GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 31, 2007

The Honorable John Conyers, Jr.
Chairman
Committee on the Judiciary
House of Representatives

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable John L. Mica
Ranking Republican Member
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Jerry F. Costello
Chairman
The Honorable Thomas E. Petri
Ranking Member
Subcommittee on Aviation
Committee on Transportation and Infrastructure
House of Representatives

The Honorable F. James Sensenbrenner, Jr.
House of Representatives

Subject: *Aviation Security: Federal Coordination for Responding to In-flight Security Threats Has Matured, but Procedures Can Be Strengthened*

Five years after the terrorist attacks of September 11, 2001, concerns continue to be raised about the nation's system for protecting commercial aviation. Past disclosures of terrorists' plans for smuggling liquids onboard aircraft to construct a bomb in flight highlighted the continued need to examine this key aspect of homeland security. One layer of the aviation security system involves the ability of the federal government to respond to actual or potential security threats while a commercial aircraft is in flight. These security threats can include the following:

- Passengers considered to be security risks to aviation are found to be onboard flights bound for or leaving the United States.
- Situations develop while the aircraft is in flight—for example, a passenger becomes disruptive or acts suspiciously, a bomb threat is received, or an unidentified package is found onboard the aircraft.

- A commercial aircraft transmits a signal designed to alert authorities that a hijacking is in process.[1]

Procedures for addressing these in-flight security threats involve a wide range of federal agencies and entities. The Department of Homeland Security (DHS) is responsible for taking much of the lead in responding to these incidents, and the Transportation Security Administration (TSA) was established to ensure the security of all modes of transportation—including aviation.[2] Responding to an in-flight threat, however, involves many agencies beyond DHS and TSA. Depending on the nature of the threat, managing and responding to in-flight threats can involve extensive coordination among more than 15 federal agencies and agency components, each with its own set of responsibilities that may influence the threat response. For example, another DHS component, Customs and Border Protection's (CBP) National Targeting Center (NTC), is responsible for comparing names and other identifying information of passengers onboard commercial aircraft flying to or from the United States with terrorist watch lists of persons considered to be potential security risks. If a passenger is determined to match an identity listed on a terrorist watch list, the Federal Bureau of Investigation (FBI), a Department of Justice (DOJ) agency, is often involved in conducting a risk assessment of the threat posed by that passenger while the flight is en route. Further, the Department of Transportation's (DOT) Federal Aviation Administration (FAA) becomes involved with in-flight threats as it monitors aircraft traffic entering into and operating within U.S. airspace to ensure safe operations, while the Department of Defense's (DOD) North American Aerospace Defense Command (NORAD)—a bi-national command established by agreement between the governments of the United States and Canada—becomes involved with the situation as it ensures the air sovereignty and air defense of U.S. airspace. Since these security incidents involve aircraft that are already in flight, timely and effective coordination among these agencies and components is paramount.

You asked that we examine in-flight security threats and current federal efforts to respond collaboratively to them. In response, on February 28, 2007, we issued a classified report addressing the following questions: (1) What were the number and types of in-flight security incidents that occurred onboard commercial aircraft during 2005 that were reported to TSA, and to what extent did these threats result in aircraft being diverted? (2) What is the process that federal agencies follow to identify, assess, and respond to in-flight security threats? (3) To what extent did interagency coordination problems occur during 2005, if at all, and what steps did the involved agencies take to address any identified problems?

As our February 2007 report contained information that was deemed to be either classified, sensitive security information, or law enforcement sensitive, this version of the report is intended to generally summarize our overall findings and recommendations while omitting sensitive information about the in-flight security threat resolution process, including specific agency roles and responsibilities and coordination challenges that have occurred and steps agencies have taken to address them. Our classified February 2007 report also summarized the events associated with security-related aircraft diversions that occurred in 2005, but

[1]Aircraft that violate restricted airspace may also pose a security threat. We previously reported on the interagency operations to manage aircraft incursions into restricted airspace. For more information, see GAO, *Homeland Security*: *Agency Resources Address Violations of Restricted Airspace, but Management Improvements Are Needed*, GAO-05-928T (Washington, D.C.: July 2005).

[2]TSA was originally created as an agency within the Department of Transportation (DOT). The Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, signed into law on November 25, 2002, transferred TSA from DOT to DHS.

those summaries included classified or sensitive information and therefore could not be included in this report. As our intent in preparing this report is to convey, in a publicly available format, the non-classified, non-sensitive results of the classified February 2007 report, we did not attempt to update the information here to reflect changes that may have occurred since the publication of the February 2007 report.

Although the information provided in this report is much more limited in scope, the overall methodology used for our initial report is relevant to this version of the report as well because the information contained here was derived from the initial classified report. To address the objectives of our initial report, we analyzed security incident reports from TSA dated January 1, 2005, through December 31, 2005. Because TSA is the primary agency responsible for aviation security and maintains records of aviation security incidents, the TSA incident reports were our primary source of security threat information. These TSA incident reports contain descriptions of in-flight threat incidents that were reported to TSA and include information on the threat type and whether or not the aircraft was diverted. To understand the in-flight security threat resolution process, the extent to which interagency coordination problems occurred, and the steps agencies have taken to strengthen interagency coordination, we met with representatives from key offices within DHS, DOT, DOD, and DOJ who have responsibility for in-flight security threat resolution.[3] We also analyzed documentation—including agency aviation security incident reports—from these agencies to supplement information obtained from TSA security incident reports. In addition, we met with representatives of two domestic and five foreign air carriers—including some air carriers that have been involved in aircraft diversions—to discuss air carrier and government responsibilities pertaining to in-flight security threats. We also interviewed officials from three domestic and two international air carrier associations that represent the interests of air carriers and travelers to obtain their views on air carrier and government responsibilities pertaining to in-flight security threats. We conducted our work from April 2005 through November 2006 in accordance with generally accepted government auditing standards.

Results

Aviation Security Consists of Multiple Layers

The Aviation and Transportation Security Act, enacted in November 2001, created TSA as the agency responsible for securing all modes of transportation, including aviation.[4] Since then, TSA has worked with other stakeholders to develop a layered approach to ensure the security of commercial aviation, involving multiple diverse and coordinated measures. These measures include enhancing passenger and checked baggage screening, offering security training for flight and cabin crews to handle potential threats onboard aircraft, expanding the Federal Air Marshal Service (FAMS) to place more federal air marshals on domestic and international commercial flights, and training pilots on commercial passenger and cargo

[3]Specifically, within DHS we met with representatives and analyzed documents from TSA, including the Federal Air Marshal Service, the Office of Intelligence, and the Transportation Security Operations Center; Customs and Border Protection's National Targeting Center; and the Homeland Security Operations Center. Within DOT, we met with representatives and analyzed documents from FAA and the National Capital Region Coordination Center. Within DOJ, we met with representatives and analyzed documents from FBI, including the Terrorist Screening Operations Unit and the Terrorist Screening Center. Within DOD, we met with representatives and analyzed documents from NORAD and U.S. Northern Command. We also met with representatives from the National Counterterrorism Center.

[4]Pub. L. No. 107-71 (2001).

aircraft on how to use lethal force against an intruder on the flight deck through the Federal Flight Deck Officers (FFDO) Program.[5]

Many Agencies Are Involved in Resolving In-flight Security Threats

Consistent with its role as the lead federal agency responsible for aviation security, TSA established the Transportation Security Operations Center (TSOC), TSA's operational center for managing all types of transportation security incidents. To assist TSOC in performing its duties, in November 2004, TSA issued a security directive requiring all commercial air carriers flying to, from, or within the United States to report all in-flight security threats to TSOC so it can coordinate the federal response.[6] The security directive contains the criteria for which types of threats air carriers should report to TSOC, but according to TSA officials, the guidelines were purposefully left vague because TSA preferred that air carriers report too many incidents rather than too few. For example, the security directive states that air carriers should report all incidents and suspicious activity that could affect the security of U.S. civil aviation. Prior to the issuance of this security directive, air carriers were not required to report potential in-flight security threats to TSA. As a result, TSA and other federal agencies did not always have the information they needed to appropriately respond to security incidents.

Although TSA was created and vested with authority to secure the nation's aviation system, this effort requires a significant degree of interagency collaboration and coordination because it involves many different aspects of homeland security, aviation operations, and law enforcement—everything from examining thousands of passenger lists for inbound and outbound international flights to ensure that suspected terrorists are not boarding aircraft, to diverting flights to alternative airports—and, if needed, mobilizing military fighter jets to intercept threatening aircraft. Four main departments are involved in this interagency effort: Homeland Security, Justice, Transportation, and Defense. Additionally, the National Counterterrorism Center (NCTC), a component of the new Office of the Director of National Intelligence, may also be involved. The nature and extent of each agency's involvement depends on the type and nature of the threat. The specific roles and responsibilities of each agency involved in the resolution of in-flight security threats is considered law enforcement sensitive and thus could not be included in this report.

[5]Administered by TSA, the FFDO Program deputizes volunteer pilots of commercial passenger aircraft as armed federal law enforcement officers for the purpose of defending the flight deck "against acts of criminal violence or air piracy." Since the program was officially established on February 25, 2003, TSA has deputized thousands of eligible flight crew members as FFDOs.

[6]Security Directive 1544-04-15, "Incidents and Suspicious Activity Reporting," became effective on December 8, 2004, and applies to all air carriers that are required to adopt and carry out a security program regulated under CFR Part 1544, and that operate flights to, from, or within the United States. A security directive is used by an agency to notify aircraft and airport operators or field staff of a specific security concern where additional security measures are necessary to respond to a threat assessment or a specific threat against the United States. The security directive will require the entity that receives it to carry out certain measures. If these certain measures cannot be carried out, the entity that receives the security directive must have alternative measures approved.

Agencies Use Interagency Communication Tools to Coordinate during In-flight Security Threats

One communications tool that agencies use to gather and disseminate information for all types of in-flight security threats is the Domestic Events Network, an around-the-clock unclassified teleconference with controlled access administered by FAA and monitored by approximately 60 users from a variety of federal agencies as well as state and local entities.[7] This network was originally established as a conference call on the morning of September 11, 2001, to coordinate the federal response to the hijacked aircraft and has remained in existence since then as an open telecommunication line that serves as a basis for interagency communication. Any Domestic Events Network user can broadcast information, allowing other agencies on the network to communicate and monitor a situation in real time. Another important interagency communications tool is the Defense Red Switch Network, which is a secure, classified network administered by DOD. However, some officials involved in the interagency resolution of in-flight security threats may not have the appropriate clearances to participate in the Defense Red Switch Network discussions. As a result, decisions reached via discussions over the Defense Red Switch Network are typically broadcast over the unclassified Domestic Events Network so officials without access to the classified network can stay informed.

Relatively Few In-flight Incidents Were Reported during 2005, with a Small Percentage Resulting in Aircraft Diversions

Federal agencies and air carriers reported relatively few in-flight security threat incidents to TSA during calendar year 2005 as compared with the number of flights that occurred.[8] In-flight security threats include a wide range of incidents, but all are considered to threaten the security and safety of an aircraft and occur between the times the aircraft departs and lands. Approximately two-thirds of these reported incidents involved disruptive passengers such as passengers who were intoxicated, unruly, or trying to smoke in a lavatory. The remaining one-third of reported incidents included, for example, situations in which passengers that the U.S. government had previously identified as representing a security risk were identified onboard international flights traveling to or from the United States,[9] suspicious passenger behavior, or an aircraft accidentally transmitting a signal that a hijack was in process. In calendar year 2005, a relatively small percentage of all reported in-flight security threats were deemed serious enough to initiate the diversion of the aircraft from its original destination.[10]

---

[7]Events broadcast over the Domestic Events Network may include incidents that occur in an airport terminal as well as situations that arise onboard an aircraft.

[8]The specific number of in-flight security threats is considered law enforcement sensitive and therefore could not be included in this report.

[9]The specific number of passengers previously identified as representing a security risk, as well as the process that is used to identify these passengers, is considered law enforcement sensitive and therefore could not be included in this report.

[10]The specific number of aircraft diversions that occurred in 2005 and a detailed discussion of each diversion are considered law enforcement sensitive and therefore could not be included in this report. For purposes of this review, the phrase "initiate a diversion" refers to the security decision that an aircraft should be diverted because of an in-flight security threat. We are not referring to the operational implementation of the diversion, such as directing the aircraft to a specific location.

Process for Resolving In-flight Security Threats Requires Extensive Agency Coordination and Typically Involves Four Main Stages

The process that federal agencies follow to identify, assess, and respond to in-flight security threats generally involves multiple federal agencies and other entities (such as air carriers), each having specific roles and responsibilities that vary according to the facts and circumstances of the threat. TSA is responsible for coordinating the overall interagency process for resolving in-flight security threats but does not control the actions of other agencies; rather, each agency has its own mission, responsibilities, and procedures. For example, NORAD uses its own procedures for deciding how to respond to an in-flight security threat (such as launching military jets to intercept a flight). The coordination process that agencies use to resolve reported threats has never been systematically or comprehensively documented. Using interviews and agency documents, we developed a four-stage framework for describing the typical interagency process for resolving in-flight security threats. The four process stages are (1) identifying the threat and notifying affected agencies; (2) sharing pertinent information and collaboratively assessing the severity of the threat; (3) deciding on and carrying out the appropriate in-flight response, such as initiating a diversion; and (4) if necessary, completing the law enforcement response when the flight has landed.

Federal agencies have options for responding to an in-flight security threat incident such as (1) ordering the aircraft to divert by either denying it access to U.S. airspace or requiring it to land at a U.S. airport that is different from its intended destination,[11] and (2) launching military fighter jets to monitor or intercept the aircraft. In general, TSA is the federal agency responsible for deciding if an aircraft should be diverted because of an in-flight security threat, and FAA is responsible for managing the operational aspects of the diversion.[12] The specific process agencies typically follow to make these determinations is considered sensitive security information and therefore could not be included in this report, but in general, TSA, the pilot in command,[13] or FAA may initiate a diversion if it is considered the most appropriate response to the security threat, based on the unique facts and circumstances of each incident and the judgment of the individuals involved.

Agencies Experienced Relatively Few Coordination Problems in Resolving In-flight Security Threats and Took Steps to Address Them, but Opportunities Exist to Further Strengthen Coordination

Agencies have taken steps to enhance the interagency coordination process for resolving in-flight security threats. Although we identified a few coordination problems during 2005, none resulted in serious consequences such as a hijacking. Problems included misunderstandings of other agencies' roles and responsibilities and untimely information sharing—due in part to

[11]For purposes of this report, we are defining an aircraft diversion as the redirecting of a commercial aircraft to a location other than its intended destination because of an in-flight security threat involving that specific aircraft. We are not including flight cancellations, aircraft that are required to change their flight path but land at their intended destination, or ground-based security incidents, such as an airport closure, that result in an aircraft being redirected to an alternative airport.

[12]Once a diversion is initiated, FAA and its air traffic controllers are responsible for any operational aspect of the diversion within U.S. airspace. For example, FAA is responsible for providing information and assistance to both TSA and the pilot to ensure that an aircraft is diverted safely.

[13]The pilot in command is the pilot responsible for the operation and safety of an aircraft during flight.

a lack of clear policies and procedures. Agencies took some steps to address identified problems and proactively worked to strengthen coordination. Nevertheless, we identified three concerns with the current process for resolving in-flight security threats:

- Agencies lack a comprehensive document describing each agency's roles and responsibilities for responding to in-flight security threats and the information to be shared among agencies**.** Without such a document, interagency communication and information sharing can be hindered, potentially leading to confusion and a slower response. Since the response to in-flight security threats is inherently an interagency effort, having established policies and procedures to guide this information exchange and resulting actions is important. Agency officials involved in the resolution of in-flight threats generally agreed that a concept of operations plan or similar document would help strengthen the interagency threat resolution process.

- Procedures guiding the interagency coordination process are not uniformly established or shared. Some agencies lack established procedures, and some do not routinely share them, even though agencies agreed this could improve interagency coordination. In previous work, we found that a lack of clearly established policies and procedures for sharing information among agencies can hinder interagency coordination efforts.[14] Two key federal entities involved in the interagency resolution of in-flight security threats—FAA and TSOC, TSA's operational center for managing all types of transportation security incidents—have not finalized internal standard operating procedures outlining roles, responsibilities, and interactions with partner agencies. Agency officials from FAA and TSOC stated that their procedures would be finalized, but did not specify a date for when this would occur. In addition, agencies have also not routinely shared their procedures with other agencies that they regularly coordinate with to resolve in-flight threats, even though doing so could improve interagency coordination. For example, as of October 2006, FAA had not received standard operating procedures or other detailed procedural documentation from NORAD or TSOC. According to agency officials, sharing these procedures could help ensure that each agency establishes compatible policies and procedures to enhance the safety of in-flight security threat resolution and strengthen overall interagency coordination.

- Some agencies have not documented and applied lessons learned from interagency exercises. FAA and TSA conduct interagency exercises to enhance coordination for responding to in-flight threat scenarios, but no mechanism exists for documenting the exercise results. As a result, officials did not systematically document or distribute the results of the exercises or identify any follow-up action items. TSA officials stated that they believed it was clear during the exercises who was responsible for follow-up activities, if any were needed. However, by not systematically producing after-action reports, agencies are unlikely to realize all of the benefits that participating in interagency exercises can provide. We have found that after-action reports provide accountability and wider dissemination of information because they identify problems or issues and can be used to track the progress of corrective action.[15]

---

[14]See GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

[15]With regard to monitoring and evaluation efforts, we reported in January 2005 that U.S. Coast Guard units we studied were limited in their ability to benefit from port security exercises because after-action reports did not accurately capture all exercise results and lessons learned. GAO, *Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention*, GAO-05-170 (Washington, D.C.: Jan. 14, 2005).

Conclusions and Recommendations for Executive Action

As the post-September 11 interagency threat resolution process matures, it is important for agencies to develop mechanisms and procedures that enable effective and efficient coordination. Such steps are necessary, for example, to ensure that even when key individuals are absent, others will know how to respond. To strengthen the interagency coordination process for resolving in-flight security threats, we recommended in our February 2007 report that the Secretaries of Homeland Security, Transportation, and Defense, and the Attorney General, take the following two actions:

- develop a concept of operations plan or similar interagency document that outlines the general interagency coordination strategy and clearly delineates lines of communication among all agencies and entities involved in resolving in-flight security threats and

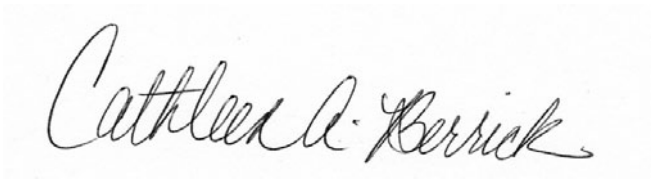
- ensure that each agency involved in the resolution of in-flight security threats has documented internal standard operating procedures that clearly identify agency procedures for resolving in-flight security incidents, and establish mechanisms for sharing these standard operating procedures with other agencies as appropriate.

We also recommended that the Secretaries of Homeland Security and Transportation direct the Administrators of TSA and FAA, respectively, to enhance the effectiveness of interagency exercises involving in-flight security threats by fully documenting and disseminating the results to all participants and ensuring that any follow-up action items are addressed as appropriate.

DHS and DOD agreed with the recommendations.[16] DOT and DOJ did not comment on them.

[16]Agency comments on the recommendations are considered sensitive security information and therefore could not be included in this report.

We will send copies of this report to the Secretary of the Department of Homeland Security; the Secretary of the Department of Transportation; the Secretary of the Department of Defense; the Attorney General; and interested congressional committees. We will also make this report available at no charge on GAO's Web site at http://www.gao.gov. If you or your staff have any questions about this report, please contact me at (202) 512-3404 or berrickc@gao.gov. Other key contributors to this report were Dawn Hoff, Assistant Director; Lisa Canini; Rudy Chatlos; Adam Hoffman; David Hooper; James Madar; Denise McCabe; Leslie Sarapu; Kathryn Smith; and Stan Stenersen.



Cathleen A. Berrick
Director, Homeland Security and Justice

(440616)

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548