Office of Inspector General

Audit Report

FAA'S CONTINGENCY PLANS AND SECURITY PROTOCOLS WERE INSUFFICIENT AT CHICAGO AIR TRAFFIC CONTROL FACILITIES

Federal Aviation Administration

Report Number: AV-2015-112
Date Issued: September 29, 2015

Memorandum

U.S. Department of Transportation

Office of the Secretary
of Transportation

Office of Inspector General

Subject: **ACTION:** FAA's Contingency Plans and Security Protocols Were Insufficient at Chicago Air Traffic Control Facilities
Federal Aviation Administration
Report No. AV-2015-112

Date: September 29, 2015

From: Matthew E. Hampton
Assistant Inspector General
for Aviation Audits

Reply to Attn. of: JA-10

To: Federal Aviation Administrator

The Federal Aviation Administration (FAA) operates a vast network of facilities and equipment to manage America's National Airspace System. On September 26, 2014, an FAA contract employee deliberately started a fire that destroyed critical FAA Telecommunications Infrastructure (FTI) equipment at FAA's Chicago Air Route Traffic Control Center[1] (Chicago Center) in Aurora, IL. This equipment provides critical voice and data communications that support air traffic operations at FAA facilities nationwide. As a result of the damage, Chicago Center was unable to control air traffic for more than 2 weeks, thousands of flights were delayed and cancelled into and out of Chicago O'Hare and Midway airports, and aviation stakeholders and airlines reportedly lost over $350 million dollars.

Given the high volume of air traffic in the Chicago airspace, six Members of Congress[2] requested that we review the emergency and security protocols at Chicago air traffic control (ATC) facilities. Specifically, they asked us to determine whether adequate protocols, emergency plans, and security measures are in place to prevent or mitigate the impact of such emergencies in the future.

Accordingly, our objectives were to (1) assess whether FAA has developed and implemented a business continuity plan for the Chicago air traffic control facilities that provides for adequate levels of redundancy and resiliency,[3] and (2) evaluate

[1] Centers are the major communication hubs for flight plan routing and the systems that provide radar and communication services to aircraft operating above 18,000 feet. FAA has 21 Centers geographically dispersed across the United States.

[2] For a list of the Members of Congress who requested this audit, see exhibit D.

[3] Redundancy is defined as the presence of more than one independent means of accomplishing a given function. Resiliency is defined as the ability to detect, avoid, mitigate, adapt, and recover from the interruption of a service or capability.

whether the security measures in place at the Chicago facilities are currently maintained and sufficient to mitigate potential risks to the U.S. air traffic control system. In addition, we are currently conducting a separate self-initiated audit to examine IT security controls and contingency plans at large consolidated Terminal Radar Approach Control Facilities (TRACONs), including Chicago TRACON.[4]

We conducted our work in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology, and exhibit B lists the organizations we visited or contacted.

RESULTS IN BRIEF

The fire at Chicago Center demonstrated that FAA's contingency plans for the Center and the airspace it controls do not ensure redundancy and resiliency for sustained operations. For example, FAA's plans at the time did not contain procedures for transferring air traffic and airspace responsibilities from Chicago Center to other facilities. As a result, FAA quickly abandoned its contingency plans after the fire and reverted to an outdated 2008 plan to begin the process of restoring normal operations. Moreover, the damage to Chicago Center highlighted weaknesses in FAA's current air traffic control infrastructure, which has limited flexibility to respond to system failures and facilitate the return to normal operations. For example, the loss of computerized flight data processing was a major constraint to returning to normal air traffic levels during this event. Specifically, each scheduled flight through Chicago airspace required handwritten flight progress strips[5] which increased controller workload, limited traffic, and presented additional risk into the National Airspace System (NAS). While FAA completed a 30-day review of its contingency plans following the Chicago Center incident, significant work remains to prevent or mitigate the impact of similar events in the future. Furthermore, new technologies that are expected to improve FAA's continuity of air traffic operations will not be available for years.

The security protocols in effect at the time of the Chicago Center fire were insufficient to identify, counter, or mitigate the impact of an insider threat to the air traffic control system. For example, the protocols lacked the controls necessary to block facility access to a contract employee no longer assigned to the facility. Instead, FAA officials told us that the prevention of *external* threats was the primary focus of FAA security policies prior to the Chicago Center incident. In the aftermath of the Chicago event, FAA conducted a review of the existing security policies and procedures within the facility. This security review resulted in 42 recommendations,

[4] *Audit of Security Controls over FAA's Large Terminal Radar Approach Control Facilities*, (OIG Project No. 14F3012F000), August 7, 2014. OIG reports and announcements are available on our Web site at http://www.oig.dot.gov/.

[5] Flight progress strips are used by air traffic controllers to record the progress of a flight, and help to pass information from one controller to another. They contain vital information including aircraft identification, aircraft type, assigned altitude, departure, destination, etc.

24 of which FAA considers essential to improve facility security. Implementing these recommendations will require substantial investments by the Agency.

We are making recommendations to help FAA improve redundancy and resiliency in the NAS and implement improvements to its operational contingency plans and security protocols.

BACKGROUND

FAA's Air Traffic Organization (ATO) is responsible for providing safe and efficient air navigation services to the NAS and, among other things, develops and implements contingency plans for restoring air traffic service in response to emergencies. ATO also develops contingency policies, which provide guidance and procedures for maintaining continuity of air traffic services during outages and requires ATC facilities to conduct annual contingency plan training.

FAA's Office of Security and Hazardous Materials Safety's (ASH) mission is to develop and administer policies and programs that help ensure aviation safety, support national security and promote an efficient airspace system. ASH has the primary responsibility for security and critical infrastructure protection, emergency operations, contingency planning, and intelligence activities. ASH functions include developing and implementing policy to protect employees, facilities, and assets; conducting inspections at FAA facilities to determine compliance with facility and communications security; and managing the identification (ID) programs for the Agency.

In 2014, there were two events in which smoke and/or fire at a Chicago area air traffic control facility resulted in significant flight delays and cancellations. The first incident, on May 13, 2014, at Chicago TRACON, was caused by an overheated exhaust fan and resulted in a facility evacuation that lasted about 4 hours. The second incident, on September 26, 2014, at Chicago Center, was a deliberately started fire that destroyed Chicago Center's FTI telecommunication system[6] and disabled the capability to transfer flight data electronically. The fire and smoke, combined with water from the fire suppression system, also damaged power sources, phone and internet services, and weather systems.

[6] FTI provides critical voice and data communications that support air traffic operations at FAA facilities nationwide. FTI is owned and maintained by Harris Corporation and leased to the FAA.

FAA'S CONTINGENCY PLANS DID NOT ADDRESS REDUNDANCY OR RESILIENCY OR ENSURE CONTINUITY OF AIR TRAFFIC OPERATIONS AFTER THE CHICAGO FIRE

The contingency plans developed by Chicago's major air traffic control facilities did not address redundancy or resiliency and were insufficient to restore operations after the Chicago fire. As a result, FAA immediately discarded Chicago Center's contingency plan after the incident. In addition, the damage to Chicago Center required extensive cleanup and system repairs and revealed weaknesses in FAA's current air traffic control infrastructure. Although FAA completed an internal 30-day review of its contingency planning, many new technologies which are expected to improve FAA's continuity of air traffic operations will not be available for years.

FAA Experienced Delays and Other Difficulties in Restoring Operations Due to an Insufficient Contingency Plan at Chicago Center

Chicago Center's contingency plans at the time of the Chicago incident were insufficient to meet the demands of restoring operations. Although the plans were up-to-date and met the requirements prescribed in FAA's current policies,[7] they focused on maintaining high levels of safety with minimal traffic movement and did not address redundancy or resiliency. The contingency plans were designed mainly for short-term use and only allowed for non-radar flight routes.[8] Immediately after the fire, the facilities supporting Chicago Center had to reroute high-altitude flights and increase the separation between aircraft, according to their contingency plans.[9] In addition, FAA directed the major Chicago airports to initiate a ground stop;[10] however, all of these actions were insufficient to keep up with air traffic demand.

Given these limitations, Chicago Center personnel discarded the existing contingency plan and collaborated with the adjacent Centers (Cleveland, Minneapolis, Kansas City, and Indianapolis) to develop a new plan. This plan, based on Chicago Center's 2008 contingency plan and airspace map, included transferring responsibility for controlling Chicago Center's airspace to the four adjacent Centers, as well as to the underlying TRACONs. Although the 2008 plan and map required extensive adjustments to ensure adequate radar and radio communication coverage for Minneapolis and Cleveland Centers, it was a valuable aid for beginning the process of returning Chicago Center to normal operations (see exhibit C).

[7] FAA Order JO 1900.47D, Air Traffic Control Operational Contingency Plans, Effective March 8, 2013.

[8] A flight path or route which the pilot is performing his/her own navigation. The pilot may be receiving radar separation, radar monitoring, or other ATC services while on a non-radar route.

[9] Every air traffic facility is required to have a contingency plan to respond to emergency situations.

[10] A ground stop is a procedure requiring aircraft that meet specific criteria to remain on the ground. The ground stop may be airport specific, related to geographical area, or equipment related.

In contrast to the new plan, FAA's discarded plan (developed in August 2014) did not contain any procedures for transferring control of air traffic to neighboring facilities—largely because FAA had stopped requiring that plans contain these procedures. FAA officials explained that the Agency eliminated the requirement for en route airspace in 2009 because previous outages never lasted more than a few hours and FAA never lost multiple capabilities (i.e., communications, automation, radar, and flight data processing) at once.

Instead, based on the technical capabilities at the time, FAA chose to create a Spare Air Route Traffic Control Center (SPARTCC) facility at FAA's Technical Center in Atlantic City, NJ, to be used during contingency situations. However, FAA was not able to use the SPARTCC facility during the Chicago fire due to incompatible equipment. At the time of the Chicago Center fire, the SPARTCC was equipped with the HOST[11] system, while Chicago Center had already transitioned to the En Route Automation Modernization (ERAM) system. Although the SPARTCC was declared "Activation Ready"[12] in 2009, FAA stated that it would have taken at least 4 weeks for the SPARTCC to become operational and manage air traffic. FAA plans to update the SPARTCC with ERAM after all other planned sites are installed. FAA completed the planned ERAM installations in March 2015; however, the SPARTCC has yet to be equipped with ERAM.

In addition, Chicago facility employees did not have adequate training on the contingency plans. Air traffic facilities are required by Order 1900.47D to complete annual contingency exercises and compile a lessons learned report after contingency events and exercises. These reports are maintained and shared in a Web-based application secured behind FAA's Intranet firewall. While Chicago Center met the annual requirements, FAA officials explained that the effectiveness of training was limited because it was mainly comprised of table-top exercises or fire drills for support staff, rather than the controller workforce. FAA officials explained it is very difficult to realistically practice contingency plans because it is not safe or practical to disable live operational systems for training exercises. However, facility personnel we interviewed believe contingency exercises can be significantly improved by simulating more realistic scenarios.

As a direct result of the Chicago Center incident, FAA plans to modify its current contingency plans to introduce the potential for transferring air traffic control responsibilities from one en route facility to neighboring support facilities. Although the new policy has not been finalized or published, there are several views concerning how facility contingency plans should be revised. According to a senior FAA official, each facility should develop a detailed contingency plan that includes transferring

[11] HOST is the legacy en route automation system, which consists of 40-year old computer hardware and software system.

[12] The "Activation Readiness" declaration indicates the completion of the design and implementation phases, including the systems and procedures, required for activation of the SPARTCC.

airspace, flight paths, and corresponding changes to automation systems. However, Chicago air traffic officials we interviewed stressed the importance of flexible contingency plans that can be adapted to different situations. In addition, officials at Chicago Center believe it will be important for future contingency plans to include a recovery plan for reverting airspace and services back to normal operations.

The Chicago Incident Resulted in Extensive Damage and Repair Efforts

The Chicago Center incident on September 26, 2014, required significant, time consuming, and costly repair efforts to restore operations. According to officials at Chicago Center, the return to normal operations, in many respects, was more difficult than responding to the original system failure. FAA Technical Operations and Air Traffic employees, as well as FAA management from Chicago Center and adjacent facilities, worked with contract employees to replace or repair damaged equipment and restore Chicago airspace to normal operations by October 13, 2014. Among other recovery tasks, FAA and its contractors:

- manufactured and installed over 20 racks of telecommunication equipment,
- replaced 10 miles of cable,
- rerouted communications to adjacent facilities,
- restored 835 telecommunication circuits,
- installed a wireless communication network at Chicago Center, and
- conducted a flight inspection[13] of the entire airspace to ensure that all frequencies and newly installed telecommunications equipment functioned properly.

FAA estimated that the cost for recovery operations at Chicago Center was more than $5.3 million dollars (see table 1). This amount does not include the cost of new FTI communications equipment.

[13] Flight Inspection ensures the integrity of instrument approaches and airway procedures that constitute our NAS infrastructure.

Table 1. FAA's Estimated Cost of Recovering Operations at Chicago Center

Expense	Current Estimates
Travel	$ 367,271
Overtime	$ 1,266,726
Cleanup	$ 1,175,726
Building Repair	$ 533,198
Equipment	$ 184,655[14]
Security/Guard Services	$ 28,974
Miscellaneous	$ 953,045
Contractor Claims	$ 800,000
Total	**$ 5,309,595**

Source: FAA data as of April 2015

FAA's Current Air Traffic Control Infrastructure Lacks Flexibility and Resiliency

The Chicago Center incident highlighted the limited flexibility and lack of resiliency in critical elements of FAA's current air traffic control infrastructure, including limited communication capacity and the inability to easily transfer control of airspace and flight plans. For example, re-routing communications for air traffic control to other facilities is not a rapid or seamless process. While the current infrastructure can be reconfigured to adapt in emergency situations, the execution time is measured in days rather than hours. Moreover, once traffic has been rerouted, the complex nature of air traffic control operations makes it very challenging to sustain for any significant period of time.

The incident highlighted the following infrastructure limitations:

Communication Between FAA Facilities. The location of FAA's FTI equipment inside the facility made it more vulnerable to an extended outage. Outside of the Chicago Center facility, FTI is connected by two independent (primary and backup) fiber optic pathways in order to ensure redundancy and diversity.[15] However, inside the Chicago Center building, all FTI equipment racks (both primary and backup) are located in close proximity to one another with no physical barriers. An industry official explained that separating the existing FTI equipment inside an ATC facility would present several challenges, such as cost, physical space limitations, installation time, and the risk of service disruptions. However, as a result of the incident, the FTI contractor is planning to add more services directly to its internal network to improve

[14] FAA equipment cost does not include new FTI equipment. Harris Corporation was responsible for the cost of the new FTI equipment.

[15] For the purposes of this report, we refer to diversity problems as instances where there is not adequate separation between FTI primary and backup paths. We did not examine the overall FTI architecture or design.

the time it takes to redirect communications. This would allow communications to be moved and redirected remotely within hours without depending on local telecommunication providers. This is important because after the fire, in some instances, it took local telecommunication companies days to redirect communications, which prolonged the recovery process.

The FTI loss during the incident also caused Chicago Center to initially lose its internet and phone services, which impeded communications with other air traffic facilities and hindered the recovery process. For example, Chicago Center relied on employees' personal cell phones and mobile internet service to send airspace maps and other vital information until FAA could install a secure wireless network. Presently, FAA's other Center facilities lack a secure wireless network that can be switched between FAA's local area network (LAN) and alternate internet access for contingency situations.

In addition, the loss of communication capability greatly impacted other air traffic facilities that are connected with Chicago Center and underscored the interdependence among air traffic facilities. Several Chicago air traffic officials indicated that they did not realize how dependent they are on Chicago Center for many critical systems, including voice switches, radar surveillance and data tags, automation, and flight information. For example:

- Chicago Terminal Radar Approach Control (TRACON) ran out of available voice communication circuits and needed an additional 12 phone lines installed. FTI did not have enough bandwidth available; therefore, commercial lines were installed, but these lines occasionally dropped calls.

- Chicago Midway Tower had limited voice switch capabilities because there were issues with the direct communication lines that feed its voice switch. Midway tower also lost all radar data tags on its Airport Surface Detection Equipment-Model X (ASDE-X) system, which controllers use to help prevent accidents on runways.[16] The tags include vital information such as flight number, speed, and aircraft type.

- Chicago O'Hare and Midway Towers initially lost their digital Automated Terminal Information Service (ATIS)[17] system, which broadcasts key flight information such as available runways and weather to pilots. Until the digital ATIS was restored, controllers had to manually record this vital information and update the recording at least once per hour.

[16] ASDE-X helps maintain safe separation of aircraft and vehicles on the airport surface and aid controllers in avoiding ground collisions.

[17] ATIS is a continual broadcast of recorded aeronautical information, such as weather information, which runways are active, available approaches, and other information required by pilots.

Radar Surveillance for Tracking Aircraft. FAA lacks a national system to centralize and distribute long-range radar.[18] Many of the current radar systems do not have the flexibility to easily transfer radar information to multiple facilities; this information must be manually moved and tested. Several facilities that received sections of Chicago Center's airspace had challenges with inadequate radar coverage. Specifically, while Chicago TRACON has a direct feed to the short-range terminal radar,[19] it lost the long-range radar following the fire because this information is routed through Chicago Center. As a result, Chicago TRACON had to manage aircraft outside of the effective range of radar coverage. In addition, at Kansas City Center, FAA had to re-route and adjust the long-range radar information to manage arrival and departure traffic.

Automation To Manage Air Traffic Control. ERAM, a foundational program for the Next Generation Air Transportation System (NextGen),[20] is an automation system that helps controllers manage high-altitude traffic. According to FAA officials, Chicago Center's ERAM system was not able to provide air traffic control services in the aftermath of the incident due to the damage to the Center's telecommunications network. As a result, FAA had to transfer Chicago Center's air traffic control responsibilities to adjacent facilities, because ERAM does not automatically enable one Center to control another Center's airspace.

Furthermore, the four adjacent Centers had to modify their site-specific ERAM software to allow the system to monitor Chicago Center airspace. Additional communication lines were also added so that ERAM could coordinate aircraft "hand-offs"[21] between ATC facilities that normally do not communicate with each other. A recent report by the National Research Council[22] highlighted both the Chicago incident and a previous ERAM outage at Los Angeles Center in April 2014. The report also warned about apparent software design flaws and insufficient back-up systems, as well as questioned whether implemented fixes actually resolved identified problems. The report and operational experience have raised concerns about ERAM's flexibility and ability to support NextGen initiatives.

Filing, Processing, and Distributing Flight Plans. Flight plans[23] are processed and distributed through FAA's 21 Centers. When the fire destroyed the FTI communications at Chicago Center, flight plans could not be electronically

[18] Air Route Surveillance Radars (ARSRs) are long range radars with a range of about 250 nautical miles.

[19] Airport Surveillance Radars (ASRs) are short range radars with a range of about 60 miles.

[20] NextGen is FAA's multibillion-dollar transportation infrastructure project aimed at modernizing our Nation's aging air traffic system.

[21] An action taken to transfer the radar identification of an aircraft from one controller to another.

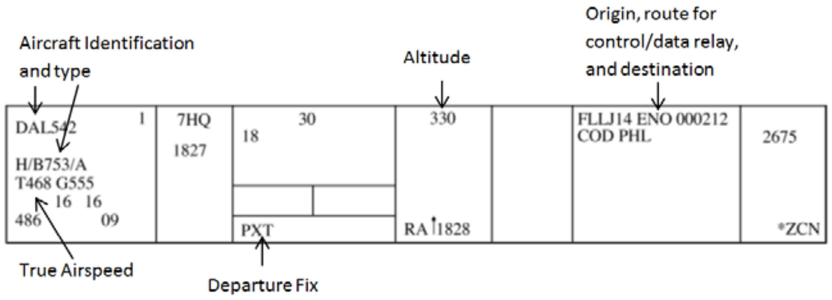
[22] National Research Council of the National Academies – A Review of the Next Generation Air Transportation System: Implications and Importance of System Architecture.

[23] Flight plans are specific information relating to the intended flight of an aircraft that is filed with an air traffic control facility. Information includes departure and destination, aircraft identification, route of flight, altitude, estimated time, etc.

transferred. Therefore, every facility coordinating traffic with Chicago Center had to manually process flight plan information during the entire outage.

FAA officials explained that the biggest obstacle to providing air traffic services was the inability to automatically transfer flight plan information between facilities. Manual flight plan processing was a principal driver of the increased workload and introduced unnecessary risk into the NAS because of the increased potential for errors. For example, for every flight departing Midway Airport, controllers had to radio the pilot to receive the aircraft, altitude, and route information; handwrite the flight progress strip (see figure 1); input this data into the computer; and then call Chicago TRACON on a landline to coordinate the flight. This process led to significant delays because pilots had to wait 20 to 30 minutes to depart while controllers manually entered the data.

Figure 1. Example of a Typical Flight Progress Strip

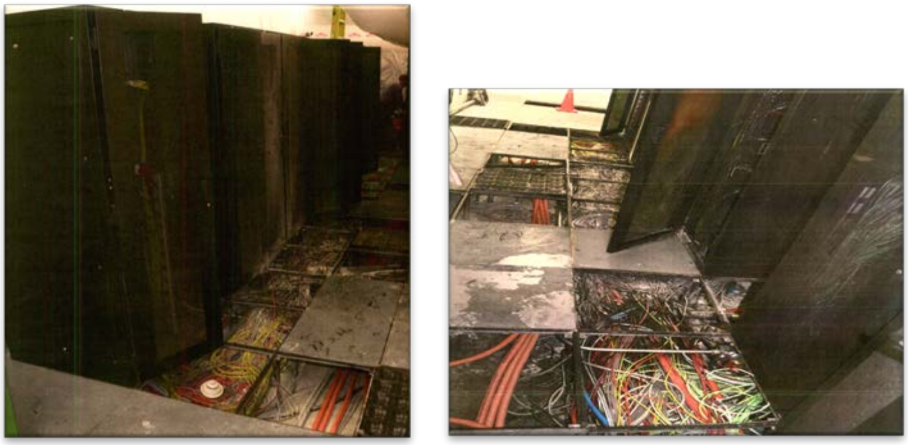


Source: FAA

Fire Suppression Capabilities. Chicago Center's fire suppression system was water-based, and although the system was effective at containing the fire, it caused extensive equipment damage. Approximately half of the FTI equipment racks were destroyed by water from the fire suppression system (see figure 2). This extended the cleanup and restoration effort and limited resiliency.

Industry experts stated that a compressed gas fire suppression system would have reduced some of the equipment damage at Chicago Center. Unlike dry chemicals, foam, or water, compressed gas systems do not leave a residue, and equipment undamaged by the fire can typically be quickly reactivated and returned to service. However, these systems are more expensive and require more complex system engineering. In the past, Chicago Center used a Halon gas system, but it was removed when Halon systems were banned nationwide because of environmental concerns.

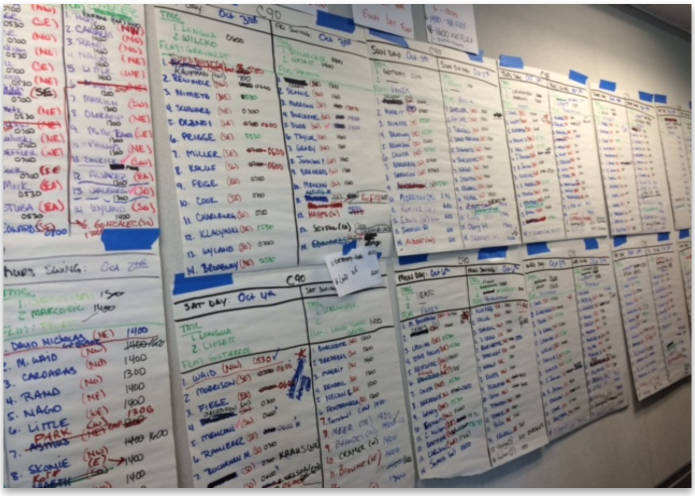
Figure 2. Chicago Center's Fire Damage



Source: FAA

Controller Staffing Impacts. Sustaining operations for extended periods under contingency conditions severely strained Chicago Center's staffing resources. About 180 controllers traveled to the adjacent facilities to assist with problems associated with insufficient frequency and radar coverage and to manually enter flight data. Chicago Center controllers were required to be onsite at the other facilities because controllers at adjacent facilities were not familiar with the Chicago Center's airspace and procedures. Daily controller facility assignments had to be scheduled manually on Chicago Center's "schedule wall," as depicted in figure 3. This process was very labor intensive because Chicago Center's administrative network was down and the scheduling software was not designed to schedule Chicago controllers at other facilities. In addition, several support facilities, such as Champaign tower, had to operate extended hours and handle up to four times their normal level of air traffic.

Figure 3. Example of Manual Controller Scheduling



Source: OIG

FAA Completed a 30-Day Review of Operational Contingency Plans, but Significant Work Remains To Implement Corrective Actions

To FAA's credit, the Agency took swift action to review its contingency plans following the Chicago Center fire. Specifically, the Agency's ATO completed a 30-Day Assessment of Operational Contingency Plans as directed by the FAA Administrator and identified five "next steps" (see table 2) to be completed within 1 year. While efforts have begun, some of FAA's proposed completion dates may be overly optimistic. Additionally, FAA's next steps have not yet been linked to completion milestones, nor have the required resources been identified.

Table 2. Next Steps Within 1 Year From FAA's 30-Day Assessment of Operational Contingency Plans

Next Steps	Status and FAA Action Taken and Planned
(1) Establish a central office to manage contingency planning, including policy and oversight of facility plans.	**Partial.** In February 2015, FAA created the Temporary Operational Contingency Office (TOCO). This office will terminate in March 2016.
(2) Implement target levels of efficiency while simultaneously achieving target levels of safety during NAS contingencies.[24]	**Open.** FAA has not officially implemented the targets. According to FAA officials, meeting these targets depends almost entirely on funding, the development of new contingency plans, the scope and type of a given emergency, and the damage incurred.
(3) Update FAA Orders and facility contingency plans to address requirements for site-specific contingency plans.	**Ongoing.** FAA is drafting a new Operational Contingency Plan (OCP) Order requiring air traffic facilities to develop a plan for transferring control of airspace to surrounding facilities. FAA originally anticipated completion in June 2015, but recently moved the projected publication date to fall 2015. Air traffic facilities will be developing new plans, but they cannot be implemented until the new order is published.
(4) Conduct technical assessment of new contingency plans for supportability and viability, and provide infrastructure cost estimates.	**Ongoing.** The FAA's Air Traffic Organization (ATO) is reviewing existing technological limitations of Center facilities and has identified rough order of magnitude (ROM) cost estimates for infrastructure improvements. However, no completion dates have been provided.

[24] These targets include: (1) Return Core 30 airports to 90 percent operating capacity within 24 hours and (2) Return Center and TRACON airspace to 90 percent of normal operating capacity within 96 hours.

Next Steps	Status and FAA Action Taken and Planned
(5) Conduct assessment of system resiliency within air traffic control facilities and provide detailed cost estimates for proposed improvements.	**Ongoing.** In December 2014, FAA created a Resiliency Assessment Team tasked to develop recommendations to improve the resiliency of critical services at FAA's busiest facilities. According to FAA, recommendations for targeted fiscal year 2017 investments have been briefed to FAA's Capital Investment Team (CIT). However, to date, OIG has not received a copy of the final report.

Source: FAA 30-Day Review of Contingency Plans

While the five next steps described in table 2 are positive, FAA has not yet determined how to permanently manage future contingency plans, policy, and oversight after the Temporary Operational Contingency Office (TOCO) is dismantled in March 2016.

In addition, it is not yet clear whether the target levels of efficiency identified by the FAA Administrator are realistic based on the current state of technology in the NAS. These targets include: (1) Return Core 30 airports[25] to 90 percent operating capacity within 24 hours, and (2) Return Center and TRACON airspace to 90 percent of normal operating capacity within 96 hours. According to FAA officials, the technical and resiliency assessments included in FAA's "next steps" are focused on determining what infrastructure and system changes are needed to achieve these targets (see table 2 above). To date, these assessments have not been completed; therefore, it is unknown if the Administrator's efficiency targets will or can be met.

Furthermore, until FAA's new contingency plan regulations are finalized and published, which is expected in fall 2015, air traffic facilities will not be able to begin the process of updating facility-specific contingency plans. Finally, it will take extensive resources and time to develop, approve, and coordinate these new contingency plans throughout the NAS.

New Technologies and Planned Capabilities for Improved Continuity of Air Traffic Operations Will Not Be Available for Years

FAA plans to introduce several capabilities through NextGen that are designed to improve critical communications, surveillance, and the distribution of flight data. Since contingency plans that require the transfer of airspace responsibility are difficult to sustain for extended periods of time, the implementation of NextGen technologies may enable FAA to improve the continuity of air traffic operations during emergency events. Table 3 describes some of these NextGen technologies, including their implementation progress and challenges, as well as estimated costs and timeframes. Many of these capabilities will not be available for years, and the overall cost and timeframe for implementing them is uncertain.

[25] The top 30 United States airports in terms of passenger activity.

Table 3. Planned NextGen Technologies Intended To Improve Continuity of Air Traffic Operations

NextGen Technology	Description of Expected Benefits	Progress and Challenges	Estimated Costs and Timeframes
Communication			
NAS Voice Switch (NVS) Technology	• Standardize air traffic facilities' voice communication infrastructure. • Replace existing voice switching and radio control equipment with a Voice over Internet Protocol.[26] • Allow controllers to be able to talk with pilots flying anywhere in the NAS. • Allow facilities to easily alter and add frequencies during contingencies.	• Initial operational testing of NVS is scheduled to be completed by September 2019. • Will require FAA to train thousands of air traffic and technical operations personnel. • Will be challenging for FAA to operate and maintain the existing and NVS systems concurrently until full implementation.	While FAA has estimated some costs, Agency officials state that they will not approve cost and schedule information until 2017, at the earliest.
Flight Plan Filing, Distribution, and Processing			
Expanding use of the System Wide Information Management (SWIM)	• Improve flight data services.	• In fiscal year 2015, FAA expects to add traffic flow and aircraft spacing information. • Some elements of SWIM are operational, and future capabilities are being considered.	The total cost and completion date of this modernization effort is unknown.
Flight and Inter-facility ATC Data Interface Modernization (FIADIM)	• Reduce the probability of flight data outages between facilities by utilizing a flexible internet protocol network.	• If funding is approved, FAA plans to develop alternatives for flight data modernization with various FAA automation systems.	FAA has requested $9 million in Facilities and Equipment funding for fiscal year 2016.
Radar Surveillance			
Surveillance Interface Modernization (SIM) tool	• Improve radar resiliency and flexibility by transitioning to a private internet protocol. • Allow more robust routing of radar data to multiple locations.	• FAA has not determined whether it will proceed with implementing the program.	FAA has not determined how much this effort will cost or when it could be available.

Source: OIG analysis

[26] Voice over Internet Protocol (VoIP) is a technology that converts voice communications into a digital signal that travels over the Internet.

In the short term, FAA stated that it will conduct a comprehensive evaluation of how planned NextGen capabilities can enhance the resiliency, contingency, and continuity of NAS operations for all air traffic services. According to FAA's 30-Day Assessment of Operational Contingency Plans dated November 2014, the review will be completed within 12 months.

FAA FACILITY SECURITY PROTOCOLS WERE INSUFFICIENT TO MITIGATE POTENTIAL RISKS TO THE U.S. AIR TRAFFIC CONTROL SYSTEM

Security systems in effect prior to the incident were insufficient to identify, counter, or mitigate the impact of a contract employee's intent on sabotaging the air traffic control system. FAA recently completed a 30-day security review that identified needed enhancements. Although FAA's Office of Security and Hazardous Materials Safety (ASH) has developed implementation plans and funding recommendations, these are dependent on sustained management attention and acquisition of sufficient funding.

FAA Security Protocols Lacked Sufficient Controls To Limit Facility Access

Prior to the Chicago Center sabotage, the primary focus of FAA security policies was the prevention and mitigation of external threats. FAA relies on multiple layers of security, including risk assessments, security officers, and employee and contractor vetting and access controls. In addition, FAA policy[27] requires facilities to complete a comprehensive security inspection based on the facilities' security level, accreditation, and local risk factors, such as crime. The onsite inspection is designed to monitor overall facility compliance with required baseline protective measures identified during previous assessments or inspections. Comprehensive inspections can also serve to evaluate the significance of changes in a facility that could require additional protective measures or another complete facility security assessment.

Chicago Center was required to complete a comprehensive security inspection on a 12- to 18-month cycle. Although Chicago Center received supplemental security inspections between 2012 and 2014, a comprehensive security inspection of Chicago Center was not completed in August 2013, as required. In October 2014, after the fire, a comprehensive facility security inspection of Chicago Center was completed. Although the inspection did not find significant deficiencies, FAA security officials are aware of the lapse and are updating internal policies to ensure future compliance.

FAA's security protocols in effect prior to the incident lacked the controls necessary to block facility access to current or former employees. For example, at the time of

[27] FAA Order 1600.69B, FAA Facility Security Management Program, Effective March 29, 2005.

the incident, there was no requirement to deactivate an employee’s Personal Identity Verification (PIV) card or to limit facility access to employees scheduled to transfer to another FAA facility. The contract employee responsible for the fire worked at Chicago Center for about 7 years, held a security clearance, and had a FAA PIV card. Although the employee’s last scheduled shift was on September 18, 2014, he still had full access to Chicago Center on September 26, 2014 (the day of the sabotage), including the main facility building and the FTI equipment room. As a result of the security review conducted after the fire, FAA has begun modifying its policies and procedures to reduce the risk of future occurrences.

FAA’s Security Analysis Identified Needed Enhancements That Will Take Several Years and Require Significant Investment

Following the Chicago Center incident, FAA’s ASH completed a comprehensive security analysis as directed by the FAA Administrator. The analysis examined current and future risks to FAA personnel, facilities, equipment, systems and operations, as well as lessons learned from the 2013 Navy Yard shooting incident. FAA’s review concluded that the security protocols in effect on September 26, 2014, were insufficient to identify, counter, or mitigate the impact of an insider threat.

The analysis yielded 42 recommendations, 24 of which are considered significant to the improvement of facility security. Although the specific findings constitute Sensitive Security Information,[28] the review found that modifications to risk assessment, access control, personnel screening policies and processes, and training enhancements are needed to strengthen FAA security against both external and internal threats to the Agency. FAA publicly reported that it plans to:

- Adjust and refine the Agency’s risk assessment approach for both facility and personnel security, from the outer perimeter to the equipment rooms for critical NAS facilities.

- Identify potential opportunities to accelerate technology upgrades and deployment to expand advanced access control capabilities.

- Refresh and/or develop new training for managers and employees that details security responsibilities, identifies indicators of potential insider threats, and instructs the workforce on how to respond to the threats.

[28] Sensitive Security Information (SSI) is controlled under 49 CFR parts 15 and 1520. SSI may not be disclosed to persons without a "need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation.

- Complete security reevaluation of 77 Tier-1[29] facilities. This includes adjustments to personnel and vehicle screening, and acceleration of installation of a PIV compliant physical access control system.

FAA concluded that implementation of these security recommendations is dependent primarily on additional funding and staffing resources. The fiscal year 2016 President's Budget Request designated ASH as a separate line of business for the first time. ASH requested initial funding of $11.3 million to begin improvements in facility and personnel security (see table 4).

Table 4. Security Initiatives in the Fiscal Year 2016 President's Budget Request

Program	Budget Request	Full Time Equivalents (FTE)
Implement facility and personnel security recommendations for critical operational facilities identified in the Chicago Center security review.	$8.8 million	18
Install and manage an Agency-wide Emergency Notification System (ENS). The system will be used to transmit emergency messages nationwide.	$1.5 million	1
Form the Insider Threat Detection and Mitigation Program (ITDMP) and Defensive Counterintelligence Program (DCIP) to establish capabilities to protect FAA from insider activity, foreign intelligence, and cyber-espionage.	$1.0 million	2
Total	**$11.3 million**	**21**

Source: FY 2016 President's Budget Request

To implement the remaining recommendations, ASH has identified additional funding needs for fiscal year 2017. However, to continue to improve facility security, FAA will have to determine and request future budget and staffing levels.

CONCLUSION

Our national aviation system is vitally important to the economic health and security of our country. The Chicago incident highlighted the need for enhancing security and increasing the flexibility and resiliency of the national air traffic control system. Although our review focused on Chicago Center, we believe that these infrastructure limitations would be similar at many of FAA's 21 Centers. To minimize future risks and disruption to the NAS, FAA must develop robust new contingency plans and security policies and procedures based on the lessons learned from the Chicago Center FTI fire. It will also be critical to define resource requirements and follow through on its recommendations from its 30-day reviews. Until then, FAA will remain vulnerable

[29] FAA has identified a total of 77 major air traffic facilities and airports based primarily on level of operations and number of passengers.

to significant security and safety issues should a similar systematic attack on the National Airspace System occur.

RECOMMENDATIONS

To help FAA improve redundancy and resiliency in the NAS and implement improvements to its operational contingency plans and security protocols, we recommend that the Agency:

1. Apply the lessons learned from the Chicago Center incident to the redesign of operational contingency plans for all Center facilities.
2. Identify and implement changes needed to improve annual contingency training exercises to simulate more realistic scenarios.
3. Evaluate the feasibility and cost of physically separating primary and backup components of critical communication infrastructure when comparing alternative implementation options for all future investments.
4. Install a secure wireless network that can provide access to FAA's local area network (LAN) and connectivity to the internet at Center facilities.
5. Assess the feasibility and cost of replacing the existing fire suppression systems in critical equipment areas with a waterless system at Center facilities.
6. Develop an implementation plan and quantify all costs required for the implementation of each recommendation in FAA's 30-day Review of Contingency Plans.
7. Develop an implementation plan and quantify all costs required for the implementation of the 42 recommendations derived from the Comprehensive Security Review.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided FAA with our draft report on August 18, 2015, and received its official response on September 11, 2015, which is included as an appendix to this report. FAA concurred with all seven of our recommendations and proposed appropriate actions and completion dates. Accordingly, we consider all recommendations as resolved but open pending completion of the planned actions.

We appreciate the courtesies and cooperation of FAA representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-0500 or Robert Romich, Program Director, at (202) 366-6478.

#

cc: DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted our work from October 2014 through August 2015 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.

At the request of six members of Congress from Illinois, we reviewed the operational contingency plans, and emergency and security protocols at Chicago air traffic control facilities. The audit included site visits to FAA Headquarters, and the Air Traffic Control System Command Center (ATCSCC). We visited or contacted the primary Chicago area air traffic control facilities: Chicago Air Route Traffic Control Center (ZAU), Chicago Terminal Radar Approach Control (C90), Chicago Midway Air Traffic Control Tower (MDW), and Chicago O'Hare Air Traffic Control Tower (ORD). In addition we interviewed officials from the Federal Bureau of Investigation (FBI), Harris Corporation, National Air Traffic Controllers Association (NATCA), and Professional Aviation Safety Specialists (PASS).

To assess whether FAA has developed and implemented a business continuity plan for the Chicago air traffic control facilities that provides for adequate levels of redundancy and resiliency, we reviewed facility operational contingency plans and interviewed FAA Headquarters and local air traffic facility officials[30]. We reviewed the plan requirements contained within the FAA Order on Contingency Planning (1900.47D). We thoroughly analyzed the timeline of the September 26, 2014 Chicago Center fire, including transferring control of airspace, lessons learned, and infrastructure limitations. Finally, we reviewed the Air Traffic Organization report on the 30-Day Assessment of Operational Contingency Plans and proposed improvements.

To evaluate whether the security measures in place at the Chicago facilities are currently maintained and sufficient to mitigate potential risks to the air traffic control system, we interviewed FAA Headquarters, air traffic facility officials, and security subject matter experts. We reviewed FAA Orders on Air Traffic Facility Security (1600.69B and 1900.1G) and annual facility security inspection reports. Finally, we reviewed FAA's 30-day security report and recommendations.

We coordinated internally with the OIG audit of the Security Controls over FAA's Large Terminal Radar Approach Control facilities.[31]

[30] The audit did not include a review of the redundancy and resiliency of FAA's Telecommunications Infrastructure (FTI) because it was outside of the audit scope.

[31] OIG Project No. 14F3012F000, August 7, 2014.

EXHIBIT B. ORGANIZATIONS VISITED OR CONTACTED

FAA Organizations

- Office of Security and Hazardous Materials Safety (ASH)
- Program Management Organization (PMO)
- Technical Operations
- Mission Support, Temporary Operational Contingency Office (TOCO)

FAA Air Traffic Control Facilities

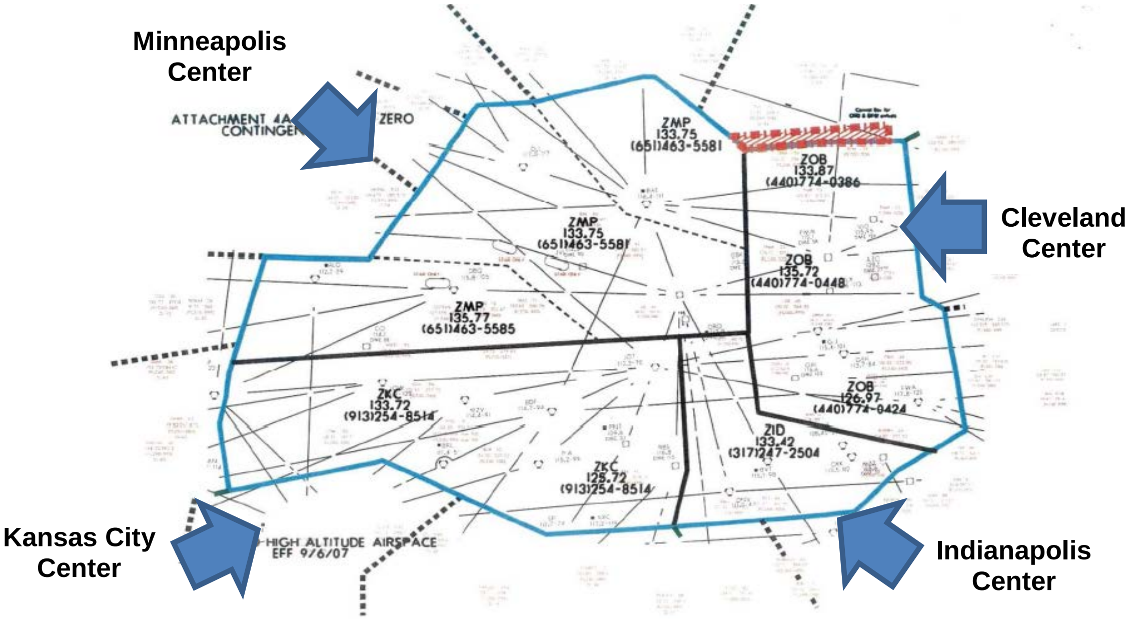
- Air Traffic Control System Command Center (ATCSCC)
- Chicago Air Route Traffic Control Center (ZAU)
- Chicago Midway Air Traffic Control Tower (MDW)
- Chicago O’Hare Air Traffic Control Tower (ORD)
- Chicago Terminal Radar Approach Control (C90)
- Washington Air Route Traffic Control Center (ZDC)

Industry, Associations, and other Federal Agencies

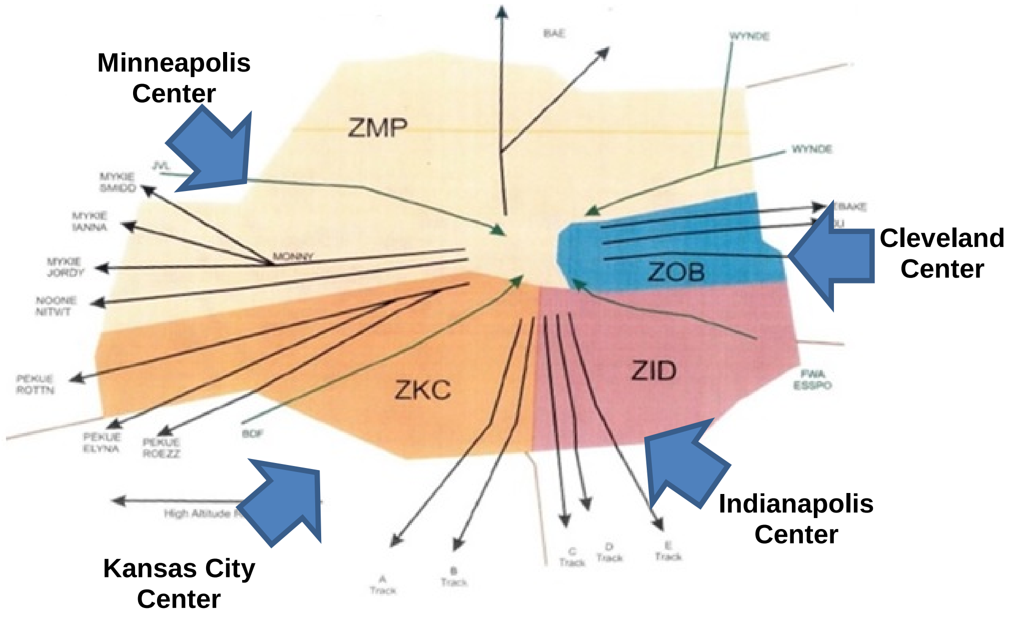
- Federal Bureau of Investigation (FBI)
- Harris Corporation
- National Air Traffic Controllers Association (NATCA)
- Professional Aviation Safety Specialists (PASS)

EXHIBIT C. 2008 CHICAGO CENTER'S CONTINGENCY PLAN AIRSPACE MAP COMPARED TO THE POST FIRE AIRSPACE MAP

2008 Chicago Center's Contingency Plan Airspace Map



Chicago Center's Post Fire Contingency Plan Airspace Map



Source: FAA

Exhibit C. 2008 Chicago Center's Contingency Plan Airspace Map

EXHIBIT D. MEMBERS OF CONGRESS REQUESTING THIS AUDIT

Given the high volume of air traffic in the Chicago airspace, six Members of Congress from Illinois requested that we review the emergency and security protocols at Chicago air traffic control (ATC) facilities. Specifically, they asked us to determine whether adequate protocols, emergency plans, and security measures are in place to prevent or mitigate the impact of such emergencies in the future.

The six Members of Congress include:

- **The Honorable Richard J. Durbin** (D-IL), U.S. Senate
- **The Honorable Bill Foster** (D-IL 11), U.S. House of Representatives
- **The Honorable Mike Quigley** (D-IL 5), U.S. House of Representatives
- **The Honorable Tammy Duckworth** (D-IL 8), U.S. House of Representatives
- **The Honorable Jan Schakowsky** (D-IL 9), U.S. House of Representatives
- **The Honorable Dan Lipinski** (D-IL 3), U.S. House of Representatives

EXHIBIT E. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Robert Romich	Program Director
Tasha Thomas	Project Manager
Kevin Montgomery	Senior Analyst
Andrew Olsen	Senior Auditor
Erik Phillips	Senior Analyst
Teklay Legese	Auditor
Audre Azuolas	Writer/Editor

Federal Aviation
Administration

Memorandum

Date: September 11, 2015

To: Matthew E. Hampton, Assistant Inspector General for Aviation Audits

From: H. Clayton Foushee, Director, Office of Audit and Evaluation, AAE-1

Subject: Federal Aviation Administration's (FAA) Response to Office of Inspector General (OIG) Draft Report: FAA's Contingency Plans and Security Protocols Were Insufficient at Chicago Air Traffic Control Facilities

On September 26, 2014, an unprecedented criminal act by an off-duty, contract employee resulted in the large-scale destruction of critical operating systems, forcing the Chicago Air Traffic Control Center (ARTCC) to declare "ATC Zero"[1] and to transfer control of Chicago-area airspace to other ARTCCs. The Chicago Center fire underscored how even highly redundant systems such as the National Airspace System (NAS) can be compromised when an individual with insider knowledge of critical systems is motivated and determined to maximize destruction. Despite the massive amount of system damage, the FAA was able to restore most air service to Chicago area airports within a relatively short period of time. In three days, more than 80 percent of the average traffic was restored at O'Hare, and more than 90 percent of the average traffic was back in operation at Midway.

While safety was not compromised, this incident exposed some weaknesses in FAA contingency planning, as well as characteristics of the current infrastructure design that precluded a more complete and timely recovery. Accordingly, the Agency has systematically evaluated its ability to minimize the "insider threat," analyzed aspects of the architecture where one or more points of attack have a high probability of significantly compromising air traffic operations, and identified the system capabilities necessary to isolate, respond, and restore operations quickly.

Immediately after the event, the Agency initiated a 30-day review of contingency plans to ensure that critical enhancements are implemented to improve air traffic control service delivery during irregular operations. The FAA established new efficiency and recovery targets for emergency operations, which will minimize the disruption of air traffic operations during unplanned, irregular, or emergency events. To achieve these new targets, the FAA is currently updating the Air Traffic Contingency Order, developing new contingency plans for ARTCCs, and assessing the effectiveness of all contingency plans. When these new protocols are

[1] ATC Zero (Air Traffic Control Zero) is an official term used by the FAA that means the FAA is unable to provide the published ATC services within the airspace managed by a specific facility.

completed in September 2015, the Agency will begin making the associated investments to critical infrastructure, including the prepositioning of additional equipment and the rerouting of communications circuits. These steps will increase redundancy, reduce recovery time, and make the system more resilient and less vulnerable to the type of attack that occurred in Chicago.

In addition, the FAA has proactively implemented a number of security enhancements against insider threats. The Agency has bolstered oversight of FAA facility security assessments, is increasing assessment frequency, increased access control restrictions, and improved capabilities for security officers to verify employees and contractors. The FAA has also increased monitoring of contractor company compliance with security requirements and instituted mandatory reviews of contract and contractor personnel changes.

The FAA agrees with all of OIG's seven recommendations, as written. Budget requests for additional resources required to support the implementation of all recommendations have been submitted. For recommendations 1, 2, 3, and 5, operational contingency plans and security protocols are already in progress and will be completed by April 29, 2016. With regard to recommendation 4, the FAA is currently deploying secure wireless networks at the 21 center (ATRCC) facilities. Four centers will be complete by September 2015, 8 will be completed by September 2016, and 9 will be completed by September 2017, pending approval of requested funding. Regarding recommendations 6 and 7, the Agency has already developed an implementation plan, quantified costs, and identified next-step activities to implement each of the security review recommendations. Pending approval of the budget requests, the Agency plans to complete action on these recommendations by September 30, 2016.

We appreciate this opportunity to offer additional perspective on the OIG draft report. Please contact H. Clayton Foushee at (202) 267-9000 if you have any questions or require additional information about these comments.