REVIEW OF FAA'S PROGRESS IN ENHANCING AIR TRAFFIC CONTROL SYSTEMS SECURITY

Federal Aviation Administration

Report Number: FI-2010-006

Date Issued: November 2, 2009

Memorandum

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

Subject: ACTION: Report on Review of FAA's Progress in Enhancing Air Traffic Control Systems Security Report Number FI-2010-006

Date: November 2, 2009

From: Rebecca C. Leng
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA–20

To: Federal Aviation Administrator

This report presents the results of our review of FAA's renewed initiatives in addressing air traffic control (ATC) systems security weaknesses discussed in our FY 2007 audit report of the Department's information security program.[1] In that report, we identified the need to implement an operational business continuity plan (BCP) to ensure continued en route services[2] in the event of a long-term disaster. We also identified the need to enhance the system security certification and accreditation process across *all* air traffic control systems, not just the ones used to support en route operations.

Homeland Security Presidential Directive (HSPD)–7 designates air traffic control systems as part of the Nation's critical infrastructure, due to the important role commercial aviation plays in fostering and sustaining the national economy and ensuring citizens' safety and mobility. The Secretary of Transportation is responsible for ensuring that air traffic control facilities, systems, and operations are protected from significant disruption caused by man-made or natural events and are able to resume essential services in a timely manner if disrupted, to minimize the impact on the Nation's economy.

[1] *Audit of Information Security Program, DOT*, OIG Report Number FI-2008-001, October 10, 2007. OIG reports can be found on our Web site: www.oig.dot.gov.

[2] The 22 en route centers (Air Route Traffic Control Centers, or ARTCCs) control aircraft at cruising altitude (above 18,000 feet) in transit over the continental United States and out into the Atlantic and Pacific oceans. Each center handles a different territory of airspace, passing control from one center to another as respective borders are reached, until the aircraft begins to descend and is controlled by a terminal radar approach control facility (TRACON) and airport control tower as it nears its destination.

To fulfill the requirements of HSPD–7, the Federal Aviation Administration (FAA) must protect air traffic control systems with a two-pronged approach: preventing disruption wherever possible and minimizing disruptions when they do occur. Implementing a BCP for en route services and enhancing security reviews of all air traffic control systems are key to accomplishing these goals.

Our objectives were to determine FAA's progress in correcting security weaknesses previously identified in the air traffic control system by assessing (1) the status of BCP implementation and (2) the enhanced methodology used in the certification and accreditation of air traffic control systems security at operational sites. This performance audit was conducted in accordance with generally accepted government auditing standards prescribed by the Comptroller General of the United States and included such tests as we considered necessary to detect fraud, waste, or abuse. Details of our scope and methodology can be found in Exhibit A.

RESULTS IN BRIEF

FAA has designated the William J. Hughes Technical Center in Atlantic City as the recovery site where operations would be resumed if any en route center became inoperable. It has made good progress in preparing the Technical Center to serve as the recovery site, such as establishing a duplicate en route system environment on-site and installing additional emergency power at the center. Yet several unresolved technical challenges, staffing issues, and funding requirements could delay recovery site readiness. Beyond this, FAA has not assessed how activating the recovery plan during an emergency would affect air travel and the economy across the country—a key concern in HSPD–7. Further, while FAA has enhanced the process of reviewing ATC systems security, the reviews were not properly carried out to ensure security protection of operational ATC systems.

Status of BCP Implementation

The unresolved technical issues concern radar coverage and air-to-ground communications. While FAA has demonstrated the capability to use alternate methods to redirect radar and communications signals from the affected en route center to the recovery site, it has not established that using alternate methods can meet FAA's operational requirements to ensure safe air travel. Specifically, FAA planned to use modems and regular telephone lines to transmit single-path radar

signals[3] to the recovery site; however, it did not test the integrity of this transmission to ensure that signals cannot be lost or disrupted.

FAA's testing of its ability to re-route communications signals also entailed a significant limitation—it used the network connections and communications equipment in an en route center that was supposed to be out of service. According to FAA, it will have to work with local telephone companies to establish new connections between field communications equipment and the recovery site. However, no detailed plan exists to implement this proposed action or to test whether communications through these new connections can meet FAA's stringent latency requirement.[4] FAA needs to demonstrate that activating the recovery site will not compromise the safety of air travel.

The recovery site cannot become operational without air traffic controllers on-site. FAA has created a database containing the names of all controllers and the airspace sectors in which they are certified to direct traffic. Should an en route center become nonfunctional, FAA will use this database to identify controllers qualified to direct traffic in the affected airspace. However, FAA has not developed a plan to address related labor issues, including personnel relocation and temporary housing. Further, FAA has not performed a cost estimate for developing a fully functional BCP, as required by FAA's Acquisition Management System. Instead, FAA allocated $15 million to this development effort by reallocating funds from other parts of its operations. Developing a cost estimate based on the tasks that need to be completed is a basic project management control. Without it, FAA cannot determine whether it has allocated adequate funds for implementing all tasks critical to continued en route services at the recovery site, such as relocating air traffic controllers. FAA needs to develop a plan for relocating and housing air traffic controllers at the recovery site and conduct a credible cost estimate for implementing the BCP.

Finally, under the current BCP, FAA pledges to restore 80 percent of any affected en route center's capabilities at the recovery site within 3 weeks of shutdown. However, FAA did not analyze the impact on air travel that would be caused by losing an en route center for 3 weeks. The impact could vary significantly, depending upon the affected en route center's traffic volume and the ripple effect of delays to other parts of the country. The loss of the New York or Chicago center, for example, would have a far greater impact than would the shutdown of

---

[3] More than 40 percent of long-range radars are single-path—with connections to only one en route center. Should the en route center become inoperable, it could no longer serve as a connection point between the radar and other ATC facilities.

[4] Latency is defined as the total time required to successfully transmit a unit of information across two network connection points. FAA requires that air-to-ground communications be completed within milliseconds (one thousandth of a second).

less busy centers. Without such analysis, the Secretary of Transportation will not be able to inform the Administration and the Congress about the potential impact on air travel—and the economy—if FAA had to activate BCP operations. FAA needs to assess the potential impact and provide the results to the Secretary in support of HSPD–7.

Security Certification Reviews

FAA has enhanced the review process of ATC systems security in recent years by sending teams to ATC facilities to evaluate systems in operation—directing air traffic. This represents a significant improvement from the previous approach, which focused on reviewing security controls of the ATC (baseline) systems in the computer laboratory, but not the systems deployed to operational sites.[5] However, FAA has not followed its own procedures to ensure that operational sites at risk of having unauthorized system configurations are selected for evaluation.[6] Our review of the site-selection methodology for five sample systems found only one for which system configuration variance was reviewed in the site-selection decision. A prior audit identified instances in which ATC systems were configured differently in the field than from the baseline system, resulting in security vulnerabilities for ATC operations. Currently, FAA has no way of knowing whether its personnel selected the sites that did, in fact, pose the greatest security risk for review. FAA needs to focus on reviewing system configuration variances during site selection.

Further, the security reviews conducted at operational sites for our sample systems lacked examination and/or testing, and were incomplete. The review teams relied primarily on interviews with system operators to develop conclusions on the adequacy of security controls. Further, 43 percent of security control items in our sample systems were not reviewed. As a result, FAA cannot rely on these reviews to detect and correct security vulnerabilities in operational ATC systems. FAA therefore needs to better ensure the integrity and completeness of the security reviews conducted on operational ATC systems.

Overall, despite FAA's progress over the past 2 years in implementing a BCP for continued en route services and expanding security evaluations of operational ATC systems, additional action is needed to strengthen security protection and minimize the impact of long-term service disruption. Issues concerning the

---

[5] ATC (baseline) systems are developed and tested in the computer laboratory before being deployed to operational sites. For example, the Host Computer is deployed to the 22 en route centers to support high-altitude air traffic control operations.

[6] System configuration involves setting up hardware and/or software to meet one's particular needs, such as changing factory-set defaults. In the case of FAA systems, hardware or software can be configured one way in the computer laboratory, then altered in various ways to fit the needs of local installations.

security of a critical national infrastructure should receive priority attention at a time of increased threats from nation-state-sponsored cyber attacks. We made a series of recommendations, beginning on page 14, to help FAA implement a fully functional BCP and strengthen its ability to protect operational ATC systems. FAA concurred with the recommendations. FAA's formal response is included in its entirety in the Appendix to this report.

FINDINGS

Despite Progress, the Designated Recovery Site Is Not Yet Fully Ready to Provide Air Traffic Control Services in Case of En Route Center Disaster, and Impact on Air Travel Has Not Been Assessed

Since 2007, FAA has made good progress in preparing the Technical Center to serve as the recovery site, by establishing a duplicate en route system environment and installing additional emergency power on-site. Yet unresolved technical challenges, staffing issues, and funding requirements could delay recovery site readiness. In addition, FAA has not assessed how activating the recovery site during an emergency would affect air travel, threatening the Secretary's ability to inform the Administration and Congress of potential impact on the Nation's economy, a key concern in HSPD–7.

Unresolved Technical Challenges, Staffing Issues, and Funding Requirements Could Delay Recovery Site Readiness

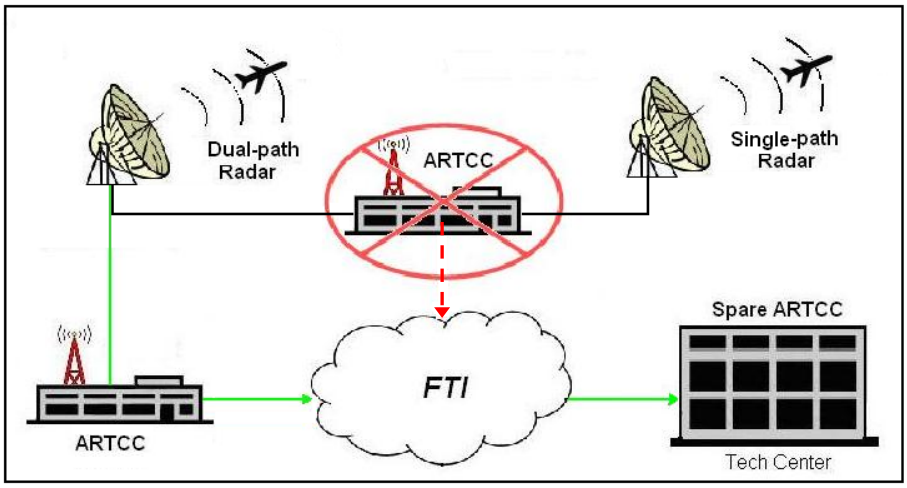
Technical Challenges

- *Surveillance.* This involves redirecting radar signals from the affected en route center to the recovery site. Long-range radar facilities are very important to air traffic controllers because they act as their eyes in the sky. Currently, 44 percent (60 of 137) of all long-range radar facilities that feed en route centers are single-path, meaning that the radar data are being fed only to a single air traffic control facility. This is a problem because if the en route center that receives the data is lost, the radar data cannot be easily re-routed to the recovery site. While FAA has identified an alternate method to transmit single-path radar signals, it did not test the integrity of this transmission to ensure signals cannot be lost or disrupted.

  As shown in Figure 1, dual-path radars can send signals to the backbone network (Federal Telecommunications Infrastructure [FTI]) even if one

path is lost; once there, FAA has shown that the signal can be redirected back to the recovery site during BCP operations. In contrast, the single-path radars lack this redundancy; if the one path is lost, the radar signal cannot reach FTI or, therefore, the recovery site.

Figure 1. BCP Mitigation Strategy for Single-path Radar



Source: OIG

FAA's planned strategy is to enable a backup modem on these radars and send the data over existing telephone/facsimile lines back to the recovery site. However, FAA did not test the integrity of this transmission to ensure that signals will not be lost or disrupted. As a result, FAA has no assurance that its current strategy can provide radar data sufficient to meet FAA operational standards; this strategy may, then, endanger flight safety if called upon to take over BCP activation.

Single-path radars are as important as dual-path, and sometimes cover areas just as large. For example, a single-path radar facility in the Memphis region is responsible for providing radar coverage to an area half the size of the state of Mississippi. FAA must test the integrity of the planned use of back-up modems and existing telephone/facsimile lines to re-route data from single-path radars to the recovery site.

- *Communications.* Ground-to-air voice communications is a vital part of air traffic control operations that must be fully operational and meet safety requirements in order for the BCP to work in a live environment. This involves re-routing voice communications signals from the affected en route center to the recovery site. Major equipment involved in this area includes radio towers used to receive and transmit voice communications, which are connected to the voice switching equipment used at en route

facilities that enables controllers and pilots to communicate. FAA has made good progress in preparing the recovery site with the necessary equipment, but faces challenges in the transmission of voice signals between the recovery site and radio sites.

FAA has demonstrated its ability to redirect a ground-to-air voice channel from a remote radio facility used by the Memphis Center to the recovery site. A controller at the recovery site was able to communicate with a pilot flying through Memphis Center airspace. However, the test did not simulate realistic disaster conditions by bypassing the network connection and radio control equipment located at the Memphis Center. The test was also limited in that it represented just one of the many voice channels that will need to be redirected during actual BCP operations.

According to FAA, the risk of affecting National Airspace System (NAS) operations is too great—due to operational limitations in the existing en route air traffic control communications system equipment—for simulation testing. We understand FAA's concerns about not harming NAS operations. Nevertheless, the only way in which FAA can prove operational readiness of the recovery site is by conducting realistic communications testing that reflects the actual loss of an en route center. In a similar situation in the late-1990s, FAA did perform simulation testing on operational ATC systems to ascertain its readiness for the Year 2000 conversion, and did not in any way affect ongoing NAS operations.

FAA informed us that it will have to work with local telephone companies to establish new connections between field communications equipment and the recovery site should an en route center become nonfunctional. However, no detailed plan exists to implement this proposed action or to test whether communications through these new connections can meet FAA's stringent latency requirement (for speed of communications). Without sufficient testing, FAA has no assurance that it could re-route hundreds of communications channels while still meeting operational requirements for signal speed. FAA needs to develop a detailed plan addressing how it will install network connections between radio towers and the recovery site through the local exchange carrier during BCP operations, and conduct tests to ensure that communications through the new connection can meet the latency (speed) requirements for air travel safety.

Staffing Issues

According to National Institute of Standards and Technology (NIST) guidelines, having the right personnel available for BCP operations is a critical process. FAA has made progress in the area of human integration by creating a "ready reserve" database that contains the names of available and qualified air traffic controllers who could be called upon to serve during BCP operations. However, FAA lacks a human integration plan to relocate and house the required BCP staff, including the controllers who would need to be relocated from their assigned en route centers to the recovery site. In the absence of such a plan, FAA may not be able to activate the BCP in a timely manner because the recovery site cannot become operational without qualified air traffic controllers on-site. FAA needs to develop a plan to address human integration issues such as relocating and housing air traffic controllers at the Technical Center recovery site on a long-term basis.

Funding Requirements

FAA has not performed a cost estimate for implementing a fully functional BCP that includes personnel relocation and temporary housing for staff, as required by FAA's Acquisition Management System. Instead, it allocated $15 million to the development effort by reallocating funds from other FAA programs and projects. FAA has spent a little less than half of the allocated funds, primarily to upgrade equipment at the recovery site. While it has about $7.5 million remaining in the budget, there is no support or analysis showing whether the remaining funds will be sufficient to resolve outstanding needs to make the BCP fully functional, such as resolving the technical challenges associated with radar and communications signals or relocating FAA personnel. Developing a cost estimate based on the tasks that need to be completed is a basic project management control. Without it, FAA cannot determine whether it has allocated sufficient funds for implementing all tasks critical to continued en route services at the recovery site. It needs, therefore, to sufficiently analyze costs to implement all tasks critical to continued en route services, and use such analysis to secure the funding necessary to complete the business continuity plan.

Impact on Air Travel from Activating the BCP Has Not Been Assessed

NIST guidelines call for developing a business impact analysis—a standard business practice conducted prior to the development and construction of a business continuity program. FAA's BCP estimates restoration of 80 percent of

any affected en route center's capabilities within 3 weeks at the Technical Center recovery site. However, the agency did not formally assess how the loss of each of the 22 en route centers for 3 weeks would affect NAS operations as a whole.

Loss of air traffic control facilities has a proven negative effect on NAS operations, and especially on the airline industry. Such disruptions have resulted in a rippling, nationwide effect on flight cancellations and delays. For example, in late 2007 the loss of the Memphis Center for 3 hours caused over 500 flight delays and cancellations throughout the region. In 2003 the loss of the San Diego Terminal Radar Approach Control facility for 35 hours resulted in over 700 flight cancellations and significant delays throughout the NAS.

Since en route centers operate with varying levels of traffic, their losses would affect the NAS in different ways. Major en route centers such as New York, Cleveland, Atlanta, and Chicago handle a tremendous volume of air traffic, compared with smaller centers such as Seattle and Salt Lake City. A 2004 study by MITRE Corporation[7] suggested that airlines would lose $76 million a day if the New York Center were closed (which did not include the economic impact of cascading flight delays across the country).[8] Without a center-by-center business impact analysis, the Secretary would not be able to inform the Administration and the Congress about the potential impact on air travel—and the economy—if FAA had to activate BCP operations. To support HSPD–7, FAA needs to conduct a business impact analysis for either individual en route centers or centers having the greatest impact on the NAS.

Review of Operational ATC Systems Security Is Inadequate to Ensure Proper Protection

In response to our past recommendations, FAA has enhanced the certification and accreditation process used to review and certify the adequacy of air traffic control systems security deployed to operational sites. However, the process used lacks an effective way of selecting operational sites at risk of having unauthorized system configuration for security reviews. Past reviews have identified instances in which FAA system was configured differently in the field than from the baseline system in the computer laboratory in order to meet the operational needs of different sites. These configuration variances have led to security weaknesses. In addition, the security reviews conducted at operational sites lacked examination

[7] MITRE is a nonprofit organization that manages three Federally-funded research and development centers, including, for FAA, the Center for Advanced Aviation System Development.

[8] *Description of Limitations and Potential Mitigation Strategies for Ensuring National Airspace System (NAS) Continuity of Operations: Provisional Findings,* MITRE Corporation, July 2004.

and testing to ensure proper implementation of security controls, and more than 40 percent of the security controls in our sampled systems were not reviewed at all.

Operational Sites at Risk of Having Unauthorized System Configuration Were Not Considered for Security Review

FAA's site-selection methodology requires the security review team to look at information on four key aspects of the system—security categorization, system environment, network connections, and configuration variances—before selecting operational sites for review. Yet review teams did not perform an adequate analysis of site-specific system configurations during the site-selection process to determine which operational locations were most likely to exhibit configuration variances.

- *Security Categorization.* FAA systems are categorized by how critical a system is in supporting FAA's mission. The categorization levels for ATC systems range from low to moderate. Systems with a categorization of low are usually nonmission-critical systems; systems with an overall categorization of moderate are usually mission-critical.

- *System Environment.* ATC systems are grouped into one of three system environments: NAS Operations, Mission Support, and Administrative. Systems that operate in the NAS operational environment and also have a security categorization of moderate are mission-critical and have a significant impact on the performance of air traffic operations. Systems supporting the mission support and administrative environments do not have as significant an impact on air traffic operations.

- *Network Connections.* The likelihood that a cyber threat may be directed against a system is based on that system's exposure level to the threat. A system's network interface defines the connectivity and communications protocol, which are critical to assessing the risk of a cyber threat. Network interfaces are categorized into one of six groups.[9] The Internet/Extranet Internet Protocol (IP) environment has the highest risk of all system network connections.

- *Configuration Variances.* System configurations are established before deployment to the field. Most system configuration differences occur in order to meet the operational requirements that vary at each site. Since configuration differences may affect a system's security posture, FAA requires that sites be

[9] NAS IP, Admin/Mission Support IP, Internet/Extranet IP, Closed System IP, Non-IP, and None.

visited where system configuration differences exist, and checked to ensure that no security vulnerabilities have been inadvertently introduced.

Security categorization, system environment, and network connections often remain the same for a system deployed to all installation sites. While these are important criteria for determining how many installation sites should be visited, they do not directly help with site selection. Instead, it is the last criterion, configuration variances, that is key to identifying high-risk installation sites. This makes the evaluation of configuration variances a key step in selecting specific operational sites for review, which is critical because some air traffic control systems are deployed to hundreds of operational sites. To determine the number of and specific site locations to be visited, the security review team relies on system owners to provide documentation and discussion of these key aspects during the site-selection-determination process.

In reviewing the process and documentation of the site-selection methodology for five sample systems, we found evidence that only one system's configuration variance was reviewed or discussed to identify where differences between the local system and the baseline system might exist. Additionally, FAA was not able to provide justification for site locations chosen for security review (see Table 1).

Table 1. Documentation of FAA Site-Selection Process

System Name[a]	Total Sites	Sites Reviewed	Configuration Variance Documented?	Justification of Site Selection Documented?
ADAS	23	4	No	No
ARTS III	5	3	No	No
ASOS	885	5	Yes	No
OASIS	19	4	No	No
WMSCR	3	3	No	Yes

[a] Full system names can be found in Exhibit A.
Source: OIG

Detailed analysis of system site configurations is an important step in choosing at-risk systems for review, as well as in justifying the selection. Without a proper analysis of systems' local configurations, FAA is not able to select, for security review, the sites that are at the greatest risk—the ultimate goal of this process.

A previous audit[10] uncovered unauthorized system configurations being added to operational air traffic control systems to meet local operational needs, without central management's knowledge. These unauthorized system configurations made air traffic control systems vulnerable to attack—both from inside and outside. In FY 2006, FAA's Alaska Region experienced such an attack, which prevented aeronautical information such as required flight data needed to support various flight services from being transmitted and received. This attack was facilitated by a vulnerable system on the network that had an unauthorized system configuration. The attack forced FAA to manually provide flight information to pilots flying in that region.

To eliminate such risks and prevent similar disruption, FAA needs to enhance the selection process to include a more thorough review of system configurations. FAA should also require the selection team to document the outcomes of the site-selection process, including which specific sites were selected and for what reasons.

Systems Security Reviews at Operational Sites Lacked Examination/Testing and Were Incomplete

FAA review teams conduct security reviews of operational ATC systems by using standard security questionnaires that are developed based on the security requirements identified in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. The questionnaires typically contain from 96 to over 200 security questions, depending on the security categorization rating of the system. We found that the security reviews conducted at operational sites lacked examination and testing, and provided inadequate coverage for security checks. As a result, FAA cannot rely on these security reviews to ensure adequate security protection in operational ATC systems.

Lack of Examination and Testing

To assess the adequacy of the implementation of security controls, NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, provides three methods of review: examination, interview, and testing. NIST 800-53A states that reviewers should, *at a minimum*, conduct examination-type reviews on each of the controls and use interview- and testing-type reviews to provide further assurance of proper

[10] *Audit of Security and Controls over En Route Center Computer Systems*, OIG Report Number FI-2004-078, August 9, 2004.

implementation of a security control. We found little examination and/or testing conducted at operational sites.

- *Examination:* This is the process of physically reviewing, inspecting, or observing security controls to ensure security controls have been properly implemented.

- *Interview:* This is the process of conducting discussions with individuals concerning the posture of the systems security controls.

- *Testing:* This is the process of exercising the control under specified conditions and comparing the actual outcome against expected outcomes.

NIST guidance states that security control assessments are the principal vehicle used to verify that information systems are meeting their stated security goals and objectives. It further stresses that these assessments are not about checklists, simple pass-fail results, or paperwork to pass inspections or audits.

While review teams documented their conclusions on the questionnaires—whether specified controls worked or not—they did not specify the methods used in developing their conclusions. During one security review, OIG staff observed that FAA reviewers relied primarily on interviews with system operators in developing their conclusions, with limited examination and no testing of security controls in operational ATC systems. Specifically, the review team conducted interviews with an individual or a small group of individuals familiar with the system. Further observation revealed only limited examination-type reviews in the field, which included simply basic checks of user settings and the system's hardware connections. This happened because FAA's training for those assessing the systems did not address the importance of examination or testing.

With such a high reliance on interviews and little assurance from examination- and test-type reviews, FAA is unable to adequately ensure that minimum required security controls are in place to protect air traffic control systems. Such superficial reviews can prevent FAA from identifying vulnerabilities that could expose the ATC system to unauthorized access.

Incomplete Review of Security Controls

Our review of 21 questionnaires completed for 5 ATC systems found that more than 40 percent of the security controls on FAA's questionnaires were not reviewed. In examining 5,035 individual control questions, we found that

2,174 were left blank—43 percent—with no justification for the lack of coverage (see Table 2).

Table 2. Results of Review of FAA Questionnaires for Five Systems

System Name	Number of Questionnaires Completed/ System	Total Number of Security Questions	Total Number of Security Questions Left Blank	Percentage of Security Questions Left Blank
ADAS	6	1,302	512	39%
ARTS III	2	712	268	37%
ASOS	8	1,519	740	48%
OASIS	2	434	214	49%
WMSCR	3	1,068	440	41%
Total	**21**	**5,035**	**2,174**	**43%**

Source: OIG

On two questionnaires, more than 70 percent of security controls, including critical access control and software change control, were not reviewed—again without justification. As a result, FAA cannot rely on these security reviews to ensure adequate security protection of operational ATC systems. This resulted from weak oversight of these reviews.

FAA needs to strengthen its on-site review procedures to ensure complete coverage of security checks and examination and testing to ensure that required security controls are in place.

RECOMMENDATIONS

We recommend that the Federal Aviation Administrator direct the Chief Operating Officer of the Air Traffic Organization and the FAA Chief Information Officer to:

En Route Business Continuity Plan

1. Conduct testing to ensure that radar signals will not be lost or disrupted when using modems and telephone/fax lines to send radar data to the recovery site.
2. (a) Develop a detailed plan addressing how FAA will install network connections between radio towers and the recovery site through the local exchange carrier during BCP operations, and (b) conduct tests to ensure that

communications through the new connection can meet the latency (speed) requirements for air travel safety.

3. Develop a plan to address human integration issues such as relocating and housing air traffic controllers at the Technical Center recovery site on a long-term basis.
4. Conduct a credible cost estimate for testing the integrity of the alternate methods of re-routing radar and voice communication signals to the recovery site, and addressing human integration issues at the recovery site. Use such analysis to secure funding accordingly to complete the business continuity plan.
5. Assess the potential impact on air travel of losing each, or at least the most critical, en route centers for 3 weeks, and provide the results to the Secretary of Transportation in support of HSPD–7.

Air Traffic Control System Security Review

6. Enhance the site-selection process by requiring (a) thorough reviews of site-system configuration to ensure that sites that pose the greatest risk of unauthorized hardware/software configurations are selected for review and (b) documented justification for the sites selected for review.
7. Enhance training on on-site review by requiring review teams to conduct examination and/or testing to verify that required security controls are in place at operational sites.
8. Increase oversight of the on-site review process to ensure that all security control checks on the questionnaires are completed or properly justified if not reviewed.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided FAA a draft of our report on July 20, 2009, and received its written comments on October 14, 2009. In its comments, FAA concurred with our recommendations and has begun to take appropriate or alternative corrective actions and provided acceptable target dates for completing these actions.

While FAA concurred with all of our recommendations, it informed us that there are some limitations in addressing recommendation 5—to assess the potential impact on air travel if an en route center was disrupted for 3 weeks. To address

this recommendation, FAA plans to prepare for each ARTCC (1) a list of the airports with commercial airlines, and (2) the number of air traffic operations conducted, on average, during a 3-week period. According to FAA, however, its assessment may be limited due to the lack of information on other factors that would affect the impact—such as airlines' plans to change their bases of operations in the event of a major disruption. FAA notes that it is unlikely that airlines would voluntarily provide this strategic information.

We agree that the list FAA plans to compile will provided needed information to conduct its impact assessment. However, the list alone may not allow the Secretary to meet HSPD–7 requirements to inform the Administration and Congress of the potential impact on air travel and the economy when activating BCP operations. Accordingly, we encourage FAA and the Secretary's office to work with airlines to develop a comprehensive impact analysis. FAA's formal response is included in its entirety in the Appendix to this report.

ACTIONS REQUIRED

FAA's actions taken and planned are responsive to our recommendations and are considered resolved. These actions are subject to follow-up provisions in Department of Transportation Order 8000.1C. We appreciate the courtesies and cooperation of FAA representatives during this audit, especially those at the William J. Hughes Technical Center in Atlantic City. If you have any questions concerning this report, please call me at (202) 366-1407 or Nathan Custer, Program Director, at (202) 366-5540.

#

cc: Chief Information Officer, DOT
Assistant Administrator for Information Services/
Chief Information Officer, FAA
Chief Operating Officer, ATO
Martin Gertel, M-1
Anthony Williams, ABU-100

EXHIBIT A. SCOPE AND METHODOLOGY

Our objectives were to determine FAA's progress in correcting security weaknesses previously identified in the air traffic control system by assessing (1) the status of the BCP and (2) the methodology used in the certification and accreditation of air traffic control systems security at operational sites.

To achieve our objectives, we attended monthly progress briefings with Department of Transportation and FAA Chief Information Officers, along with FAA senior management representing the Air Traffic Organization's (ATO) BCP program and the Information Systems Security Manager (ISSM) Organization. We reviewed the BCP concept of operations to understand the scope of the BCP. We held meetings with personnel representing the work groups of the BCP program and reviewed technical requirements documents to determine the status and progress of the program. We conducted a tour of the recovery facility at the Technical Center and observed demonstrations of rerouting both radar and voice communications signals. We examined the human integration program and program funding documents.

We interviewed ATO ISSM officials and reviewed documents to determine the effectiveness of their site-selection methodology of the certification and accreditation process. We visited the Minneapolis en route center to observe the actual efforts that took place during the security review. In addition, we attended a workshop sponsored by the ATO to determine what was being done to educate and train security review teams. We examined security review results of the following selected systems to determine the adequacy of reviews performed:

- Automated Weather Observation System Data Acquisition System (ADAS)
- Automated Radar Terminal System (ARTSIII)
- Automated Surface Observing System (ASOS)
- Operational and Supportability Implementation System (OASIS)
- Weather Message Switching Center Replacement (WMSCR).

We performed our audit work from October 2007 through May 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Nathan Custer	Program Director
Mitchell Balakit	Senior Information Technology Specialist
Christopher Cullerot	Information Technology Specialist
Michael P. Fruitman	Writer-Editor

APPENDIX. AGENCY COMMENT

Federal Aviation Administration

Memorandum

Date: October 14, 2009

To: Rebecca C. Leng, Assistant Inspector General for Financial and Information Technology Audits

From: Ramesh K. Punwani, Assistant Administrator for Financial Services/CFO

Prepared by: Anthony Williams, x79000

Subject: OIG Draft Report: Follow-up Review of FAA's Progress in Enhancing Air Traffic Control Systems Protection

Thank you for the opportunity to review and comment on the findings and recommendations of the subject draft report dated July 20. The Federal Aviation Administration (FAA) concurs with all recommendations. The following is FAA's response to each recommendation.

OIG Recommendation 1: Conduct testing to ensure that radar signals will not be lost or disrupted when using modems and telephone/fax lines to send radar data to the recovery site.

FAA Response: Concur. This method of testing was performed during several demonstrations that occurred between August 8, 2007, and September 25, 2008, and resulted in no lost or disrupted radar signals. It is almost identical to the way FAA receives data today. The only difference is FAA will use regular telephone lines instead of leased lines. Currently, FAA is using dial-up lines in a number of its air route traffic control centers (ARTCC) as backup for radar data connectivity.

OIG Recommendation 2: (a) Develop a detailed plan addressing how FAA will install network connections between radio towers and the recovery site through the local exchange carrier during business continuity plan (BCP) operations, and (b) conduct tests to ensure that communications through the new connection can meet the latency (speed) requirements for air travel safety.

FAA Response 2(a): Concur. FAA's detailed plan on BCP operations is contained in its External Communications Activation Plan and Harris playbook, issued March 16, 2009 and December 9, 2008, respectively. The plan was assessed during the table top exercises in January 2009 and determined to be sufficient by the test team. This plan is available for the Office of Inspector General's (OIG) review upon request.

FAA Response 2(b): Concur. FAA tested redirecting a communications circuit from Memphis center to the Spare ARTCC (SPARTCC) and found there is no difference between re-routing the communication circuit at the ARTCC (i.e., this is how it was accomplished during the demonstration) versus re-routing it at the local carrier within the Federal Telecommunication Infrastructure cloud. FAA's way of testing proved that re-routing can be done without any latency issues.

OIG Recommendation 3: Develop a plan to address human integration issues such as relocating and housing air traffic controllers at the Technical Center recovery site on a long-term basis.

FAA Response: Concur. The air traffic controllers' union contract states that under conditions such as a BCP event, personnel may be required to relocate their duty station. Additionally, the BCP activation plans cover how FAA will relocate field personnel and provide them housing. These plans were completed in March and are available for the OIG's review upon request.

OIG Recommendation 4: Conduct a credible cost estimate for testing the integrity of the alternate methods of re-routing radar and voice communication signals to the recovery site, and addressing human integration issues at the recovery site. Use such analysis to secure funding accordingly to complete the business continuity plan.

FAA Response: Concur. The necessary infrastructure to convert the labs is in place, the activation plans are issued, and all readiness assessments and demonstrations have been completed. The BCP program will officially declare the SPARTCC "activation ready" once the Service Level Agreement (SLA) and the NAS Change Proposal (NCP) for Internet Protocol (IP) radar have been signed. The SLA and NCP serve as the basis of FAA's funding requests. The SLA has been signed and the NCP will be signed by October 31, 2009.

OIG Recommendation 5: Assess the potential impact on air travel of losing each, or at least the most critical, en route centers for 3 weeks, and provide the results to the Secretary of Transportation in support of the Homeland Security Presidential Directive (HSPD)–7.

FAA Response: Concur. The 2004 MITRE study included information on the "Potential Revenue Loss to Air Carriers Due to ARTCC Outage Scenarios" showing the results for each ARTCC. FAA does not see added value in further analysis above what MITRE concluded in its 2004 report. The range is over $40 million per day for New York Air Route Traffic Control Center to over $5 million per day for the Salt Lake Center Air Traffic Control. Clearly, the service impacts vary with the volume of traffic and the national and seasonal flows. Additionally, the FAA will provide the OIG with a list of airports (with commercial airlines) that underlie each ARTCC, and a total number of air traffic operations that each of those ARTCC's conducts, on average, during a three-week period. This information will be provided by November 30, 2009.

OIG Recommendation 6: Enhance the site-selection process by requiring (a) thorough reviews of site-system configuration to ensure that sites that pose the greatest risk of unauthorized hardware/software configurations are selected for review and (b) documented justification for the sites selected for review.

Appendix. Agency Comments

FAA Response: Concur. Since fiscal year (FY) 2007, the Air Traffic Organization (ATO) has enhanced the Certification and Authorization (C&A) Level of Effort (LOE) process to better identify and justify site-selection. FAA has been discussing methodology with the OIG for selecting specific sites and the number of sites for each system undergoing C&A. This methodology is described in the following paragraphs.

The LOE process requires that the System Owner submit an LOE Briefing and System Characterization document prior to scheduling field site visits for that system. The information required provides technical details on the system architecture and operating environments, and includes configuration variances that may exist at certain sites, based on the System Owner Program Office, and their support organizations when appropriate. The LOE Briefing has a specific section that requires detailed information on system configuration differences and locations where the configuration differences may exist. The ATO Information System Security (ISS) Program reviews both documents and identifies specific sites that are tagged as "must be visited" sites. In addition, the objective of selecting an adequate number of representative sites must be met for each system. Typically, there is a minimum of three operational sites that must be visited for all systems, unless a system has less than three fielded locations. This objective of a minimum of three sites is implemented even for systems that are deployed with the same standard configuration baseline. For example, if a system is operating at 20 ARTCCs, then a minimum of three ARTCCs must be visited to obtain an adequate representative sample, even though the systems have the same configuration baseline. There is also a conscious effort to distribute the site visits across multiple facilities for systems being recertified, so that different facilities are selected for the current year, as compared to the last C&A site visits (typically three years earlier). This approach provides a broader site visit sampling spreading across different C&A years. So visits in FY 2010 for a specific system will intentionally pick different sites than those selected in FY 2007, unless there are specific reasons to revisit the same facility for that system (i.e., certain facilities tend to be used as a "key site" for implementing technology/functionally upgrades, prior to making the changes at other sites for that specific system).

Additionally, the ATO LOE process requires mandatory visits to sites where systems are configured differently from the standard system configuration baseline to assess the risk of the different configurations at specific sites. For example, if a system is deployed to 20 ARTCCS and one of the systems has a significantly different configuration than the other 19 (e.g., hardware, software, internal/external connectivity), then that site with the different configuration must also be audited in addition to the minimum three site visits.

System sites are also selected based on the facility type where the system is deployed to assess the risk of systems deployed in different operating environments. For example, systems that may be deployed in both the En Route (e.g., ARTCCs) and Terminal [e.g., Terminal Radar Approach Control (TRACON) facilities] environment must include site visits to both En Route and Terminal facilities to assess the system risk in those operating environments.

Mandatory site visits and justification are documented in the Risk Assessment Site Survey Plan and the System LOE Determination, which is developed each Fiscal Year for every ATO system that is scheduled to complete C&A.

Appendix. Agency Comments

Results of the LOE Determination are emailed by the ATO ISS Program to the Independent Risk Assessment and Test Team (IRAT) and System Owner, including a copy of the System Site Survey Plan. After the LOE Determination is transmitted, further discussions occur between the IRAT and the System Owner organization to validate the system configuration baseline and possible configuration differences that may be fielded. If configuration differences are identified after the LOE Determination, the ATO ISS Program is notified and the System LOE Determination is modified to include mandatory site visits to the sites where configuration differences exist.

OIG Recommendation 7: Enhance training on on-site review by requiring review teams to conduct examination and/or testing to verify that required security controls are in place at operational sites.

FAA Response: Concur**.** FAA has completed implementation of this recommendation as described below.

The ATO security operating environment is very complex, with hundreds of systems, thousands of manned and unmanned facilities, operations, and management processes sprawling across 50 states and international borders. Understanding how to properly apply risk analysis and security testing processes across the ATO environment is equally complex and must take into account several key aspects.

The first key aspect is that the ATO consists of three distinct operating environments – NAS, Mission Support, and Administrative. The NAS environment includes systems that directly support safety-critical Air Traffic Control (ATC) services. Because of the safety critical nature of the NAS environment, NAS systems must be protected and operate at higher information assurance levels than Mission Support and Administrative systems. Mission Support systems indirectly support the conduct or management of ATC operations and do not impact safety of ATC operations. Administrative systems support the provision of routine ATO administrative services, such as email. Mission Support and Administrative systems have a completely different operations, management, and maintenance infrastructure than NAS systems. Additionally, there are major differences in the application of security controls and processes for conducting risk assessment and testing in each environment.

The second key aspect in ATO is the separation of NAS systems operating environment from the Mission Support/Administrative systems operating environment. Separation is provided through the use of two network infrastructures that are physically and logically isolated, as follows:

- NAS Operations (Ops) IP Network
- Mission Support/Administrative IP Network.

The physical and logical separation of the NAS and Mission Support and Administrative networks is a critical factor in ensuring that NAS systems can continue to provide a high level of service availability, information integrity, and confidentiality needed to maintain air traffic safety and efficiency.

The third key aspect of the ATO operating environment is the use of authorized communications gateways and Internet Access Points (IAPs) to provide boundary protection between the NAS and Mission Support and Administrative environments and external network infrastructures. Additionally,

specialized system communications gateways, such as the ARTS Gateway (AGW), provide boundary protection between NAS systems and other non-NAS systems [e.g., the ARTS and National Offload Program (NOP)].

The ATO operating environment was specifically architected to separate the NAS environment from the Mission Support/Administrative environment because NAS systems provide safety critical ATC services. NAS systems operate on a physically separate network infrastructure from all other FAA systems in order to maintain a higher service assurance level and minimize risk. Any disruption to a

NAS system may cause impacts to safety and efficiency. Even short-term system outages cause ripples throughout the NAS that may result in significant adverse impacts in terms of extra fuel consumed and time delays. Because of safety and economic factors, the primary consideration in conducting security testing of NAS operational systems is to ensure that NAS services are not interrupted.

In order to maintain NAS safety and efficiency, and continue to provide the NAS operating environment with a high level of information assurance, ATO has taken several steps during the past three years to enhance its security testing methodology, and to provide enhanced test methodology training to Independent Risk Assessment Team (IRAT) personnel, which is described in the following paragraphs.

Since fiscal year (FY) 2007, the ATO has enhanced the process for testing critical ATC systems at NAS operational sites by conducting observation and demonstration testing of implemented security controls. With the implementation of NIST 800-53A, greater use of examination and testing will be needed. For most NAS systems, the stringent implementation validation of all changes to systems is fully tested at the support centers William J Hughes Technical Center (WJHTC) and Mike Monroney Aeronautical Center (MMAC) prior to releasing to the field. The formal process of releasing System Support Modifications (SSM) for NAS Systems and creating an audit mechanism through the Maintenance Management System**,** allows the tracking of individual sites implementing planned upgrades and modification. For NAS systems, field personnel are implementing changes as directed through SSM issued for the system, otherwise system configurations seldom change.

As for conducting electronic security scan testing, it is a well known fact that even the use of non-intrusive security testing tools does occasionally cause various operating system failures or lock-ups. Therefore, ATO relies on greater observation and demonstration testing methods at the system operational sites, and conducts much of the security testing using replicas of fielded systems in the WJHTC or MMAC test environments.

In fielded operational sites, observation and demonstration consists of the FAA system specialist demonstrating system security controls through presentation of “screen shots” or printouts of system security policies. Although demonstration and observation testing requires more time than system scanning, it significantly reduces the chances that testing will inadvertently “bring down” an operational NAS system. Additionally, demonstration and observation testing eliminates potential “false positives” that are encountered through the use of scan test tools. Part of the enhanced process moving forward will be to perform extractions from the observation and demonstration testing (e.g., printouts) in order to better document testing results at the operational site. For fielded assets such as routers, firewalls, managed switches, etc., greater use of extractions of configuration files and rules

are planned to validate against the version controlled releases of those files from WJHTC and MMAC, which would be tested in the support system environment.

A key measure that ATO has undertaken is to conduct operational site security testing of new ATC systems, prior to commencement of ATC operations. The full range of security tests, including scan testing is conducted on the system at the operational site. This ensures that the system is tested in the exact operational site configuration. Examples of operational site testing included the Wide Area Monitoring System (WAM) and Operational and Supportability Implementation Systems. ATO will

continue to conduct operational site testing using scan test tools on all new ATC systems as they continue to be deployed in the NAS.

The ATO also conducts security testing for legacy ATC systems using passive and active (e.g., penetration testing) software tools on system at either the WJHTC or MMAC laboratories. The labs at WJHTC and MMAC also have the capability to be configured to represent a specific operational site. For example, the WJHTC ATOP lab can be configured to the same operational site configuration as the ATOP system deployed at New York, Oakland, and Anchorage.

Additionally, ATO conducts on-site testing of operational ATC mission support systems if there will be no impact to operational ATC Systems. Some examples of ATC mission support systems tested on-site include National Off-Load Program (NOP), CRU-X, CAEG, IAPs, LSSD, and STARCASTER.

Moving forward, the ATO will use a combination of all the methodologies listed above to continually assess ATC system security, while continuing to minimize the potential for adversely impacting air traffic safety or efficiency.

Risk Assessment Team personnel, both FAA and contractor, participated in the enhancement of the system security testing methodology and were trained as part of the development efforts. All new IRAT FAA personnel are trained on-the-job via shadowing techniques and study of risk assessment process documentation. New contractor personnel are required to have security risk assessment and testing experience and are trained on the specific methodology via internal company training.

OIG Recommendation 8: Increase oversight of the on-site review process to ensure that all security control checks on the questionnaires are completed or properly justified if not reviewed.

FAA Response: Concur. FAA has completed implementation of this recommendation. The ATO uses a questionnaire as part of the Risk Assessment on-site review process. The questionnaire consists of NIST SP 800-53 rev2 security controls that address all 17 NIST 800-53 Security Control Families. Systems that have a FIPS-199 Security Categorization (SC) of Low, Moderate, or High are evaluated using the appropriate Low, Moderate, or High set of NIST 800-53 rev2 security controls (i.e., questionnaire). For example, a questionnaire that contains the “Moderate” set of security controls will be used to assess a system with a “Moderate” FIPS-199 SC. Questionnaires that contain the “Moderate” set of security controls consist of the Moderate and Low set of NIST 800-53 Security Controls. Finally, questionnaires that contain the “Low” set of security controls consist of only the Low set of NIST 800-53 Security Controls.

Appendix. Agency Comments

Depending on their life cycle support, there are some NIST Security Control Families, and specific controls within Families, that are not applicable for conducting interviews of system technical personnel. Implementation of some NIST Common Security Control Families, such as CA, may be the sole responsibility of another FAA organization, such as FAA Headquarters or the System 2nd Level Support Facility, and not the on-site system specialist. For example, questions in the CA Family of NIST 800-53 Security Controls may be categorized as "Common Controls" and are the responsibility of FAA Headquarters organizations, not the responsibility of field site personnel.

Starting in FY 2009 the ATO enhanced the on-site review process, in order to eliminate "blank" or "NA" questions that may result from on-site reviews. Enhancements include tailoring the questionnaires to indicate whether a specific question (security control) is appropriate for use on site, depending on the role(s) of the facility/site personnel. For example, field specialists that are not responsible for issuing changes to a system's Technical Manual will be annotated as N/A for that site, and further annotated to indicate what organization is responsible or would be the source of the information being requested (e.g., WJHTC issues Technical Manual Revisions). The tailoring may include documenting on each specific question (security control) whether it applies, including the rationale. For example, some questions that are not applicable for on-site review, such as the CA family, are annotated "N/A Common Control," and are not addressed during the on-site review. This enhanced process includes responses to all questions on the site survey form, and reduces the chance that a question may not be addressed, and provides justification for focusing responses for specific questions based on an individual's organization's role in developing and implementing security controls.

S:\\ABU-100\OIG GAO\09-20 ATC Sys Sec revised final 9/2/09

Appendix. Agency Comments