

## **Chicago Center Fire** *Contingency Planning and Security Review*

### **Background**

In the early morning hours of September 26, 2014, the Federal Aviation Administration's (FAA) Chicago Air Route Traffic Control Center (ARTCC) declared "ATC Zero" after an employee of the Harris Corporation deliberately set a fire in a critical area of the facility. The fire destroyed the Center's FAA Telecommunications Infrastructure (FTI) system – the telecommunications structure that enables communication between controllers and aircraft and the processing of flight plan data.

Chicago Center manages flights traveling through high altitude airspace over multiple states in the Midwest, covering 91,000 square miles. When the fire began, the FAA implemented its contingency plans to ensure that aircraft in the air landed safely and traffic could continue to move throughout the country. The Chicago Center transferred control of high altitude air traffic to neighboring en route centers in Minneapolis, Kansas City, Cleveland and Indianapolis so controllers in those facilities could direct traffic in and around the Chicago area.

FAA employees worked around the clock to establish new routes, procedures and communications channels to keep traffic flowing. Nearly 200 of Chicago Center's workers traveled to other FAA air traffic facilities during the outage to help provide local knowledge at locations that were handling Chicago Center traffic.

As a result of this unprecedented effort, Chicago's O'Hare and Midway Airports operated at near-normal levels. In fact, air traffic controllers at O'Hare Airport handled more flights than any other airport in the country on 11 days during the outage.

Over the course of 17 days, FAA technical teams worked 24 hours a day alongside the Harris Corporation to completely rebuild and replace the destroyed communications equipment. They restored, installed and tested more than 20 racks of equipment, 835 telecommunications circuits and more than 10 miles of cable.

The loss of Chicago Center had the potential to cause weeks of significant disruptions in the National Airspace System (NAS). Chicago is a unique nexus in our system – when delays occur there, they ripple across the entire country. Recognizing the potential impacts to the NAS, FAA Administrator Michael Huerta pledged to have the facility back up and running by Monday October 13, 2014. Thanks to the dedicated work of FAA employees and other critical partners that deadline was met.

The fire at Chicago Center and its after effects inconvenienced passengers, reportedly cost the airlines over \$350 million dollars and raised questions about the resiliency of our National Airspace System and its ability to withstand a similar systematic attack in the future.

## **Call for Review**

The air transportation system is vital to our economy and people rely on it to function safely and efficiently 24 hours a day, 7 days a week. The FAA's contingency planning focuses on the safe handling of aircraft. When a major outage or similar disruption occurs, the agency's goal is to manage the aircraft in the air to ensure they reach their destinations safely. Following the September fire, the FAA worked quickly to handle aircraft traversing Chicago Center's airspace and implemented its contingency plans to hand off airspace responsibilities to adjacent facilities. Still, the efficiency of the system the nation has come to depend on suffered.

The FAA must have the most robust contingency plans possible, with safety as the number one priority. But, given the importance of aviation to our country's economy, the plans should also include tools and actions to bring the system back online to as close to normal, as quickly possible.

Administrator Huerta called on the Air Traffic Organization (ATO) and the FAA's Office of Security and Hazardous Materials Safety (ASH) to conduct a 30-day review of our security and contingency plans, along with labor partners National Air Traffic Controllers Association (NATCA) and Professional Aviation Safety Specialists (PASS), and to develop action plans to mitigate future loss of major capabilities.

The security team was asked to focus its review on current and future risks to FAA personnel, facilities, equipment, systems and operations.

For the FAA operational contingency plans and requirements review, Administrator Huerta challenged the ATO team to examine plans with the target objective of maintaining the highest levels of safety and also achieving 90 percent of normal operations within 24 hours of a major event similar to the situation at Chicago Center.

## **Findings**

### **Contingency Planning**

The ATO review of the agency's air traffic contingency plans found that current plans do maintain a high level of safety during unlikely contingency operations. However, it did confirm that target levels of efficiency are not factored into the contingency plans in place for events similar to the Chicago Center incident.

The review also found that current infrastructure and air traffic management systems are robust, but have limited technical flexibility to support operational contingencies. Current infrastructure can be reconfigured to adapt in emergency situations, but the time it takes for this to occur is measured in days, when today's system demands that it be measured in hours. Once the infrastructure is reconfigured, operations can produce high levels efficiency, but the non-standard nature of the operation in terms of people, process and procedures, makes it very challenging to sustain for any significant period of time.

## **Security**

The FAA uses layers of security measures, including risk assessment, access controls, security officer operations, and employee and contractor vetting and suitability determinations, to protect our workforce, facilities, equipment, and the services provided to the flying public and aviation stakeholders.

The comprehensive security review included examination of current policies, processes, and operations in facility and personnel security across a broad spectrum of potential threats. The review found that mitigation of external threats has been the primary focus of the FAA security regime, but nascent efforts to detect and counter insider threats must be expanded and accelerated.

While many of the specific findings cannot be shared publicly, the review found that refinements in the risk assessment approach, adjustments in policies and processes, and enhancements in training and education in several areas across security layers will strengthen the FAA's overall security posture against both external and internal threats to the agency, its mission responsibilities, and its employees.

## **Action Plan**

### **Contingency Planning**

The FAA plans to immediately begin to revise its contingency strategy and policies to include the operational efficiency goal of achieving 90 percent of normal operations within 24 hours of a major outage.

The FAA will modify its current contingency strategy to introduce the potential for divestment of airspace to neighboring facilities through pre-planned airspace structures. FAA policies will be updated to provide standard operating procedures as well as guidance to local facilities for making such changes based upon an evolving understanding of the event. These plans will extend the reach of surrounding facilities into the affected airspace, without changing how they do operations today.

By changing the facility level plans in this way, the FAA expects to provide a solid foundation to its facility management structure for decision-making relative to: 1) maintaining airspace and personnel safety, 2) building back efficiency of National Airspace System operations over time, and 3) determining what, if any, infrastructure modifications must be undertaken to support the contingent operation while restoration activities are conducted.

Beyond the development of a new contingency strategy and airspace coverage plans, the FAA will begin engineering studies and subsequent implementation of airspace system modifications aimed at increasing both the speed of response, and the sustainability of the contingent operation. The FAA will achieve this by first introducing pre-planned and pre-configured options into its air traffic management systems infrastructure, and second, by increasing system technical flexibility

to support operations through the acceleration of NextGen technologies. These actions will be structured in a three- stage plan which can be executed only if resources are made available.

### **Stage 1: New Contingency Plans for Efficiency**

In response to the new facility contingency plans, the FAA will work with its telecomm and automation systems so that radars, voice radios, flight planning data, and weather and aeronautical information will be more rapidly available to support operations in the new configuration.

While these changes will significantly improve response to a large facility outage, they will still limit operational flexibility during a contingency, and are not sustainable beyond a few weeks. However, the goal of these actions will be that within 12 months, the FAA will reduce its response time to major facility outage from days to hours. This reduction in response time over present capabilities will benefit to the aviation community and the flying public by reducing exposure to significant economic loss.

### **Stage 2: Enhanced Contingency Plans**

The second stage of the FAA's plan will enhance these pre-planned actions, by reducing or eliminating the manual nature of operations during contingencies. This stage will provide more options for reconfiguring airspace, allow for the potential to deal with more than a single facility outage, provide faster response times to needed changes based on evolving understanding of airspace user needs, and significantly increase the sustainability of the new operating posture. This enhanced capability will be made through the recreation of the specific sectors and services of the off-line facility at surrounding facilities, thus allowing the more effective use of personnel in an operation that more closely resembles normal activities.

A number of system improvements and accelerations of planned technologies will increase the ability to sustain operations up to several months. Typical of the type of changes required is the automation of flight plan distribution and inter-facility hand-offs. Acceleration of the NAS Voice System and the expanded use of System Wide Information Management (SWIM) for internal NAS weather and flight data distribution will allow systems to be configured with the look and feel of any other facility. This, coupled with the ability to create new sectors at other en route centers, will allow for more robust sector management at the new facility. This capability, expected to be fully implemented by FY-18, will significantly increase the potential to restore a much wider range of sustained disruptions, while maintaining an extremely high operational efficiency rate. This level of improvement will further reduce the potential economic loss for airspace users.

### **Stage 3: Enhanced Continuity with NextGen Technologies**

This incident in Chicago is a stark reminder of the reasons the FAA is working toward an even more robust and scalable system. In the long term, NextGen capabilities represent the most efficient and cost effective way to create resiliency for both contingency and continuity of

operations in the NAS. NextGen capabilities will build on the enhancements planned for Stages 1 and 2, providing airspace flexibility by reducing the facility-dependent information flows.

The FAA is examining how to best utilize NextGen capabilities to meet resiliency, contingency, and continuity needs so that services could be made available quickly if capabilities are lost. By leveraging the completed rollout of ADS-B and the impending rollout of the NAS voice system, data communications with aircraft, and enhanced information integration into decision support tools, the FAA could rapidly recreate capabilities and reduce the impact of unplanned outages should a critical facility lose function.

### **Security**

Each facility has unique characteristics and plays different roles in the system depending on its function and location. Based on several security review findings, FAA will adjust and refine the agency's risk assessment approach for both facility and personnel security to ensure the unique capabilities, services, and locations are appropriately weighed in selecting specific security measures from the outer perimeter to the innermost equipment rooms for critical NAS facilities. These factors must also be included in determining the security requirements for personnel working in sensitive positions in those facilities, in order to prevent disruption of FAA services by a security threat. The FAA has also identified potential opportunities to accelerate technology upgrades and deployment to expand advanced access control capabilities that will further enhance the overall security regime against external and internal threats. Many of these actions can be executed only if resources become available.

Modifications in some access control, personnel screening, and contract requirement policies and processes will also yield improvements across multiple layers of facility and personnel security. Last but not least, refreshing and/or developing new training for managers and employees that details security responsibilities, identifies indicators of potential insider threats, and instructs the workforce on how to report and respond to security threats, such as active shooter incidents, is critical to ensure policies and procedures are understood and executed appropriately and consistently at all FAA facilities, thus enhancing security across the whole enterprise.

### **Conclusion**

This incident in Chicago underscores the need for the FAA to have the most robust and flexible system possible. The aviation system is vitally important to the economic health and security of our country. We need to be certain we can keep it running as safely and efficiently as possible even in the face of unforeseen events. In the future, the agency's ability to agilely shift air traffic management responsibilities between facilities is a key objective that will be achieved through the implementation of NextGen.