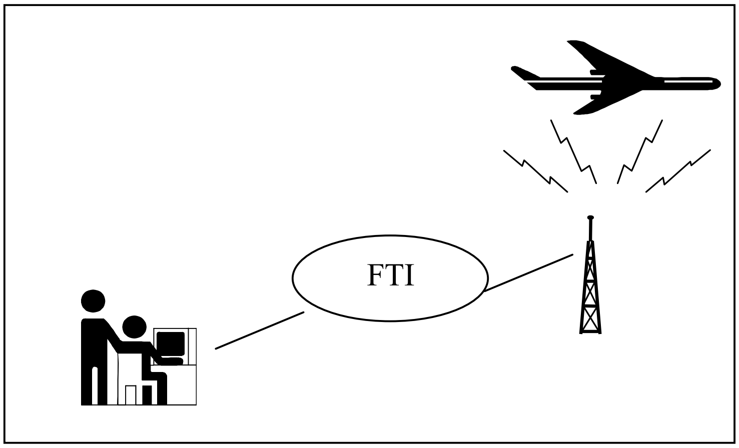
3. We recommend that the Federal Aviation Administrator direct the FTI project team to integrate only the networks supporting air traffic control operations, but consolidate the support and management functions for all of the air traffic control and administrative networks.

C. Future Air-to-Ground Communications Requirements Need to Be Included in the FTI Cost Estimate.

A factor used in evaluating FTI alternatives was "the ability to meet anticipated National Airspace System capability requirements to support future concepts of operations." One of the major National Airspace System modernization initiatives is the NEXCOM project to "digitize" Air-to-Ground communications systems in order to accommodate growing communication needs with limited radio frequency spectrum.[16] NEXCOM will provide digital transmissions critical to other modernization projects such as Free Flight.

While FAA stated supporting NEXCOM communications as a requirement for FTI, it excluded this requirement from contractor proposals and cost estimates. FTI is a critical component in supporting communications between air traffic controllers and airline pilots. As indicated in Figure 4, Controller-Pilot Communications, there are two components supporting controller/pilot communications—Ground-to-Ground transmissions to radio towers, and Air-to-Ground transmissions to pilots.

Figure 4
Controller-Pilot Communications



FAA has an agreement with the National Air Traffic Controllers Association (NATCA) that communications between air traffic controllers and pilots should occur within 250 milliseconds after initiation. NEXCOM will require a longer Air-to-Ground communications span and, accordingly, require a faster communications support for Ground-to-Ground communications. The NEXCOM project team estimated that this would impose a more stringent latency requirement (15 to 25 milliseconds) on FTI. Currently, this stringent latency

[16] The first segment of NEXCOM will provide digital voice support for high altitude sectors. Later segments of NEXCOM will provide digital voice and data link capabilities to both high altitude sectors and designated terminal areas.

requirement could be met only with dedicated transmission lines, not shared transmission lines planned for FTI.

FAA is working with the industry to evaluate NEXCOM and other alternatives, and has not yet finalized its strategy for the next generation Air-to-Ground communications. Because of this uncertainty, the FTI project team proposed, and FAA senior management approved, deferring the NEXCOM support issue to future years. For example, FAA addressed the technology (latency) gap by only asking perspective FTI vendors to demonstrate that they have the technical capability to provide faster transmission speeds when needed by FAA.

Since FTI is an all-inclusive contract, FAA will have to order services needed to support future Air-to-Ground transmissions from the FTI vendor, but has not included the funding requirements in the FTI cost estimate. The FTI Service Module, that is used by perspective contractors in proposing technical solutions and estimating costs, requires only 50 millisecond latency to support en-route and terminal operations. The FTI project team expects that:

- The technology for shared transmission lines may be enhanced in upcoming years to enable FTI to meet the 15 to 25 millisecond latency requirement, or

- NEXCOM latency requirement on FTI may be lowered as a result of other enhancements.

A NEXCOM Aviation Rulemaking Committee recently has recommended that FAA expedite the testing of digital communications. Pending the outcome of the test, FTI may have to provide faster communications support in a few years. If the expected technology improvement does not materialize in time, FAA will have to add dedicated transmission lines to FTI to support NEXCOM implementation. To avoid possible delays in supporting modernization projects, FAA should estimate the funding requirement for NEXCOM support and include it in the FTI cost estimate.

Recommendation:

4. We recommend that the Federal Aviation Administrator instruct the FTI project team to estimate funding requirements for NEXCOM support and inform the Office of Management and Budget and congressional appropriations committees about this funding contingency as part of the FTI cost estimate.

D. The FTI Cost Estimate Needs to Be Better Supported.

In July 1999, FAA's Joint Resources Committee approved an initial FTI cost baseline of $1.9 billion--$200 million for transitioning old networks to FTI, and $1.7 billion for supporting both new and old networks over 10 years. The Joint Resources Committee also required the team to submit a revised cost estimate (re-baseline) for approval 90 days after contract award which currently is scheduled for October 2001.

We found that the initial cost estimate for FTI lacked creditable support. The cost estimate for the integrated FTI network solution was based on discussions with industry representatives, other Government agencies, and internal support groups. The team did a comprehensive job documenting cost estimates for various activities such as program management, service acquisition, network transition, in-service maintenance, and equipment disposition. However, there were no field studies or surveys to support these estimates.

During the audit, we identified that costs were materially underestimated, and the FTI project team confirmed our results. However, the team identified cost offset opportunities such as reducing estimated installation sites from 804 to 341 (60 percent). As a result, the team made significant adjustments to individual cost items without changing the total cost estimate.

Because factors used in estimating network costs were subjective, FAA ordered an independent evaluation which was completed in April 2001. However, we found that the estimate only focused on contractor costs. We understand that FAA plans to rely on this estimate to evaluate contractors' cost proposals. However, we are concerned that there is no plan to perform a similar evaluation for the Government's portion of estimated costs to help re-baseline the FTI cost estimate. According to FAA's initial cost estimate, the Government's portion accounted for about 50 percent of total FTI costs.

Recommendation:

5. We recommend that the Federal Aviation Administrator instruct the Joint Resources Committee to ensure the revised cost estimate (re-baseline) submitted for approval reflects an updated estimate for the Government's portion of the FTI cost estimate.

E. Labor Union Concerns Could Affect FTI Implementation.

Some FAA personnel will need to be reassigned as a result of FTI implementation. FAA's planning documents stated that:

> When a particular program is 'absorbed' by the FTI Program, the Program Management costs are reduced by the amount of FAA personnel involved in the management of the given program. These personnel are not necessarily eliminated from the Government payroll, but they are reassigned to support evolving needs in other areas.

Among the network systems to be replaced by FTI, three—DMN, BWM, and NADIN--are owned by FAA and managed by FAA Airway Facility employees, who are represented by the PASS labor union. FTI project team has requested PASS to be part of the Integrated Product Team for implementing FTI. However, PASS has been reluctant to do so. According to union officials, PASS is concerned that their members may not receive meaningful work since FAA has not provided any specific information on the planned reassignment.

We also found a large disparity between FAA and PASS in estimating the jobs requiring reassignment. PASS estimated that potentially 2,000 of its members are working on telecommunications and could lose their work, completely or partially, as a result of FTI implementation. Conversely, FAA estimated that only about 150 positions would be impacted. PASS members are expected to help FAA test the transition to FTI. Any delays in receiving PASS cooperation could result in a prolonged transitional period.

Recommendation:

6. We recommend that the Federal Aviation Administrator instruct the FTI team to work with PASS officials to identify specific positions that will be impacted as a result of FTI implementation, and develop a plan for reassigning personnel occupying these positions.

MANAGEMENT RESPONSE

We provided a draft of this report to the FAA Associate Administrator for Research and Acquisitions, Deputy Associate Administrator for Air Traffic Services, Deputy Chief Information Officer, Director for Office of Information Systems Security, and the FTI project manager on July 6, 2001.

On July 26, 2001, FAA provided a preliminary response indicating that the FAA Chief Information Officer has sponsored an assessment team to perform an in-depth review of FTI security requirements and the vendor proposed solutions. The assessment team, led by an individual from outside FAA, will be composed of industry experts, other Government agency personnel, and FAA contractors. The team is tasked to complete its work by September 12, 2001. FAA has agreed to provide final comments upon completion of the assessment team's work. The complete text of FAA comments is in the Appendix to this report.

OFFICE OF INSPECTOR GENERAL COMMENTS

We support FAA's initiative of having the assessment team perform additional security reviews. It is our understanding that the assessment team will recommend whether FAA should proceed with the planned FTI acquisition based on its conclusion that FTI is, or can be, adequately secured. In our opinion, unless the assessment team considers security implications of the National Airspace System as a whole, including both the FTI network and individual air traffic control systems, the assessment result is incomplete.

ACTION REQUIRED

In accordance with DOT Order 8000.1C, we would appreciate receiving your final comments upon completion of the assessment work. If you concur with our findings and recommendations, please state specific actions taken or planned for each recommendation and provide target dates for completion. If you do not concur, please provide your rationale. You may provide alternative courses of action that you believe would resolve the issues presented in this report.

We appreciate the courtesies and cooperation of FAA representatives. If you have questions concerning this report, please call me at (202) 366-1964 or John Meche at (202) 366-1496.

-#-

EXHIBIT A

Ground-to-Ground Network Systems

Network Types	*Major Networks*	*FY 2000 Costs (millions)*
Land-based	Leased Interfacility NAS Communications System (LINCS) & Leased Circuits*	$123
	National Airspace Data Interchange (NADIN)	3
	Bandwidth Manager (BWM)	2
	Data Multiplexing Network (DMN)	2
	Agency Data Telecommunications Network (ADTN)	14
	Federal Telecommunications System (FTS)	19
Satellite	FAA Telecommunications Satellite System (FAATSAT)	17
	Alaskan National Airspace System Interfacility Communications System (ANICS)	6
Radio	FAA Owned-Microwave (FOMS)--	12
	Radio Communications Link (RCL)	
	Low-density Radio Communications Link (LDRCL)	-------
	Total	$198

* Costs for LINCS and leased circuits were $76 million and $47 million, respectively.

EXHIBIT B

Schedule for Securing FAA Infrastructure-critical Systems

	Total Number of Systems--Vulnerability Assessed	Total Number of Systems--Security Certified
June 2000	34	6
February 2001	82	20
September 2001	102	40*
September 2002	None	78
May 2003	None	102

U.S. Department
of Transportation

**Federal Aviation
Administration**

Memorandum

Subject: **ACTION**: Response to Draft Report on Replacement of Telecommunications Systems, FAA

Date: July 26, 2001

From: Associate Administrator for Research and Acquisitions, ARA-1

Reply to
Attn. of:

To: Deputy Assistant Inspector General
For Financial, Information
Technology, and Departmentwide
Program

The purpose of this letter is to provide some additional comments to your FAA Telecommunications Infrastructure (FTI) discussion draft of July 6, 2001. The discussion draft draws a number of conclusions and makes five recommendations relative to FTI. This letter will focus on your security concerns, your recommendations 1 and 2 which relate to those concerns, and your concern expressed in recommendation 3 relative to the suitability of FTI services to support future air-to-ground requirements such as Next Generation Air/Ground Communication (NEXCOM).

You correctly point out in the discussion leading to recommendation 2 that a key objective of the FTI program is to consolidate the management of FAA telecommunication services. Indeed, the capability to integrate the ordering, provisioning, measurement of performance, invoicing of services, etc. is a central element of the FTI business case. It is consistent with proven industry practices and we agree with your observation that the opportunity to manage our services according to industry best practices should not be lost.

In the discussion leading to recommendation 1, you make two central points. First, in pursuing the management goals outlined above, you assert that the FAA compromises the integrity of the National Airspace System (NAS) by not adequately requiring separation of NAS critical and administrative network services. While we agree with your objective of maintaining separate service domains, we do not share your conclusion. FTI security requirements are rigorous in establishing partitioned network services between NAS and administrative users. FTI security requirements were developed by a group of security experts from Government and industry and there have been numerous reviews within the FAA and with the telecommunications industry. Additionally, as you are aware, AIO-1 has sponsored an independent assessment team made up of security experts and led by an individual from outside the FAA that will examine the full set of security services required under the FTI program and the proposals currently offered under FTI source selection. We expect their initial findings within the next several weeks and final recommendations in late August. We will then make a determination how to incorporate their recommendations before awarding the FTI contract. The review will consider whether the FTI service approach exacerbates, improves, or is otherwise neutral vis-à-vis the existing security vulnerabilities of NAS user systems. The answer to this question is paramount, in our view, before any judgements can be made about FTI vulnerability. On this issue, therefore, we would urge you to broaden your analysis beyond the business case study to include a review of the proposals. A study of the proposals may serve to ameliorate your concerns. After all, it is the Vendor proposals that should serve as the basis of our discussion, and **NOT** the documents produced during the Investment Analysis. In any case, we would urge that you withhold judgement on this matter until the independent assessment team completes its work. In addition, we encourage you to accept the FAA’s offer for you to participate in the work of the independent assessment team in a manner you see appropriate.

Your second key point leading to recommendation 1 is the broader question of overall NAS user system vulnerabilities and that such vulnerabilities need to be fully resolved prior to deploying FTI services. We agree that NAS security requires our resources and we are committed to the timetables required to ensure that all end-user systems address NAS security. We cannot agree, however, that deployment of FTI services be held to a standard beyond the control of the network service; instead we recommend that all end-user systems be required to pass security certification and authorization prior to being allowed to connect to FTI. A central offering of the FTI program is that a multitude of telecommunication services, including new and enhanced security services, be made available to different users, with different and changing requirements and, quite appropriately, different security demands. This capability to match security services to user needs represents a significant network enhancement, which supports the incremental improvement of NAS security. Your concerns here return us to the earlier question of whether the proposed approach for acquiring FTI services will, in fact, worsen the vulnerability of end-user systems. As discussed above, we believe this judgement can be better made after consideration of the assessment team results.

Finally, to the question of whether the FTI program has adequately addressed future requirements, particularly those that may be required for NEXCOM. We believe that we have. We understand that your concern is over estimated funding requirements for these services. Recall, however, that we are referring to services that may be required in the 2007/8 timeframe. Obtaining competitive prices for an uncertain requirement that far downstream was not practical. Of concern was whether the deployed FTI infrastructure might require major upgrade to support the NEXCOM. Our approach was to require that the offerors’ proposals demonstrate whether the deployed FTI platforms could, without significant modification, provide what is today a proven technology. In this manner, we have mitigated our greatest price risks. We understand that this is a complex strategy and would invite your analysts to work with the FTI Program team to more fully understand this approach.

Should you require further discussion on our comments, please contact me at (202) 267-7222.

Steve Zaidman

Steven Zaidman