Journal of Air Law and Commerce

Volume 82 | Issue 3 Article 4

2017

The Enemy Among Us: The Insider Threat

Valerie J. Pelton
vjpelton@yahoo.com

THE ENEMY AMONG US: THE INSIDER THREAT

VALERIE J. PELTON*

TABLE OF CONTENTS

* Valerie J. Pelton is an attorney, mediator, and former U.S. Air Force officer who has represented both domestic and international technology, telecommunications, and aerospace companies. She currently represents the U.S. Postal Service and is admitted to practice in Virginia, New Jersey, California, and the District of Columbia. Ms. Pelton was awarded an L.L.M. with Highest Honors in National Security & U.S. Foreign Relations Law from The George Washington University Law School, a J.D. from Whittier College, and a dual baccalaureate in Modern European Studies and French from Vanderbilt University.

EXECUTIVE SUMMARY

GIVEN ITS ROLE IN promoting and regulating civil and military aviation, the Federal Aviation Administration (FAA) is one of the most visible federal agencies to the general public. To fulfill its domestic and international aviation roles, the FAA must strike a balance between security and commercial interests and its own budget constraints. It is also an economic and intelligence target. While aviation security policy has evolved since 2001, policies designed to promote commerce and to facilitate overseas operations and maintenance by U.S. carriers and aerospace manufacturers have resulted in two entities that are especially vulnerable to insider activities: foreign repair stations and aircraft trusts.

In particular, foreign repair stations and aircraft trusts pose tempting targets for criminal and terrorist activities (and activities of foreign government agents) because they present unique opportunities for exploitation and disruption by ill-intentioned insiders (e.g., terrorists, criminals, moles, foreign government agents, coerced accomplices, unwitting dupes, disgruntled employees/contractors). These entities are also vulnerable to actions of altruistic insiders (e.g., employees and contractors), however well-meaning. A tapestry of executive orders, presidential directives, regulations, and statutes creates the fabric of the FAA's guidance and response to the insider threat posed by state and non-state actors.

While the vulnerabilities of repair stations and trust arrangements differ widely, the common element is the role of individuals who have access by virtue of their jobs. While insiders may act for altruistic or nefarious reasons, regardless of whether they are state or non-state actors, there are effective measures which can be taken to counter the insider threat and improve security.

I. INTRODUCTION

In the wake of revelations about the intelligence community by Pfc. Bradley Manning[1] in *WikiLeaks*,[2] and prior to leaks by Edward Snowden[3] to *The Guardian*,[4] the federal government was in the process of implementing insider threat programs. Implementation was on an agency-by-agency basis in response to Executive Order 13587 regarding Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (EO 13587).[5]

While these well-publicized cases of insider information leaks may have far-reaching adverse consequences for U.S. domestic and international intelligence collection programs which are dependent on information technology (IT), insider activities are not limited to compromise, disclosure, or destruction of IT. Foreign repair stations and aviation trusts are also susceptible to operations, communications, and technical security threats

---

[1] Bradley Manning is a U.S. Army soldier who was convicted in July 2013 of violations of the Espionage Act and other offenses including copying and disseminating classified military field reports, State Department cables and Guantanamo detainee assessments after publicly disclosing the largest volume of restricted documents in U.S. history in WikiLeaks. See Julie Tate, *Bradley Manning Sentenced to 35 Years in WikiLeaks Case*, WASH. POST (Aug. 21, 2013), http://articles.washingtonpost.com/2013-08-21/world/41431547_1_bradley-manning-david-coombs-pretrial-confinement [https://perma.cc/SP9S-6NUN].

[2] *WikiLeaks* is "an international, online, non-profit organisation which publishes secret information, news leaks, and classified media from anonymous sources." *See WikiLeaks*, WIKIPEDIA, http://en.wikipedia.org/wiki/WikiLeaks [https://perma.cc/JZ9L-5DJC] (last visited Sept. 1, 2017).

[3] Edward Snowden is a former U.S. National Security Agency contractor formerly employed by Booz Allen Hamilton who admitted he revealed information concerning classified surveillance programs to media outlets including *The Guardian* newspaper. *See* Tabassum Zakaria & Mark Hosenball, *Edward Snowden Charged with Espionage Over NSA Leaks*, HUFFINGTON POST (June 21, 2013), http://www.huffingtonpost.com/2013/06/21/edward-snowden-charged_n_3480984.html [https://perma.cc/2MNU-BUWN].

[4] *The Guardian* is a British newspaper that published the June 9, 2013, interview in which Edward Snowden identified himself as the source of unauthorized information leaks regarding U.S. national security surveillance programs. *See* Ewen MacAskill, *Edward Snowden, NSA Files Source: 'If They Want to Get You, In Time They Will'*, THE GUARDIAN (Jun. 9, 2013), https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why [https://perma.cc/5LZK-RFB2]. *See also* Peter Finn & Sari Horowitz, *U.S. Charges Snowden with Espionage*, WASH. POST (June 21, 2013), http://articles.washingtonpost.com/2013-06-21/world/40116763_1_hong-kong-nsa-justice-department [https://perma.cc/MU7M-C9WN].

[5] Exec. Order No. 13,587, 76 Fed. Reg. 63,811 (Oct. 13, 2011) [hereinafter EO 135871], http://www.gpo.gov/fdsys/pkg/FR-2011-10-13/pdf/2011-26729.pdf [https://perma.cc/E4AG-MAAQ].

posed by insiders. Because of the nature of flight maintenance operations and aircraft registry practices, foreign repair stations and aviation trusts are vulnerable to exploitation, manipulation, and disruption by insiders. Foreign repair stations and aviation trusts are potential targets of security and economic disruption. The nature of foreign repair stations and aviation trusts creates opportunities for physical intrusion, economic disruption, and deception by determined inside actors with the means, motive, skills, and access to exploit them.

Although the FAA has the difficult task of ensuring aviation safety and promoting commerce, it shares responsibility for security with other agencies. Pursuant to 49 U.S.C. § 40101,[6] the FAA is responsible for, among other things,

> (1) assigning, maintaining, and enhancing safety and security as the highest priorities in air commerce[;] (2) regulating air commerce in a way that best promotes safety and fulfills national defense requirements[;] (3) encouraging and developing civil aeronautics, including new aviation technology[;] (4) controlling the use of the navigable airspace and regulating civil and military operations in that airspace in the interest of the safety and efficiency of both of those operations[;] (5) consolidating research and development for air navigation facilities and the installation and operation of those facilities[;] (6) developing and operating a common system of air traffic control and navigation for military and civil aircraft[; and] (7) providing assistance to law enforcement agencies in the enforcement of laws related to regulation of controlled substances, to the extent consistent with aviation safety.[7]

In consultation with the Under Secretary for Border and Transportation Security[8] (BTS) of the Department of Homeland Security[9] (DHS), the FAA is charged with ensuring "the security of maintenance and repair work conducted on air carrier

---

[6] 49 U.S.C. § 40101 (2012).

[7] 49 U.S.C. § 40101(d).

[8] As a result of reorganization pursuant to DHS Secretary Michael Chertoff's Six-Point Agenda, the Directorate of Policy assumed policy coordination functions in July 2005 previously performed by BTS. *See Department Six-Point Agenda*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/department-six-point-agenda [https://perma.cc/MFX3-K3RF]. *See also Secretary Michael Chertoff U.S. Department of Homeland Security Second Stage Review Remarks*, U.S. DEP'T OF HOMELAND SEC. (July 13, 2005), http://www.tsa.gov/press/releases/2005/07/13/secretary-michael-chertoff-us-department-homeland-security-second-stage [https://perma.cc/V26M-33PW].

[9] 49 U.S.C. § 44924 (2012).

aircraft and components at foreign repair stations."[10] However, the FAA is solely responsible for establishing and implementing a

> safety assessment system for all [part 145][11] repair stations based on the type, scope, and complexity of work being performed . . . [which] (1) ensure[s] that repair stations located outside the United States are subject to appropriate inspections based on identified risks and consistent with existing United States requirements; (2) consider[s] inspection results and findings submitted by foreign civil aviation authorities operating under a maintenance safety or maintenance implementation agreement with the United States; and (3) require[s] all maintenance safety or maintenance implementation agreements to provide an opportunity for the [FAA] to conduct independent inspections of covered part 145 repair stations when safety concerns warrant such inspections.[12]

In addition to ensuring aviation safety and security, the FAA is also charged by Congress with promoting commerce. Certification of foreign repair stations used by U.S. carriers and manufacturers arguably impacts both aviation safety and commerce. In 2009, commercial aviation drove "$1.3 trillion in U.S. economic activity and, . . . [supported] more than 10 million U.S. jobs."[13] The "aviation sector is critical to our place in the global marketplace. It contribute[d] $75 billion to [the U.S.] trade balance and represent[ed] roughly [six] percent of the gross domestic product of the country."[14] In addition, "[c]ivilian aircraft engines, equipment and parts also contribute[d] $75 billion toward the U.S. trade balance [in 2009]. Civilian aircraft engines, equipment and parts have been the top net export for the past decade."[15] Aircraft trusts are instrumental in encouraging sales and facilitating registration of U.S.-made aircraft, engines, equipment, and parts. Pursuant to 14 C.F.R. § 47, trust structures also make it possible for foreign owners to maintain aircraft on the U.S. registry and to U.S. aviation maintenance, inspection, and safety standards.

---

[10] 49 U.S.C. § 44924(a).

[11] 14 C.F.R. § 145.205 (2016).

[12] 49 U.S.C. § 44733 (2012).

[13] FAA Modernization and Reform Act of 2012—Conference Report, 2012 WL 370418, 158 Cong. Rec. S333-02 (2012) at 3.

[14] *Id.*

[15] Fed. Aviation Admin., The Economic Impact of Civil Aviation on the U.S. Economy at 3 (2011).

II. BACKGROUND

When Congress enacted the Federal Aviation Act of 1958[16] (the 1958 Act) creating a Federal Aviation Agency (the Agency) with oversight and regulatory power to ensure aviation safety in the United States, it exercised its inherent powers under Article I, Section 8 of the Constitution to regulate interstate commerce.[17] The 1958 Act "consolidated among other things all the essential management functions necessary to support the common needs of [U.S.] civil and military aviation."[18] To fulfill its roles of ensuring flight safety and promoting commerce, Congress statutorily authorized the Agency, and its successor, the FAA,[19] to certify foreign repair stations and to permit foreign owners to register aircraft on the FAA Registry (the N Registry). Today, the FAA is grappling with the challenge of ensuring aviation security without stifling commerce by placing an undue burden on commercial carriers and private aircraft owners. Foreign repair stations and aircraft trusts present unique opportunities for exploitation and infiltration by terrorists and foreign governments to disrupt civil aviation and the U.S. economy. Thus, how the FAA addresses insider threats to foreign repair stations and aircraft trusts is critical to national security.

A. WHY DO FOREIGN REPAIR STATIONS EXIST?

In order to analyze foreign repair station vulnerabilities, it is useful to first know what a foreign repair station is and why it exists. Foreign repair stations are facilities outside of the continental United States which are authorized to perform "maintenance, preventive maintenance, or alterations for an air carrier or commercial operator" in accordance with its maintenance

---

[16] Federal Aviation Act of 1958, Pub. L. No. 85-726, 72 Stat. 731 (1958).

[17] U.S. CONST. art. I, § 8; Douglas B. Harris, *Fed. Aviation Act* (1958), ENCYCLOPEDIA.COM (2004), http://www.encyclopedia.com/history/encyclopedias-almanacs-transcripts-and-maps/federal-aviation-act-1958 [https://perma.cc/Z4HD-4AQN].

[18] *Id.*

[19] Congress enacted legislation in 1966 authorizing creation of the Department of Transportation (DOT), then renamed the Agency the "Federal Aviation Administration," and finally, while expressly maintaining the FAA's statutory independence, folded the FAA into the DOT. *See* H.R. Conf. Rep. No. 104-848, 104th Cong., (1996); Federal Aviation Reauthorization Act of 1996, Pub. L. No. 104-264 (1996). *See also A Brief History of the FAA*, FED. AVIATION ADMIN., https://www.faa.gov/about/history/brief_history/ [https://perma.cc/PP5X-2PFN].

program and maintenance manual.[20] The reason why they exist is a practical one.

After World War II, the international aviation boom prompted the United States to certify foreign repair stations in order to ensure that U.S. carriers and operators of U.S.-registered aircraft operating overseas could obtain maintenance and repairs.[21] With U.S. carriers increasingly adding foreign-made aircraft such as British Aerospace Jetstream turboprop aircraft as well as engines and other aircraft components to their fleets,

> [U.S.] carriers and manufacturers were regularly shipping foreign-built components to their original manufacturers for repair, and U.S.-operated turboprops, . . . as well as some corporate jets, were also being sent abroad for maintenance and alterations. FAA had to issue exemptions to permit foreign manufacturers to perform repairs on their own products, and to permit U.S. operators to obtain repairs abroad when they could not be performed in the U.S. in a timely manner because of a lack of appropriately-rated facilities.[22]

Prior to 1988, in order for a U.S. carrier or operator to obtain maintenance or repairs of its foreign-made aircraft, engines, or components, it had to request and receive an exemption from the FAA.[23] For the carrier, downtime is costly as the aircraft would be out of service and not generating fees. Furthermore, if an aircraft were at a repair facility waiting for an exemption prior to making repairs, it could incur daily storage charges or lose its slot on the scheduled maintenance facility calendar if the wait exceeded a certain number of days. In addition, the carrier could become subject to sales and use taxes and/or value-added taxes depending on the time it took the FAA to process the exemption.

By permitting foreign repair stations to obtain FAA certification, this eliminated the need to file exemptions and ensured foreign repair stations met substantially similar certification and personnel requirements as those imposed on domestic repair

---

[20] 14 C.F.R. § 145.205 (2016).

[21] Guy S. Gardner, Assoc. Adm'r for Regulation and Certification, FAA, Statement Before the Senate Comm. on Commerce, Science, and Transp., Subcommittee on Aviation, Concerning the Certification of Foreign Repair Stations, Dep't of Transp. (May 7, 1998), https://testimony.ost.dot.gov/test/pasttest/98test/Gardner1.htm [https://perma.cc/37DP-GYNY].

[22] *Id.*

[23] *Id.*

stations.[24] As a result, carriers saved time and money by eliminating paperwork and associated administrative delays. Since inception, the FAA's foreign repair station oversight has focused on aviation safety with security being left primarily to carriers and repair facilities.

B. Why Do Aircraft Trusts Exist?

In order to analyze aircraft trust vulnerabilities, it is helpful to know what constitutes a trust and why they are so prevalent in aviation. Aircraft trusts are finance agreements which enable aircraft beneficially-owned by trustees to be registered in the United States on behalf of corporations and non-U.S. citizens.[25] The purpose of an aircraft trust is to give the trustee the power to manage and control the aircraft with respect to matters involving ownership and management of the aircraft. To do so, creating a U.S. trustee ensures the aircraft is controlled by a U.S. citizen as statutorily required.[26] The trust arrangement is designed to ensure that the beneficiary has no power to influence or control the exercise of the trustee's authority with respect to ownership and management matters.[27] For a fee, U.S. banks will serve as owner-trustees of trust assets. Bank-administered trust services enable foreign owners to use "trust structures and voting trusts to secure U.S. registration of aircraft for non-U.S. citizen corporations and individuals."[28] This arrangement benefits U.S. aircraft manufacturers, their customers, and financiers. It also advances the FAA's statutory mandates of promoting commerce and safety.

At the heart of trust formation and associated FAA registration lie two statutes: 49 U.S.C. §§ 44102 and 44103. While Title 49, Subtitle VII, Part A, Subpart iii, Chapter 441 governs operation, registration and recordation of aircraft ownership rights and interests,[29] 49 U.S.C. §§ 44102 and 44103 prescribe the citi-

---

[24] *Id.*

[25] *What Is an Aircraft Trust?*, Van Bortel Aircraft Inc., http://vanbortel.com/files/Basic_Trust_FAQ.pdf [https://perma.cc/6G5G-D87J]; *see also* 14 C.F.R. § 145.51(c) (2014); 49 U.S.C. § 44924 (2012).

[26] 49 U.S.C. § 40102(a)(15).

[27] The trustee will typically provide an affidavit to the FAA. *See* 14 C.F.R. 47.7(c)(2)(iii) (2016).

[28] *Transportation and Large Ticket Products*, Wells Fargo, https://www.wellsfargo.com/com/corporate-trust/lease [https://perma.cc/EP5S-5XTH]; *see also* 14 C.F.R. § 47.

[29] 49 U.S.C. § 44101 (2012).

zenship, registration, and nationality requirements which contribute to the widespread use of trust arrangements.

1. 49 U.S.C. § 44102

Pursuant to 49 U.S.C. § 44102,[30] only aircraft which are not on a foreign registry and which are owned by a U.S. citizen, resident alien, or corporation[31] may be registered on the N Registry. While U.S. citizens and resident aliens may base and operate their aircraft outside of the United States, all corporate-owned aircraft must be based and primarily used in the United States, and the corporations must be organized and doing business under U.S. or state laws.[32]

2. 49 U.S.C. § 44103

Pursuant to 49 U.S.C. § 44103,[33] the registration certificate of a § 44102-qualified aircraft is "(1) conclusive evidence of the nationality of an aircraft for international purposes, but not conclusive evidence in a proceeding under the laws of the United States; and (2) not evidence of ownership of an aircraft in a proceeding in which ownership is or may be in issue."[34] So long as a U.S. citizen, resident alien, or corporation is the registered owner of the aircraft, and assuming the aircraft is airworthy, it may operate in U.S. airspace and be maintained on the U.S. N Registry.

The presumption of U.S. nationality of corporate owner-registrants is what makes §§ 44102 and 44103 work in favor of aircraft manufacturers and foreign purchasers of aircraft, while also promoting aviation safety and generating tax revenues for state and federal tax authorities. These two provisions have also contributed to the widespread use of aircraft trusts.

III. WHAT IS THE INSIDER THREAT?

In order to address the insider threat, it is helpful to define the terms "insider" and "insider threat." A working definition of an "insider" is an employee (or contractor) "who may represent

---

[30] 49 U.S.C. § 44102 (2012); 14 C.F.R. §§ 45, 47, 49 (2016).

[31] 49 U.S.C. § 44102(a)(1)(C).

[32] *Id.*

[33] 49 U.S.C. § 44103 (2012); 14 C.F.R. §§ 45, 47, 49 (2016).

[34] 49 U.S.C. § 44103(c).

a threat to national security."[35] The National Insider Threat Policy (NITP)[36] broadly defines the term "insider" as "[a]ny person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks, or systems."[37] In addition, a "malicious insider [is someone who] can deny, degrade, disrupt, destroy, deceive, corrupt, [and/or] usurp"[38] legitimate goals, activities, and/or actors.

While the insider threat includes "fraud, theft of intellectual property (e.g., trade secrets, strategic plans, and other confidential information), [IT] sabotage, and espionage,"[39] the term itself encompasses multiple security concepts. The NITP broadly defines the term "insider threat" as

> [t]he threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.[40]

The critical element which makes the insider threat so insidious is trust. The insider takes advantage of his status as a trusted insider to gain access to information, facilities, and/or resources from which outsiders would normally be barred absent a court order.

Contrary to its name, the NITP is not a single policy. It is an aggregation of several executive orders which "leverages existing federal laws, statutes, authorities, policies, programs, systems, architectures and resources in order to counter the threat of those insiders who may use their authorized access to compromise

---

[35] *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector*, INTELLIGENCE & NAT'L SEC. ALL., Sept. 2013, at 3, http://csrc.nist.gov/cyberframework/framework_comments/20131213_charles_alsup_insa_part4.pdf [https://perma.cc/YR9N-SVNM] [hereinafter *A Preliminary Examination of Insider Threat Programs*].

[36] *National Insider Threat Policy* (2012), http://www.fas.org/sgp/obama/insider.pdf [https://perma.cc/N9DZ-YRED]; *see also Presidential Memorandum—National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, WHITE HOUSE (Nov. 21, 2012), http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand [https://perma.cc/H5MU-RBPA].

[37] *National Insider Threat Policy*, *supra* note 36, at 4.

[38] *A Preliminary Examination of Insider Threat Programs*, *supra* note 35, at 3.

[39] *Id.* at 1.

[40] *National Insider Threat Policy*, *supra* note 36, at 4.

classified information."[41] Apart from EO 13587, the NITP relies on EO 13526[42] and EO 12968[43] to protect classified national security information by establishing access criteria, which also include "appropriate protections for privacy, civil rights, and civil liberties."[44]

The role of insiders and the threat posed by them is "the top counterintelligence challenge to [the intelligence] community"[45] and, arguably, national security. The potential scope of insider activities is limited only by human imagination. Historically, insiders are nothing new. Whether rogue stockbrokers[46] or Cold War-era moles,[47] insiders have caused organizations "financial losses, negative impacts to business operations, and damage to reputation."[48] Whether rising to the level of treason perpetrated by Benedict Arnold[49] or Robert Hanssen,[50] it is likely in-

---

[41] *Id.* at 1.

[42] Executive Order 13526 provides a "uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism" which includes classification authorities, standards, levels, categories, and duration. Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009).

[43] Executive Order 12968, as amended by EO 13467, provides access, disclosure, eligibility, and administrative proceedings guidelines for classified information. Exec. Order No. 12,968, 60 Fed. Reg. 40,245 (Aug. 7, 1995), http://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf [https://perma.cc/3RMW-V3Y6]; *see also* Exec. Order No. 13,467, 73 Fed. Reg. 38,103 (July 2, 2008), http://www.gpo.gov/fdsys/pkg/FR-2008-07-02/pdf/08-1409.pdf [https://perma.cc/DM7G-VWRV].

[44] *National Insider Threat Policy*, *supra* note 36, at 1.

[45] *See* STAFF OF S. COMM. ON INTELLIGENCE, 112TH CONG., INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE, 46 n.5 (2012), https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf [https://perma.cc/JC7M-LW2B]; *see also* Aquala Bogan, *Dave DeVries on the DoD's Mobile Device Strategy: IT Priorities and Big Data Analytics*, WASH. EXEC. (Mar. 21, 2013), http://www.washingtonexec.com/2013/03/dave-devries-on-the-dods-mobile-device-strategy-and-it-priorities/ [https://perma.cc/9GLA-XNBN].

[46] *Four Canadians Charged in Largest International Penny Stock Fraud Scheme in History*, FIN. POST (Aug. 13, 2013), http://business.financialpost.com/2013/08/13/four-canadians-charged-in-largest-international-penny-stock-fraud-scheme-in-history/ [https://perma.cc/7S57-TYMS].

[47] *Robert Hanssen*, FED. BUREAU OF INVESTIGATION (Feb. 20, 2001) https://www.fbi.gov/history/famous-cases/robert-hanssen [https://perma.cc/5TJ7-Q654].

[48] *Information Security Risk Assessment Applicability and Impact to the FAA Safety Management System*, RAYTHEON COMPANY (Apr. 30, 2012) at 10 [hereinafter *ISR—FAA Safety Management System*].

[49] *Benedict Arnold*, US HISTORY, http://www.ushistory.org/ValleyForge/served/arnold.html [https://perma.cc/N9MQ-9YAH].

sider leaks have occasioned the detention, arrest, interrogation, torture, and/or death of U.S. intelligence sources and operatives.[51]

Depending on an insider's access level and funding, as well as the complexity and scope of his operational plan and goals, an insider's activities can "take as long as external threats to execute, [while] well planned attacks can take weeks and months to prepare; ultimately the magnitude of either can be significant."[52] Although

> insiders pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases, . . . external threats are nearly surpassing the internal concerns; it will be in the near term that both internal and external threats have to be dealt with at the same levels. The methods and motivation of each may be different; however the results are nearly the same and as such must be treated at the medium to high risk levels.[53]

As significant and potentially dangerous as the actions of an insider may be, any program which is designed to counter insider threats has the potential for overzealous implementation and missteps. The insider threat program the FAA is implementing is no exception; however, how the FAA addresses insider threats is important given the FAA's public trust and visibility. Since 1958, the FAA has functioned as a primarily civilian and essentially global public entity which has twenty-four-hour domestic and international operations.[54] The FAA also plays a role in military aviation[55] as well as a global role in promoting aviation safety and aviation-related intelligence.[56] It is thus a civil, military, and intelligence target.

Since 2001, the FAA has had the unenviable task of striking a balance between aviation safety and security measures and costs

---

[50] *See Robert Hanssen*, *supra* note 47.

[51] Brian Palmer, *Has an Intelligence Leak Ever Caused an American Death?*, SLATE (Sept. 7, 2012), http://www.slate.com/articles/news_and_politics/explainer/2012/09/navy_seal_matt_bissonnette_s_no_easy_day_has_an_intelligence_leak_ever_cost_an_american_life_.html [https://perma.cc/7U42-5FPT].

[52] *ISR—FAA Safety Management System*, *supra* note 48, at 10.

[53] *Id.* at 9.

[54] *A Brief History of the FAA*, *supra* note 19.

[55] *Special Operations*, FED. AVIATION ADMIN., http://www.faa.gov/air_traffic/publications/spec_ops/ [https://perma.cc/F6NV-8592].

[56] 49 U.S.C. § 40101 (2012); *Notice Re: Coordination with the Office of Security and Hazardous Materials Safety on Aviation Safety, Security, Intelligence, and Support to Law Enforcement*, FED. AVIATION ADMIN. (July 2, 2013), http://www.faa.gov/documentLibrary/media/Notice/N_8900.222.pdf [https://perma.cc/QDA2-HRYE].

to commercial interests while operating within DOT budget constraints.

> Before September 11th, the aviation security model was mostly based on reacting to known security threats instead of being proactive against potential threats. The model, dating back to the early 1970s, was implemented through a system of shared responsibilities. Industry provided and paid for the security; FAA's role was to establish security requirements and ensure compliance with these requirements. Within the model were counter pressures to control security costs and limit the impact of security on aviation operations, so that industry could concentrate on its primary mission of moving passengers seamlessly and safely through the system.[57]

Today, financial decisions and competing priorities impact not only the cyber-vulnerabilities of NextGen,[58] but also security-related issues posed by foreign repair stations and aviation trusts. Widespread availability and use of computers, IT, and the internet make it possible to intrude electronically from virtually anywhere in the world. For example, "the FAA's systems are probed 50,000 times an hour by people intent on doing harm at some point."[59] Weighed against the cyber threat, and the funding granted by Congress to combat it, it is tempting to give human insider threats short shrift.

Faced with the evolving nature of the insider threat, the FAA is at a crossroads. It must balance national aviation security policy requirements with its statutory mandate to promote commerce and the historic openness of the aviation community. Further complicating this task is the emphasis placed on data security and "cyber" at the expense of overlooking other important areas which are vulnerable to penetration, exploitation, manipulation, and disruption. The relative ease with which an insider could potentially endanger the safety of passengers and aircrew as well as adversely impact the global economy by target-

---

[57] U.S. Dep't of Transp., Statement Before the National Commission on Terrorist Attacks Upon the United States on Aviation Security, at 1 (May 22, 2003), https://www.oig.dot.gov/sites/default/files/cc2003117.pdf [hereinafter DOT IG Statement] [https://perma.cc/T4ZS-7H99].

[58] NextGen is the FAA's satellite-based navigation system. *See* What is NextGen?, Fed. Aviation Admin. (2013), https://www.faa.gov/nextgen/ [https://perma.cc/AWU8-UXE5].

[59] James Careless, *Moving Targets*, Air Traffic Mgmt. (Mar. 3, 2015), http://www.airtrafficmanagement.net/2015/03/moving-targets/ [https://perma.cc/QYP8-HHLT] (statement by FAA Administrator Michael Huerta).

ing foreign repair stations and/or aviation trusts is particularly problematic.

IV. AVIATION SECURITY POLICY

To combat the evolving insider threat, U.S. aviation security policy is changing. The policy framework shaping the FAA's approach consists of executive orders, legislation, and directives (collectively, Policies). The most important Policies applied to the question of how to detect and deter insider threats to foreign repair stations and aviation trusts are EO 13587,[60] EO 13388,[61] the Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA),[62] National Security Policy Directive 47/Homeland Security Policy Directive 16 (NSPD 47/HSPD 16),[63] and National Security Directive 42 (NSD 42).[64] In addition to these Policies, the Executive Agent for Safeguarding Classified Information on Computer Networks (EACICN)[65] and the Insider Threat Task Force (ITTF)[66] established by EO 13587 also play key roles.

A. EO 13587

When President Barack Obama enacted EO 13587, he placed the burden on federal agencies to implement structural reforms "to ensure responsible sharing and safeguarding of classified information on computer networks."[67] He also required them to provide

> appropriate protections for privacy and civil liberties . . . [by adopting] minimum standards regarding information security, personnel security, and systems security; [to] address both internal and external security threats and vulnerabilities; and [to]

---

[60] EO 13587, *supra* note 5.

[61] Exec. Order No. 13,388, 70 Fed. Reg. 62,023 (Oct. 25, 2005) [hereinafter EO 13388].

[62] Intelligence Reform and Terrorism Prevention Act of 2004, as amended, Pub. L. 108-458 (Dec. 17, 2004), https://www.gpo.gov/fdsys/pkg/PLAW-108publ458/html/PLAW-108publ458.htm [https://perma.cc/3ZWE-VWFY] [hereinafter IRTPA].

[63] National Security Policy Directive 47/ Homeland Security Policy Directive 16, WHITE HOUSE (June 20, 2006), http://www.fas.org/irp/offdocs/nspd/nspd-47.pdf [https://perma.cc/82J6-5VE6].

[64] National Security Directive 42, WHITE HOUSE (July 5, 1990), http://www.fas.org/irp/offdocs/nsd/nsd42.pdf [https://perma.cc/ND8P-KH3Q].

[65] EO 13587, *supra* note 5, § 5.

[66] *Id.* § 6.

[67] *Id.*

> provide policies and minimum standards for sharing classified information both within and outside the Federal Government.[68]

Although designed specifically to address computer security vulnerabilities, EO 13587 applies to "all users of classified computer networks . . . and *all classified information* on those networks."[69]

Whether information is classified "Top Secret" or is sensitive but unclassified, that designation is made in accordance with EO 13256.[70] Regardless of whether the classification authority is the Department of Defense[71] or the FAA, the classification marked on a document is designed to limit access and protect against unauthorized disclosure depending on its sensitivity.[72] Given the breadth of EO 13587, anyone who uses the FAA computer network, including anyone who accesses FAA-maintained databases, may potentially face prosecution. This potential liability exists because of EO 13587's

> policies and minimum standards for sharing classified information both within and outside the Federal Government. . . . [which] address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.[73]

To balance the risk of prosecution and termination of federal employment with the U.S. Constitution, EO 13587 provides for

---

[68] *Id.*

[69] *Id.* (emphasis added).

[70] On December 29, 2009, President Barack Obama revoked E.O. 12958. Kevin R. Kosar, *Security Classification Policy and Procedure: E.O. 12958, as Amended*, CONG. RESEARCH SERV. at 11 (Dec. 31, 2009), http://www.fas.org/sgp/crs/secrecy/97-771.pdf [https://perma.cc/Z3DD-44LJ]. See Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009), https://www.archives.gov/isoo/policy-documents/cnsi-eo.html [https://perma.cc/M4ZY-69HM]; *see also* Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995), https://fas.org/sgp/clinton/eo12958.html [https://perma.cc/5BWS-K789], amended by Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003), http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html [https://perma.cc/M33Q-2W2E].

[71] *DoD Guide to Marking Classified Documents*, OFFICE OF THE ASSIST. SEC. OF DEF. FOR COMMAND, CONTROL, COMMC'N, AND INTELLIGENCE (Apr. 28, 1997), http://www.dod.mil/pubs/foi/Reading_Room/Administration_and_Management/907.pdf [https://perma.cc/JR3Q-Z47P].

[72] *Classified Information Nondisclosure Agreement (SF312) and Verbal Attestation Briefing Pamphlet*, DEP'T OF DEF. at 5 (May 2000), http://biotech.law.lsu.edu/blaw/dodd/corres/pdf/52001ph1_0500/p5200ph1.pdf [https://perma.cc/SPQ5-UE63].

[73] EO 13587, *supra* note 5, § 1.

whistleblower protection[74] as well as privacy and civil liberties safeguards[75] by extending the legal protections of the "Intelligence Community Whistleblower Protection Act of 1998, Whistleblower Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies"[76] to government employees and contractors.

Although EO 13587 applies to publicly available information such as aircraft registration numbers and information published on the FAA Registry,[77] that information is maintained in the registry database and/or in internal FAA databases. Thus, insiders who use or access this information may face prosecution if their disclosures are unauthorized. Such insiders may also potentially avail themselves of EO 13587's whistleblower protections. For example, if an FAA contractor (or an FAA employee) at a foreign repair station were to use sensitive but unclassified information accessible to him through an FAA database or the FAA website in the course of performing his work-related duties, he could potentially seek whistleblower status if he claimed his leaks, whether to the media or published on a blog, were to expose fraud, waste, or abuse.

It is also possible that an FAA contractor (or an FAA employee) could use sensitive but unclassified information for harmful purposes (e.g., disrupting air traffic, causing panic in the flying public, or wreaking economic havoc). As EO 13587 contains anti-retaliation provisions, which prohibit agencies from seeking to "deter, detect, or mitigate disclosures of information,"[78] it is possible an insider could attempt to evade adverse administrative action or criminal prosecution by claiming whistleblower status.

1. EACICN

Prior to enactment of EO 13587, the Secretary of Defense and the Director of the National Security Agency (NSA) were designated by NSD 42 as the Executive Agent and National Manager for national security systems respectively. Their separate roles were merged pursuant to EO 13587 into a joint EACICN.[79] The

---

[74] *Id.* § 7(e).
[75] *Id.* § 7(h).
[76] *Id.* § 7(e).
[77] *See FAA Registry*, FED. AVIATION ADMIN., http://registry.faa.gov/aircraftinquiry/ [https://perma.cc/T73D-HEP5].
[78] EO 13587, *supra* note 5, § 7(e).
[79] *Id.* § 5.1.

goal of linking separate military and intelligence roles and functions was to promote information sharing, particularly of classified information on computer networks.[80] The EACICN was also directed to ensure "reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government."[81] EO 13587 is important because it openly recognized the insider threat government-wide. Although the requirement to ensure personnel security and address the internal threat is tied to computer security and information security, these issues directly impact not only airspace management but aircraft maintenance and registration.

2. ITTF

Given the mounting importance of insider threat detection and prevention, EO 13587 also established the Insider Threat Task Force to provide overall guidance and standards devised by the Attorney General (AG) and the Director of National Intelligence (DNI), or their designees.[82] Curiously, unlike NSD 42, which provided for DOT (and implicitly FAA) to be involved with efforts to combat the insider threat, the ITTF does not explicitly include DOT or FAA.[83] Apart from certain enumerated agencies, ITTF membership is limited to only "such additional agencies as [the AG and DNI] may designate"[84] jointly. ITTF staff is drawn from the FBI and the Office of the National Counterintelligence Executive, "and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law."[85] Given the nature of the September 11th attacks and the vulnerability of aviation to attack, sabotage, infiltration, and exploitation, it seems odd that the FAA is not a named member of the ITTF. As the FAA is recognized globally for its aviation expertise and is statutorily responsible for aviation safety (and implicitly security), the omission is glaring. As the flying public was (and will continue to be) targeted by ter-

[80] *Id.* § 1.
[81] *Id.*
[82] *Id.* § 6.
[83] *Id.* § 6.2.
[84] *Id.*
[85] *Id.*

rorists for the foreseeable future, the FAA should be a permanent agency member of the ITTF.

B. EO 13388

While EO 13587 is one of the most significant policies which addresses the insider threat because it established the EACICN and the ITTF, promoted intelligence information sharing, and extended whistleblower protection to government employees and contractors, it is not the sole relevant authority. EO 13388 is equally important because it was designed to "strengthen the effective conduct of [U.S.] counterterrorism activities and protect . . . [U.S.] territory, people, and interests" by giving the highest priority to "the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities."[86] Just as EO 13587 has countervailing whistleblower protection provisions, EO 13388 requires agencies to "protect the freedom, information privacy, and other legal rights of Americans in the conduct of [counter-terrorism] activities" while simultaneously promoting the "interchange of terrorism information between agencies and . . . appropriate private sector entities."[87]

Although EO 13388 does not specifically identify what companies qualify as "appropriate private sector entities," presumably U.S. carriers which utilize foreign repair stations to "conduct a range of repairs and maintenance, from critical components—such as landing gear and engine overhauls—to heavy airframe maintenance checks, which are a complete teardown and overhaul of the aircraft"[88] would be among those entities. The FAA established the Quarterly Utilization Report system in 2007[89] to ensure carriers and repair stations reported outsourced repairs; however, reporting volume and locations of critical repairs is voluntary and not subject to FAA inspection.[90] Further complicating matters, many foreign repair stations which are used to

---

[86] EO 13388, *supra* note 61, § 1(a).

[87] *Id.*

[88] *Is The Flying Public Protected? An Assessment of Security at Foreign Repair Stations: Hearing Before the Subcomm. on Transp. Sec. & Infrastructure Prot.*, 111th Cong. 111-44 (2009) (statement of the Hon. Calvin L. Scovel III, Inspector Gen., U.S. Dep't of Transp.) [hereinafter 2009 DOT IG Testimony].

[89] FED. AVIATION ADMIN., THE ENHANCED REPAIR STATION AND AIR CARRIER OVERSIGHT SYSTEM (2005); *see also* Dan Bachelder, *Oversight of Contract Maintenance*, FED. AVIATION ADMIN. (June 5, 2008), www.ifairworthy.com/ppt/Contract_Maintenance.ppt? [https://perma.cc/H8AU-G4FU].

[90] 2009 DOT IG Testimony, *supra* note 88, at 4.

perform repairs are not FAA-certified facilities owned or operated by U.S. carriers.[91]

Even if the facilities were carrier-owned and operated as well as FAA-certified, the employees at foreign repair stations are largely foreign nationals. This creates issues not only as to oversight, but also information sharing as an insider, due to the nature of employees' regular work duties, might have access to threat information as well as sensitive but unclassified information provided to the carrier. Alternately, concerns about insider leaks or lack of cleared individuals at foreign repair stations could also preclude or severely limit information sharing by FAA or TSA.

Either scenario poses problems. While it may be comforting to think of terrorists (and other non-state actors) as uneducated or low-skill individuals, terrorists (or their dupes and accomplices, whether paid or coerced) could be highly skilled specialists and technicians (e.g., pilots,[92] mechanics, computer programmers, bankers, etc.). In particular, narco-terrorists[93] may have significant resources as well as the means to pursue longer-term and more complex plans.[94] Given the sophistication and longevity of the non-state enterprise, it may also act in ways and have resources comparable to that of a state actor. Nonetheless, it is state actors (including state sponsors of terrorism), which have historically possessed the depth of resources to pursue long-term, complex, and subtle plans through their insider agents.

---

[91] In 2009, there were 731 foreign repair stations and 4,126 U.S. repair stations. *See id.* at 1.

[92] While not proven, it is possible the EgyptAir Flight 990 first relief pilot may have disconnected the autopilot in order to crash the jet as an elaborate trial run for the attacks on the World Trade Centers to demonstrate the ease of seizing and crashing an aircraft, assess how effectively the news would be disseminated, and/or how law enforcement and intelligence would react to a terrorist act originating on a flight from the United States. *See* Michael Ellison, *US and Egypt Split on Fatal Plane Crash*, THE GUARDIAN (June 28, 2000), http://www.theguardian.com/world/2000/jun/09/egyptaircrash.usa [https://perma.cc/WAJ9-KJ4E]; *see also Aircraft Accident Brief, EgyptAir Flight 990, Boeing 767-366ER, SU-GAP, 60 Miles South of Nantucket, Massachusetts, October 31, 1999*, NAT'L TRANSP. SAFETY BD., at 4 (Mar. 13, 2002), http://libraryonline.erau.edu/online-full-text/ntsb/aircraft-accident-briefs/AAB02-01.pdf [https://perma.cc/F59K-QPZD].

[93] *Lessons From History: Some Background Information on Narco-Funded Terrorism*, NARCOTERROR, http://www.narcoterror.org/background.htm [https://perma.cc/Z6SR-Y7Q9].

[94] John E. Thomas, Jr., *Narco-Terrorism: Could the Legislative and Prosecutorial Responses Threaten Our Civil Liberties?*, 66 WASH. & LEE L. REV. 1881, 1882 (2009).

For example, if a facility in Mexico performs avionics control systems overhauls on an American Airlines Boeing 737-400 aircraft, it is possible that a terrorist operative could pressure a mechanic or manager at that facility to provide information about the aircraft's avionics systems. It is also possible a terrorist could work at the facility and have access to the information and aircraft in the ordinary course of his duties. This information could be used to introduce a virus into the inertial navigation system or flight control system of the target 737-400 operating out of New York. Alternatively, a mechanic could sabotage flight control wiring by stripping it of insulation or fraying it, causing it to spark or break in-flight. In either scenario, it is possible that the aircraft could go into an uncontrolled dive over the Atlantic Ocean and crash. The target need not be a particular passenger if disruption, economic dislocation, and engendering fear are the desired outcome.

If the FAA did not know that the facility was used for such repairs or did not have inspection or certification rights for the facility, it would not be able to enforce adherence to U.S. airworthiness and safety standards, much less deter hostile insider activities. Even if it were an FAA-certified facility used by American Airlines, the repair station is a Mexican company, located in Mexico, and staffed with Mexican nationals. The Mexican government would need to authorize and assist in performing background checks, security and information exchanges, etc. Furthermore, the legal safeguards of EO 13388 are not available to Mexicans and other third-country nationals.

C. IRTPA

In addition to EO 13587 and EO 13388, IRTPA was designed to "reform the intelligence community and the intelligence and intelligence-related activities of the U.S. government, and for other purposes."[95] However, Title IV, Subtitle B—Aviation Security does not address foreign repair stations or aircraft trusts. It is focused on airport-centric measures such as cargo, airport screening, and flight-deck access. To address the issue of foreign repair stations and other aviation issues, Congress enacted Vision 100,[96] which required the TSA to issue repair station secur-

---

[95] IRTPA, *supra* note 62, at Preamble.

[96] Vision 100 is the enabling legislation for FAA's Next Generation Air Transportation System. *See* Vision 100—Century of Aviation Reauthorization Act, Pub. L. No. 108-76 (2003) [hereinafter Vision 100].

ity rules for domestic and international facilities by August 2004. Despite the Congressional mandate, the TSA did not do so. To force the TSA to act, Congress subsequently issued the Implementing Recommendations of the 9/11 Commission Act of 2007,[97] which established an August 3, 2008,[98] deadline for the TSA to issue the required repair station security rules. Despite Congress statutorily extending the deadline, the TSA again failed to comply. Because of the TSA's unwillingness or inability to finalize repair station security rules, the FAA has been barred from issuing new foreign repair station certifications since 2008.[99] As no new domestic or foreign repair stations have been authorized, and the required security rules have not been issued, repair station vulnerabilities remain unresolved.

D. NSPD 47/HSPD 16

In order to implement a comprehensive and cohesive national aviation security policy which "optimize[d] the coordination and integration of government-wide aviation security efforts,"[100] President George W. Bush issued a new national aviation security policy, NSPD 47/HSPD 16.[101] NSPD 47/HSPD 16 outlines "U.S. policy, guidelines, and implementation actions to continue the enhancement of U.S. homeland security and national security by protecting the United States and U.S. interests from threats in the Air Domain"[102] on an agency-by-agency basis with particular emphasis on joint operations and integrated planning. In addition, NSPD 47/HSPD 16 generated six operating plans which provide implementation guidance concerning aviation transportation system security,[103] aviation operational

---

[97] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53 (Aug. 3, 2007).

[98] *Id.* § 1616(a), 49 U.S.C. § 44924 (2012).

[99] *Irked by the Foreign Repair Station Ban?*, AERONAUTICAL REPAIR STATION ASSOC. (July 30, 2013), http://arsa.org/irked-by-the-foreign-repair-station-ban/.

[100] *National Security Presidential Directive 47/Homeland Security Presidential Directive 16*, WHITE HOUSE http://www.dhs.gov/hspd-16-aviation-security-policy [https://perma.cc/B6S5-P53V].

[101] *National Security Policy Directive 47/Homeland Security Policy Directive 16*, *supra* note 63.

[102] DOMESTIC OUTREACH PLAN: SUPPORTING PLAN TO THE NATIONAL STRATEGY FOR AVIATION SECURITY 2, U.S. DEP'T OF HOMELAND SEC. (Mar. 26, 2007), http://www.dhs.gov/xlibrary/assets/hspd16_domoutreachplan.pdf [https://perma.cc/S38A-XVQV].

[103] AVIATION TRANSPORTATION SYSTEM SECURITY PLAN: SUPPORTING PLAN TO THE NATIONAL STRATEGY FOR AVIATION SECURITY, U.S. DEP'T OF HOMELAND SEC. (Mar.

threat response,[104] aviation transportation system recovery,[105] air domain surveillance and intelligence integration,[106] domestic outreach,[107] and international outreach.[108] While the plans provide guidance on a variety of threats and implementation of countermeasures focused on airports, cargo, and air traffic control, they do not address repair stations and aviation trusts.

E. HSPD 7

Pursuant to the Homeland Security Presidential Directive on Critical Infrastructure Identification, Prioritization, and Protection (HSPD 7),[109] DHS is responsible for coordinating critical infrastructure protection activities for aviation;[110] however, DOT is responsible for operating the national air space system as administered by the FAA.[111] While DHS is tasked with "work[ing] closely with other Federal departments and agencies, State and local governments, and the private sector,"[112] it must "collaborate [with DOT] on all matters relating to transportation security and transportation infrastructure protection."[113] As DOT "is responsible for ensuring that air traffic control facilities, systems, and operations are protected from significant disruption caused

---

26, 2007), http://www.dhs.gov/xlibrary/assets/hspd16_transsystemsecurityplan.pdf [https://perma.cc/P3KQ-SYKY].

[104] AVIATION OPERATIONAL THREAT RESPONSE PLAN: SUPPORTING PLAN TO THE NATIONAL STRATEGY FOR AVIATION SECURITY, U.S. DEP'T OF HOMELAND SEC. (Mar. 26, 2007), http://www.dhs.gov/xlibrary/assets/hspd16_opthreatrespplan.pdf [https://perma.cc/DT6U-UTBN].

[105] AVIATION TRANSPORTATION SYSTEM SECURITY PLAN, *supra* note 103.

[106] AIR DOMAIN SURVEILLANCE AND INTELLIGENCE INTEGRATION PLAN: SUPPORTING PLAN TO THE NATIONAL STRATEGY FOR AVIATION SECURITY, U.S. DEP'T OF HOMELAND SEC. (Mar. 26, 2007), http://www.dhs.gov/xlibrary/assets/hspd16_domsurvintelplan.pdf [https://perma.cc/5DKD-EXLJ].

[107] DOMESTIC OUTREACH PLAN: SUPPORTING PLAN TO THE NATIONAL STRATEGY FOR AVIATION SECURITY, U.S. DEP'T OF HOMELAND SEC. (Mar. 26, 2007), http://www.dhs.gov/xlibrary/assets/hspd16_domoutreachplan.pdf [https://perma.cc/PPY5-HGMF].

[108] INTERNATIONAL OUTREACH PLAN: SUPPORTING PLAN TO THE NATIONAL STRATEGY FOR AVIATION SECURITY, U.S. DEPT' OF HOMELAND SEC. (Mar. 26, 2007), http://www.dhs.gov/xlibrary/assets/hspd16_intloutreachplan.pdf [https://perma.cc/VB87-7PHM].

[109] *Directive on Critical Infrastructure Identification, Prioritization, and Protection*, WHITE HOUSE (Dec. 17, 2003), http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf [hereinafter HSPD 7] [https://perma.cc/VT67-S7CY].

[110] *Id.* § 15.

[111] *Id.* § 22(h).

[112] *Id.* § 17.

[113] *Id.* § 22(h).

by man-made or natural events[, it must be] able to resume essential services in a timely manner if disrupted, to minimize the impact on the Nation's economy."[114] While DOT has "its own unique characteristics and operating models"[115] which do not necessarily mesh well with DHS culture, it must coordinate and cooperate with DHS to fulfill the requirements of HSPD 7.[116] Therein lies the problem. Transportation, particularly aviation, has its own vernacular, customs, and culture. Foreign repair stations and aviation trusts are two manifestations of aviation approaches to practical issues of operational efficiency and finance.

F. NSD 42

When President George H.W. Bush enacted NSD 42[117] prior to the Gulf War,[118] the potential for foreign intelligence disruption of telecommunications and information technology was emerging as a new global threat in the post-Cold War era where countermeasures and counterintelligence were focused on evolving intelligence threats to U.S. programs, personnel, operations, and installations.[119] NSD 42 established a 22-member steering committee chaired by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and placed the Secretary of Transportation as one of the civil agency members. DOT was included presumably to ensure that aviation, rail, automotive, and maritime risks were addressed with respect to countering intelligence threats. NSD 42 marks the shift to technology and telecommunications threats and away

---

[114] Rebecca C. Leng, *Memorandum re: Report on Review of FAA's Progress in Enhancing Air Traffic Control Systems Security Report Number FI-2010-006*, DEP'T OF TRANSP. (Nov. 2, 2009).

[115] HSPD 7, *supra* note 109, § 18.

[116] Joshua B. Bolten, *Memorandum Re: Development of Homeland Security Presidential Directive (HSPD)—7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources*, EXEC. OFF. OF THE PRESIDENT, OFF. OF MGMT. AND BUDGET (June 17, 2004), http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf [https://perma.cc/67X5-CT92].

[117] National Security Directive 42, *supra* note 64.

[118] The first Gulf War started August 2, 1990, with the invasion of Kuwait by Iraq and ended February 28, 1991, with Iraq's acceptance of cease fire resolutions issued by United Nations. *Timeline: War in the Gulf*, BBC NEWS (Aug. 2, 2000), http://news.bbc.co.uk/2/hi/middle_east/861164.stm [https://perma.cc/BNJ2-MKHU].

[119] National Security Directive 47, Counterintelligence and Security Countermeasures, WHITE HOUSE (Oct. 5, 1990), *available at* http://bush41library.tamu.edu/files/nsd/nsd47.pdf [https://perma.cc/3JS9-NZPX].

from human threats and intelligence activities at a time when internal threats were evolving and, thanks to technology, becoming more likely and more widespread.

V. FOREIGN REPAIR STATIONS

Given the enormous importance of civil aviation to U.S. commerce, and the narrow profit margins of U.S. carriers,[120] foreign repair stations are an operational necessity. While minimizing downtime for maintenance and returning aircraft to service sooner is essential for efficient carrier operations, flight safety is the FAA's top priority. As FAA certification necessitates U.S. aviation maintenance safety standards be met, FAA-certified repair stations promote aviation safety and ensure American airworthiness standards are used globally.

A. 14 CFR Part 145

Pursuant to 14 C.F.R. Part 145, Chapter 11,[121] the FAA can certify foreign repair stations which provide "documentation demonstrating that the repair station certificate or rating is necessary for maintaining U.S.-registered or U.S.-operated foreign aircraft or components."[122] The emphasis is on flight safety and airworthiness, not repair station security.

B. The Certification Process

To achieve Part 145 certification, the repair station must complete the pre-application, formal application, document compliance, demonstration and inspection, and certification process.[123] This process is focused on aviation safety, not aviation security.[124] The pre-application consists of a familiarization meeting with the FAA certification team regarding the appli-

---

[120] *Airline Profitability Prospects Improve but Profit Margins Remain Anaemic*, CAPA – Centre for Aviation (Oct. 18, 2012), http://centreforaviation.com/analysis/airline-profitability-prospects-improve-but-profit-margins-remain-anaemic-85722 [https://perma.cc/28QY-X2MY].

[121] Order 8900.1 CHG 87, § 2-1243, Fed. Aviation Admin. (Mar. 8, 2010) [hereinafter 8900.1].

[122] *Id.* § 2-1244.

[123] *Id.*

[124] Doug Dalbey, Deputy Director of Flight Standards for Field Operations, Fed. Aviation Admin., Statement on Security at Foreign Repair Stations before the House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection 16 (Nov. 18, 2009) [hereinafter 2009 Foreign Repair Station Update], https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg55248/pdf/CHRG-111hhrg55248.pdf [https://perma.cc/MQY3-MZME].

cant's intent, the application process, statutory fee,[125] and submission of FAA Form 8400-6.[126] As part of the formal application, the applicant must "provide the FAA with documentation demonstrating that the repair station certificate or rating is necessary for maintaining U.S.-registered or U.S.-operated foreign aircraft or components as required by Part 145, § 145.51(c)."[127] During this phase, FAA inspectors meet with the applicant's management team to determine the "legal name of the owner and the address where the repair station will be located."[128] In the document compliance phase, the FAA inspection team reviews repair station manuals "and related attachments to ensure conformity to the applicable regulations and safe operating practices" before it determines whether the applicant's procedures, facilities, and equipment meet FAA safety requirements or require demonstration and inspection prior to certification.[129]

C. Vulnerabilities

Similar to the FAA's focus on foreign repair station oversight, the 2003 Inspector General report regarding aircraft repair stations focused on safety, not security.[130] While it is important that the FAA "made a number of changes to [its] oversight of repair stations,"[131] what the FAA did not do, and arguably could not do, was improve security to safeguard against insider threats.

In part, the FAA's inability to adequately address insider threats is due to lack of funding and lack of statutory authority. Under Vision 100, the FAA remains statutorily focused primarily

---

125 14 C.F.R. § 187.1 (2017).

126 8900.1, *supra* note 121, § 2-1244.

127 *Id.*

128 *Id.*

129 *Id.*

130 Alexis M. Stefani, *Review of Air Carriers' Use of Aircraft Repair Stations*, Dep't of Transp., AV-2003-047, 1 (July 8, 2003) [hereinafter 2003 DOT IG Report].

131 The changes included revising the regulations that apply to repair stations; improving quality control requirements; utilizing system safety requirements, risk management software, and risk assessments in repair station oversight; sharing information with air carriers; and upgrading training requirements for certain repair station personnel. *See* Margaret Gilligan, Deputy Assoc. Adm'r for Aviation Safety, *Statement Before the Senate Committee on Commerce, Science and Transportation, Subcommittee on Aviation on the Federal Aviation Administration's Oversight of Foreign Aviation Repair Stations* (June 20, 2007), https://www.transportation.gov/content/federal-aviation-administrations-oversight-foreign-aviation-repair-stations [https://perma.cc/YRU5-VXYB].

on safety while the TSA is tasked with security.[132] By bifurcating safety and security between two agencies with different organizational structures, missions, and cultures, repair station oversight has been left at a standstill with the FAA being unable to certify new repair stations or impose new security measures due to the TSA's nearly decade-long failure to comply with Congressional instruction to issue the necessary security regulations.

Although the FAA implemented procedures in 2008 and 2009 to improve information sharing, modify inspection documentation requirements with foreign aviation authorities, develop a process to capture results from foreign aviation authority inspections and FAA inspections, and modify procedures for conducting sample inspections,[133] it is difficult to see how the FAA can effectively carry out its safety mandate and effectively inspect repair facilities without action by the TSA.

In addition, the cooperation of foreign aviation authorities and air carriers is also critical. In 2003, for example, French, German, and Irish aviation authorities monitored 138 FAA-certified repair stations while FAA inspectors provided oversight for 512 FAA-certified foreign repair stations.[134] In 2011, the focus of FAA and European oversight of repair stations remained on ensuring cooperation on aviation safety.[135] However, oversight also needs to address insider threats by integrating security as a component of safety. The problem is how to do it cost-effectively without crippling the U.S. aviation industry while simultaneously obtaining global participation of and enforcement by foreign sovereigns.

Further complicating the issue of oversight is the existence of satellite repair stations. While the certified main repair station may be domiciled in one country, it may have satellite repair stations located inside or outside of its geographic boundaries.[136] For example, if an Airbus A380 aircraft operated by American Airlines from Honolulu has a maintenance issue which grounds the aircraft in Singapore, American Airlines may send it to a contract repair facility in Singapore. That Singapore-

---

[132] Vision 100, *supra* note 96.

[133] 2009 Foreign Repair Station Update, *supra* note 124.

[134] 2003 DOT IG Report, *supra* note 130, at ii.

[135] AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND THE EUROPEAN COMMUNITY ON COOPERATION IN THE REGULATION OF CIVIL AVIATION SAFETY (June 30, 2011), https://www.state.gov/documents/organization/169475.pdf [https://perma.cc/7C53-9SJA].

[136] 8900.1, *supra* note 121, § 2-1245.

based facility may be either carrier-certified, FAA-certified or Original Equipment Manufacturer (OEM)-certified. Even if it is an FAA-certified repair station, some work may be shipped to a non-FAA certified satellite repair station which has excess capacity in Singapore, or to an Airbus-certified OEM maintenance facility in a French territory such as Reunion.

As repair station personnel may be interchanged with other personnel anywhere in a repair station's (or a carrier's) satellite network, it is possible for qualified and unqualified personnel from different facilities to work on or have access to an aircraft, engine, or component undergoing maintenance at a foreign repair station and to have access to technical and operational information. From a chain of custody or inspection oversight perspective this can be problematic. Additionally, it is very risky from a security perspective. Because carriers pool parts and equipment, it is possible that an aircraft with four engines could have four different repair facilities work on the engines registered to the aircraft (none of which may actually be installed on the aircraft) and any engines in the maintenance pool (any of which may be actually installed on the airframe) while another facility works on the airframe and other facilities perform work on components or spares. Pooling and personnel interchange arrangements, while cost effective for carriers, complicate security and introduce multiple points at which an insider may sabotage an aircraft or gain access to sensitive information which can be exploited for altruistic or nefarious purposes. For example, a pooled engine that had been sabotaged by a mechanic could be installed at random on an appropriate airframe.

In 2009, the TSA issued a notice of a proposed rule which would "codify the scope of TSA's existing inspection program and . . . require regulated parties to allow TSA and [DHS] officials to enter, inspect, and test property, facilities, and records relevant to repair stations."[137] Further, the rule would "provide procedures for TSA to notify repair stations of any deficiencies in their security programs, and to determine whether a particular repair station presents an immediate risk to security."[138] While the draft rule would require FAA-certified repair stations to implement a TSA-devised security program to mitigate the risk of being targeted for terrorist activity, the program would allow for variation in security measures for "those repair stations

[137] 49 C.F.R. §§ 1520, 1554 (2009), at 59874.

[138] *Id.*

with a lower risk profile, such as those repair stations not situated on or adjacent to an airport or those repair stations located on airports that only serve aircraft with a maximum certified takeoff weight of 12,500 pounds or less."[139]

Despite the need for consistency in application and rigorous oversight, the proposed rule creates two significant areas that are vulnerable to exploitation. First, the TSA will consider a repair station to be in compliance if it is already incorporated within an airport's security program and uses the airport's access control measures.[140] Second, repair stations located at facilities for which the United States has security responsibilities (e.g., military air fields, government maintenance depots, etc.) would not be required to comply with this rule as such facilities presumptively meet or exceed TSA's proposed security requirements.[141] The proposed rule relies on voluntary compliance and cooperation of industry. It also relies on the aviation industry's willingness to absorb the cost of implementing an unfunded mandate. Assuming industry would be willing to absorb attendant implementation costs, the proposed rule fails to provide standard procedures, training, oversight, and inspection criteria to foreign repair stations.

VI. AIRCRAFT TRUSTS

While foreign repair stations present tangible opportunities for insider exploitation, disruption, and sabotage, aircraft trusts present more subtle opportunities due to their structure, legal legitimacy, and long-standing global use by banks, financial institutions, and manufacturers. As the promotion of commerce and safety are statutory components of U.S. aviation policy, it is not

---

[139] *TSA Aircraft Repair Station Security Proposed Rulemaking*, NAT'L BUS. AVIATION ASSOC. (Mar. 1, 2010), http://www.nbaa.org/ops/security/programs/repair-station/ [https://perma.cc/C79J-DDXH].

[140] Key proposed requirements include descriptions of measures used to identify individuals who are authorized to enter the repair station; measures used to control access and to detect and prevent the entry of unauthorized individuals and vehicles into or within the repair station; measures used to control access to the aircraft and/or aircraft components; measures used to escort and verify any individual's right to enter the facility; training of TSA's security requirements for all individuals with authorized access to aircraft and components; measures used to verify employee background information; the name, 24-hour contact information, duties, and training requirements of a designated security coordinator; a contingency plan; a diagram detailing boundaries and pertinent physical features of the repair station; a list and description of all entry points; and an emergency response contact list. *See id.*

[141] *Id.*

surprising that the provisions of 49 U.S.C. §§ 44102 and 44103 encourage and legitimize foreign ownership and U.S. registration.[142]

A. Trust Structures

For many aircraft purchasers, aircraft finance involves leveraged leasing[143] and trust arrangements. While aircraft trust arrangements with U.S. financial institutions and banks are a legitimate and useful tool in promoting sales of U.S.-manufactured aircraft and promoting aviation safety, their widespread use and minimal due diligence requirements make them vulnerable to exploitation by criminal and terrorist front organizations for various purposes including money laundering and gaining apparently lawful access to U.S. airspace. This cloak of legitimacy makes it possible to introduce people and hazardous or illegal cargo into the continental United States and U.S. territories and possessions.

FAA regulations and trusts intersect when someone seeks to register an aircraft. While an aircraft's owner can apply for registration on the N Registry,[144] an aircraft is eligible for registration on the N Registry only if it is owned by a U.S. citizen.[145] Although the U.S. citizenship requirement presents an issue for foreign owners who wish to register and operate their aircraft in the United States, a simple solution is to form a U.S. company. As companies are legal "persons," the company can be the owner-applicant.[146] A U.S. citizen or resident alien must be a corporate officer with at least seventy-five percent of the voting power, as non-citizens are capped at a maximum twenty-five percent ownership interest; the company's president and at least

---

142 49 U.S.C. § 44102 (2012) (Registration requirements); 49 U.S.C. § 44103 (2012) (Registration of aircraft).

143 A leveraged lease of an aircraft involves a minimum of a lessee, a lessor, and a long-term creditor. The typical aircraft lessees are airlines, charter operators, and corporations. Institutional investors such as banks, insurance companies, and pension plan funds provide the leverage and multiple lenders may be involved in financing a single aircraft transaction. *See* Deborah Brady & Paul Ingram, *A Leveraged Lease Primer—Understanding the Tax and Accounting Treatments of this Powerful Equipment Finance Tool*, Equip. Leasing and Fin. Ass'n (May 2006), http://www.elfaonline.org/cvweb_elfa/Product_Downloads/E06MAYBRADY.PDF [https://perma.cc/Y3T7-35XF].

144 49 U.S.C. § 44103(a) (2012).

145 49 U.S.C. § 44102(a)(1)(A) (2012).

146 *Corporations: An Overview*, Cornell L. Sch. Legal Info. Inst., http://www.law.cornell.edu/wex/corporations (last visited Sept. 1, 2017) [https://perma.cc/WSN9-4JKM].

sixty-seven percent of the company's directors must be U.S. citizens or resident aliens.[147]

By forming a Delaware limited liability company (LLC), the LLC can enter into a trust arrangement with a bank acting as owner-trustee. The LLC-trust arrangement is a well-established legal way for foreign and domestic purchasers of new or used aircraft to effect U.S. registration and operate their aircraft in U.S. airspace. This arrangement facilitates sales of U.S.-manufactured aircraft globally, as well as generating higher resale prices of U.S.-registered aircraft which are perceived as safer to operate and better maintained because of FAA oversight. FAA oversight of N-registered aircraft in turn promotes aviation safety as FAA airworthiness standards are more comprehensive and better enforced than those of many other national registries. As the cost of registration is only $5.00[148] instead of a percentage of the aircraft's value or purchase price, U.S. registration is a bargain. The N Registry provides reliable, efficient, and free access to aircraft and engine title information. In addition, U.S. registered aircraft have the benefit of U.S. legal protections.

B. Vulnerabilities

Because the N Registry does not pierce the corporate veil, foreign owners routinely form LLCs as part of overall trust arrangements. This legitimate practice poses potential problems, as a hostile individual could use a U.S.-registered aircraft to engage in a variety of lawful and unlawful activities within the United States. By purchasing a U.S.-registered aircraft, apart from being a means for laundering large sums of money, the aircraft could be used to ferry hostile agents to and from the continental United States, U.S. territories, or countries which grant U.S.-registered aircraft landing rights once re-registered with FAA. In essence, the aircraft itself becomes the "insider" as it is the means of introducing hostile persons (i.e., owners, passengers, crew) and means (i.e., cargo) into the United States or functioning as a weapon (i.e., crashing into ground/airborne targets; releasing chemical dispersants above cities, watersheds, or crops;

---

147 14 C.F.R. § 47.2(3) (2015).

148 *Aircraft Registry*, Fed. Aviation Admin., http://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/register_aircraft/ (last visited Sept. 1, 2017) [https://perma.cc/8R7F-DSBM].

inducing terror by detonating above a crowd, etc.). In effect, Pegasus[149] can turn into a Trojan horse.[150]

Although the USA PATRIOT Act[151] targets money laundering, it can be used to combat the insider threat posed by opaque trust arrangements. Banks which act as trustees must complete due diligence on all trust beneficial owners, guarantors, equipment lessors, and escrow depositors and recipients for any new trust transaction.[152] However, existing trusts are grandfathered. There are also exemptions to the due diligence requirement. For example, lenders and government agencies or offices are exempt, as are all USA PATRIOT Act-defined financial institutions and their subsidiaries.[153] Lessees are also exempt unless the bank processes payments from them or holds deposits on their behalf.[154]

Exemptions aside, due diligence must be performed on the actual signing party, whether it is a special purpose entity (SPE), corporation, LLC, or partnership. This means a bank must have copies of the articles of incorporation or other official documentation of the existence of any party establishing a trust as a beneficial interest holder.[155] For publicly traded entities, a tax or employer identification number or access to publicly available financial reporting information[156] is required. If the actual signing entity is a parent corporation's wholly- or partially-owned subsidiary, affiliate or joint venture, due diligence must be performed on that entity instead of the parent. For countries identified by the U.S. Department of the Treasury's Financial Crimes

---

[149] Micha F. Lindemans, *Pegasus*, ENCYCLOPEDIA MYTHICA (2001), http://www.pantheon.org/articles/p/pegasus.html [https://perma.cc/KWE3-EQ2V].

[150] Micha F. Lindemans, *Trojan Horse*, ENCYCLOPEDIA MYTHICA (1999), http://www.pantheon.org/articles/t/trojan_horse.html [https://perma.cc/KJ8N-5GEJ].

[151] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism USA PATRIOT Act of 2001, Pub. L. No. 107-56 115 Stat. 272, (2001) [hereinafter USA PATRIOT Act].

[152] U.S. financial institutions are prohibited from establishing, maintaining, administrating, or managing correspondent accounts for foreign shell banks. *See id.* § 313.

[153] 31 C.F.R. § 1010.205 (2012) (defined in 31 C.F.R. § 1010.100(t) (2014)).

[154] *Id.* § 1010.315, 330.

[155] U.S. financial institutions furnishing correspondent accounts to foreign banks must maintain records of the owners of the foreign bank and the name and address of the foreign bank's U.S. agent. *See* USA PATRIOT Act, *supra* note 151, § 319(b); *see also* 14 C.F.R. § 47.8 (2010).

[156] Publicly available information may include audited annual reports, periodic reports filed with the U.S. Securities and Exchange Commission, call reports, stock exchange listing information, etc. *See* 14 C.F.R. §§ 47.7–.8.

Enforcement Network (FinCEN), due diligence extends beyond the SPE level to include individual principals or controlling officers of the SPE, or to the corporate owner of the SPE. For non-FinCEN countries, due diligence stops at the initial SPE level.[157]

While due diligence is designed to tighten up banking loopholes and prevent money laundering, there is no similar national requirement imposed on company formation. Forming a company to facilitate purchasing aircraft is simple and can be done online on an expedited basis in as little as one hour with credit card payment.[158] Once the company is formed, the next step is trust formation. Aviation trusts typically take several weeks to structure. Once the trust aircraft is registered, the trust's owner-trustee is identified on the registry instead of the actual owner.[159] It is difficult to penetrate trust walls to identify an individual. The aircraft's owner of record is more likely to be a corporation than an individual. The citizenship requirement for registration does not impede trust formation or aircraft registration, but rather encourages the use of opaque legal structures such as trusts which make it harder to identify individuals.

Assuming it were possible to identify the corporate owner of an aircraft, that entity could be an affiliate, subsidiary, or joint venture of a parent company. Typically, the names of the president, directors, or shareholders having five percent or more beneficial ownership interest in the company are not listed on the N Registry[160] or in the trust instruments.[161] In addition,

---

[157] Individual beneficial interest holders must provide identification in the form of a U.S. Social Security number (SSN) or taxpayer identification number (TIN) accompanied by a date of birth. For individual beneficial interest holders who do not have an SSN or TIN, individual citizens of FinCEN countries, and individual owners or controlling officers of FinCEN-based SPEs, a legible copy of a passport or other government-issued ID, including country of issuance, type of document, ID number, dates of issuance and expiry, and an identifying photograph must be provided. In addition, all trust beneficial interest holders, lessors, and lessees must provide contact information, including contact name, address, telephone number, and, if available, fax number and email address. *See* 31 U.S.C. §§ 5311-5314e (2012).

[158] *Expedited Services*, STATE OF DEL., DIV. OF CORPS., http://corp.delaware.gov/expserv.shtml (last visited Sept. 1, 2017) [https://perma.cc/L2SD-B2TC].

[159] *N-Number Inquiry Results: N100FF*, FED. AVIATION ADMIN., http://registry.faa.gov/aircraftinquiry/NNum_Results.aspx?NNumbertxt=100FF (last visited Sept. 1, 2017) [https://perma.cc/734H-4GW3].

[160] *N-Number Inquiry Results: N68789*, FED. AVIATION ADMIN., http://registry.faa.gov/aircraftinquiry/NNum_Results.aspx?NNumbertxt=68789 (last visited Sept. 1, 2017) [https://perma.cc/BRX8-UYRC].

[161] *See Notice of Proposed Policy Clarification for the Registration of Aircraft to U.S. Citizen Trustees in Situations Involving Non-U.S. Citizen Trustors and Beneficiaries*, FED.

these individuals are not necessarily signatories to the trust documents or the sole users of the aircraft. Even if those individuals were identified on the registry, listing their names does not make an aircraft, airline, or the national airspace any safer from insider activities. If anything, listing individual owners or corporate officers and directors online may make them (and/or their families) targets of identity theft, kidnapping, fraud, or other crimes. Furthermore, identifying such individuals does not necessarily correspond to who an insider may be. It is possible a friend, business acquaintance, employee, contractor, or family member could be the insider who takes advantage of the opportunity presented by his association with the aircraft's owner. It is also possible an insider could be a banker, lawyer, aircraft broker, aircraft safety inspector, or any other person involved in the purchase, trust formation, or registration process. There is no reliable way to predict the likelihood that a person who is a U.S. citizen, resident alien, or foreign national would use an aircraft trust or registration to do something harmful inside the United States, to its people, or to its interests.

Viewing trust vulnerabilities from the perspective of legal and financial access, a banker or an attorney could be pressured to access client information for purposes contrary to their duties as fiduciaries. They could also manipulate trust and registration documents for purposes of aiding and abetting criminal or terrorist activities. Insiders who are bankers or lawyers could use their insider status either against or for a trust beneficiary's interests as they are in the position of drafting the legal instruments, gathering information, and obtaining executed signature pages necessary to complete trust formation and to effect registration. For example, a banker could furnish a scanned copy of a valid signature to a third party who could then use it to obtain false identification documents or to authorize fund transfers for a parallel transaction for an alter ego entity which could then be used to acquire an aircraft in order to subsequently smuggle weapons, transport terrorist cell members, or be loaded with enough ammonium nitrate-fuel oil to level a building.

With over 357,000 aircraft registered on the N Registry as of July 20, 2010,[162] there are numerous opportunities to exploit the

---

AVIATION ADMIN. (2011), https://www.faa.gov/about/office_org/headquarters_offices/agc/special/aircraft_registration_proposed_policy_clarification/media/Federal%20Register%20Notice%202.9.12.pdf [https://perma.cc/EY8U-X8SA].

[162] Re-Registration and Renewal of Aircraft Registration, 14 C.F.R. pts. 13, 47, 91 (2010), at 41977.

three-year re-registration requirement established in July 2010.[163] For a variety of reasons including lack of awareness, changes of mailing address and sales of registered aircraft, approximately 100,000 aircraft registered before October 1, 2010, are expected to not renew their registrations. Due to the time and expense entailed in terminating and revoking registrations and the institutional reluctance to terminate the registration of someone who may have moved and simply failed to update his contact information on file with the N Registry, the FAA publishes an expired and pending cancellation report.[164] An enterprising individual could take advantage of that published information to "renew" a lapsed registration and then use that registration number on a similar make and model aircraft, thus cloaking it with legitimacy and enabling it to fly to, from, or within U.S. airspace.

VII. POTENTIAL PROBLEM AREAS AND SOLUTIONS

While the insider threat has always existed, how it is addressed is important as it not only affects national security, but serves as a reflection of our societal values. Three areas which raise potential problems for repair stations and trusts include insider threat countermeasures, private sector contracts, and growing complacency.

A. Insider Threat Countermeasures

While the FAA is not an intelligence agency per se, it provides vital aviation intelligence[165] and aviation-related information to DHS and other intelligence community members while also functioning as a liaison to the aviation community. Balancing statutory and constitutional rights with countermeasures against perceived insider threats raises the ante, particularly as applied to whistleblowers, due process, and employee privacy.

---

[163] *Id.* at 41968.

[164] *See Expired/Pending Aircraft Registration Cancellation Results*, Fed. Aviation Admin., http://registry.faa.gov/AircraftRenewal_reports/PendingCancel_Inquiry.aspx (last visited Sept. 1, 2017) [https://perma.cc/S58H-GQEP].

[165] The FAA has an Office of Intelligence, which is a consumer of raw and finished information from law enforcement and intelligence agencies. Its twenty-four-hour watch operation is also responsible for fusion analysis and reporting. *See Statement of Claudio Manno to the National Commission on Terrorist Attacks Upon the United States*, National Commission on Terrorist Attacks Upon the United States (Jan. 27, 2004), http://govinfo.library.unt.edu/911/hearings/hearing7/witness_manno.htm [https://perma.cc/6DD3-6VM8].

While the FAA has a legitimate interest in safeguarding classified information, controlling access to FAA facilities, ensuring safe operations within U.S. sovereign airspace, and adherence to FAA requirements by repair stations, it must also exercise sound discretion and independent judgment within legal limits. For example, if in the course of routine monitoring or inspections an FAA employee determines that another employee or a contractor has been accessing sensitive or classified information outside the scope of his normal duties (or reporting or leaking information which was accessible because of his normal duties), the natural reaction would be to plug the leak by suspending, firing, detaining, or arresting the individual. However, as federal employee jobs are considered property,[166] the employee cannot be arbitrarily suspended, fired, demoted, or removed from his position. He is entitled to procedural due process as "[n]o person shall . . . be deprived of life, liberty, or property, without due process of law."[167] Specifically, the employee is entitled to notice of the proposed action and a meaningful opportunity to respond.[168] If the employee is a bargaining unit employee, that compounds the problem because federal employee labor unions such as the National Air Traffic Controllers' Association have contractual rights to be informed of management actions and to represent their interests and as well as those of their members.[169] If the employee is not afforded due process and properly handled, the FAA could be ordered to reinstate him and exercise proper due process measures if it wishes to terminate him lawfully.

To prevent future leaks, understanding the employee's rationale is important. If that employee leaked information about a recurrent failure of an avionics component (or an inspector whitewashing safety records or security lapses of a repair station) out of frustration because his efforts to report the problems up the chain of command were ignored (or he was labeled a troublemaker and blacklisted after doing so), that may explain why he published his claims on a blog, Twitter, or in the media. If the FAA sought adverse action against him after he published

---

166 Portman v. County of Santa Clara, 995 F.2d 898, 904 (9th Cir. 1993).

167 U.S. CONST. amend. V.

168 Cleveland Bd. of Educ. v. Loudermill, 470 U.S. 532, 542–45 (1985).

169 Laura Brown & Doug Church, *FAA and NATCA Reach Landmark Labor Agreement*, NAT'L AIR TRAFFIC CONTROLLERS' ASSOC. (Aug. 13, 2009), http://www.aviationpros.com/press_release/10398368/faa-and-natca-reach-landmark-labor-agreement [https://perma.cc/3S45-HJ5B].

his allegations, he could potentially invoke whistleblower protection.[170] In addition to media scrutiny, congressional inquiry, and a DOT Office of Inspector General (OIG) investigation, the FAA could also face unfair labor practice claims, arbitration with federal employee labor unions, and third party lawsuits. The cost and resources dedicated to defending the agency and ousting the insider are a distraction, which diverts resources from the FAA's mission and erodes morale.

Countermeasures, such as computer monitoring or close supervision and scrutiny of an employee's or a contractor's activities, can also backfire due to overzealous enforcement, prejudice, or ignorance. For example, an overzealous inspector (or security employee or IT manager) could single out employees and contractors at repair stations and the N Registry for computer monitoring or closer scrutiny and supervision because of their perceived ethnicity (or recent overseas travel, access to sensitive information, personal animus, or other reasons). Without probable cause or a reasonable suspicion of wrongdoing, that inspector (or security employee or IT manager) who acts on his gut instincts (or who overreacts to threat reports) could trigger equal protection,[171] First Amendment,[172] and privacy[173] claims against the FAA. In addition to the attendant embarrassment, stress, and negative impact on morale and the mission that the parade of horribles would have on the agency, the FAA could potentially lose some or all or its statutory independence from DOT[174] or have its funding slashed by Congress.

To prevent arbitrary actions and overzealous enforcement, the FAA could take several cost-effective steps which would improve insider threat awareness and minimize the risk of scandal and expense of legal action. The FAA could conduct annual in-person and/or online whistleblower training for current manag-

---

170 49 U.S.C. § 42121 (2012).

171 As the Fourteenth Amendment applies to the states, federal government actions that discriminate against protected classes of individuals implicate Fifth Amendment due process rights. *See* U.S. CONST. amends. V, XIV § 1.

172 U.S. CONST. amend. I.

173 *Order 1280.1B, Protecting Personally Identifiable Information (PII)*, FED. AVIATION ADMIN. (Dec. 17, 2008), https://www.faa.gov/documentLibrary/media/Order/1280.1B_.pdf [https://perma.cc/9V5W-P4AA]; *see also* U.S. CONST. amends. IX, XIV, § 1; Griswold v. Connecticut, 381 U.S. 479, 483 (1965).

174 *See* H.R. REP. No. 104-848, at 105 (1996) (Conf. Rep.) ("Section 623 amends section 106 of title 49, United States Code, to provide the FAA Administrator express autonomy and authority with regard to the internal functioning of the agency.").

ers and employees. This training would be provided to new hires as part of the onboarding process, while first-time managers would be required to complete training within thirty days of promotion. It could also use annual FAA employee survey feedback to improve whistleblower and fraud hotline reporting systems and ensure employees view them as a responsible and responsive mechanism for reporting their concerns confidentially within FAA channels. In addition, FAA managers and employees should receive annual insider threat training utilizing case studies and best practices of other agencies and private industry so that they understand what constitutes an insider and the evolving nature of the threat.

As for certified repair facilities, they should be required to provide proof of annual employee insider threat training (e.g., course sign-in or training logs) and current security procedures as a condition of certification. To minimize labor issues related to employee discipline, the FAA should work with federal employee labor unions to develop expedited review procedures for alleged insider actions and a table of appropriate penalties. To ensure widespread awareness of the insider threat, the FAA could use its employee website to publish periodic articles on insider threats and countermeasures.

Complementing employee threat awareness measures, managers should be encouraged to address and elevate employee concerns, tips, and questions regarding possible safety and security issues. Furthermore, employees and managers should be educated on their right to seek counsel from the FAA Office of General Counsel (OGC) and be encouraged to seek OGC guidance before undertaking actions affecting employees and contractors in order to ensure that the prospective actions and means to accomplish them comply with agency guidelines and U.S. law. If EO 13587 and NSD 42 were harmonized, the FAA would be named an ITTF permanent member agency and serve in similar capacity as it does on the steering committee established by NSD 42. Finally, the FAA should coordinate with Treasury, the Securities and Exchange Commission, and DHS regarding banking and financial regulations which affect transparency of aircraft trusts.

B. Private Sector Contracts

Apart from the risk posed by insider activities at repair stations and trust companies, there are collateral opportunities to exploit their vulnerabilities. For example, the FAA contracts

with numerous companies to provide services and products to support operations, including maintaining the N Registry records database and repair station certification records and inspection reports. It is likely a portion of the FAA's 2014 budget of approximately $15.6 billion[175] will be spent on contracts for goods and services related to repair stations and the N Registry, including a portion of the $77 million budgeted for technical support.[176] It is possible that a contractor supporting either operation could engage in overzealous conduct in a well-meaning attempt to further FAA efforts to combat insider threats.

It is also possible that if the FAA utilizes "enterprise insider threat software package"[177] spyware such as that solicited by TSA to enable it to combat insider threats by monitoring "the emails, chat, web browser history, and even the keystrokes of its employees"[178] and contractors, that a contractor could use his skills and access to gather competitive business intelligence or to thwart enforcement efforts.

Another possibility is such spyware could have backdoor ports which would enable the FAA, or another agency such as the NSA, to monitor and exploit repair station and bank internal correspondence and databases. If FAA contractors were to use spyware to hack into bank or repair station systems in an effort to combat perceived insider threats, it could give rise to claims for breach of contract and violations of foreign data privacy laws as well as espionage if the foreign repair station were owned by a state-owned company. If discovered, such data mining would create a global scandal and severely damage U.S. foreign relations.

Apart from the constitutional issues posed by electronic snooping highlighted by the unfolding NSA data collection scandal,[179] and the yet-to-be-determined extent of contractor involvement, all government agencies use contractors to perform

---

[175] *Budget Highlights, Fiscal Year 2014*, DEP'T. OF TRANSP., at 9 (Feb. 12, 2013), http://www.dot.gov/sites/dot.dev/files/docs/FY%202014%20Budget%20Highlights.pdf [https://perma.cc/HQ5B-D6NY].

[176] *Id.* at 13.

[177] Steve Watson, *Congress Presses TSA To Crack Down on "Insider Threats" from Its Own Employees*, INFOWARS (Oct. 5, 2012), https://www.infowars.com/congress-presses-tsa-to-crack-down-on-insider-threats-from-its-own-employees/ [https://perma.cc/7HSG-2UKP].

[178] *Id.*

[179] Barton Gellman & Ashkan Soltani, *The NSA's Problem? Too Much Data: NSA Collects Millions of Email Address Books Globally*, WASH. POST (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-

functions which are not inherently governmental. The line between what is an inherent governmental function[180] and functions "closely associated"[181] with inherent governmental functions can blur when it comes to technical and intelligence contracts.

While the FAA employs contractors to assist with myriad tasks, faced with shrinking budgets and time pressures, there is a tendency for work to be delegated to contractors which may cross the line into inherently governmental functions. There is also the potential for conflicts of interest to arise by virtue of access and opportunity, whether through use of spyware or by virtue of job function. Contractors may gain access to proprietary data, information, and technologies of rival companies as well as FAA assessments of capabilities which could give these insiders a competitive advantage in upcoming contract solicitations.

To prevent overreaching, mission creep, and delegations which violate federal law and agency regulations, the FAA's internal oversight and inspection programs must be robust, visible, and regularly updated. In addition, functions currently performed by contractors which were previously performed by federal employees (or which could be readily assumed by federal employees) should be performed in-house by federal employees to the maximum extent feasible. To further minimize insider threat risks posed by contractors, a robust acquisition integrity program such as the Department of the Navy's[182] should be integrated within FAA's OGC. Because contractors are not federal employees, FAA employees and managers need to understand the limitations on information which can be shared with contractors as well as activities which can be performed by them. To do so, annual training should be implemented agency-

---

mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?utm_term=.2da9088f4ac0 [http://perma.cc/5A3T-WKJS].

[180] Federal Activities Inventory Reform Act of 1998, Pub. L. No. 105-270, 112 Stat. 2382, Sect. 5(2) (Oct. 19, 1998); *see also Policy Letter 11-01, Performance of Inherently Governmental and Critical Functions*, OFF. OF FED. PROCUREMENT POL'Y, OFF. OF MGMT. AND BUDGET (Sept. 12, 2011), http://www.gpo.gov/fdsys/pkg/FR-2011-09-12/pdf/2011-23165.pdf [https://perma.cc/V58W-GSLM].

[181] Jacob B. Pankowski, *New Definition of "Inherently Governmental Function" Affects Government Insourcing Decisions*, NAT'L L. REV. (Sept. 24, 2011), http://www.natlawreview.com/article/new-definition-inherently-governmental-function-affects-government-insourcing-decisions [https://perma.cc/MD3P-A26B].

[182] *Acquisition Integrity Office*, DEP'T OF THE NAVY, OFF. OF THE GEN. COUNSEL, http://www.secnav.navy.mil/OGC/AIO/Pages/default.aspx (last visited Sept. 1, 2017) [https://perma.cc/4FC4-DSD3].

wide for all managers. Furthermore, in each notice of solicitation and contract award over the $150,000 simplified acquisition threshold,[183] a contract requirement should be included which requires contractors to certify that their employees received training (at no expense to the government) on conflicts of interest, inherent governmental functions, and insider threats.

C. Complacency

Arguably, complacency is the biggest problem any agency faces when combating a known threat. After an attack, security violation, or OIG inspection, employees and managers have a heightened sense of vigilance. However, the "sense of vigilance for and priority attached to tight security can dissipate with the passage of time from a terrorist event; this, in turn, may lead to a sense of complacency as well as pressures to relax security."[184]

To prevent the insider threat from becoming stale, it is important to keep employees and contractors informed of successes and failures of other agencies, private industries, and the FAA. One way to do so is to recognize the contributions of alert employees and contractors who act lawfully and use the proper channels to report activities which safeguard FAA resources and the flying public. Even if names of individuals must be withheld or some information redacted for privacy, national security, or legal reasons, summaries of successes and failures should be published on the FAA employee website. A series of well-told stories and articles highlighting different kinds of insider activities can do more to combat complacency and educate employees and contractors than countless memoranda, posters, and notices on proper and improper ways to correct problems and ensure integrity FAA-wide. Threat awareness must remain fresh and catch the imagination of the audience.

VIII. CONCLUSION

Foreign repair stations and aircraft trusts serve valuable legitimate commercial and operational purposes. While safety and security are different issues, they are related. The insider threat should be addressed rationally, consistently, and comprehensively. As the NITP is not a single policy, where there are discrepancies, such as between EO 13587 and NSD 42, they should

---

[183] 48 C.F.R. § 2.101 (2017).

[184] DOT IG Statement, *supra* note 57, at 5.

be harmonized. How the insider threat is addressed is important given the FAA's high level of public trust and visibility.

As the FAA is a civil, military, and economic target, national aviation security policy must involve the FAA. At a minimum, the FAA should be part of the ITTF, particularly since commercial aviation was and will remain a target of terrorists. International cooperation is crucial to combat threats and vulnerabilities of foreign repair stations as well as aircraft trusts. Domestic cooperation is vital; therefore, the TSA cannot unilaterally fail to issue rules relating to foreign repair stations, but must work with the FAA instead of against it. The FAA and the TSA share security interests which affect aviation safety and should act in concert to address security issues relating to foreign repair stations. Similarly, DHS must work collaboratively with the FAA on aircraft trusts to look beyond money-laundering to prevent wolves from wearing sheep's clothing.

Foreign repair station certification is in the national interest, not just because of its impact on aviation safety and its importance to our economy, but because it is a global aviation security issue. Aircraft trusts are also in the national interest as they serve legitimate commercial purposes and promote sales of U.S. aircraft. However, the USA PATRIOT Act can be used to combat the insider threat if due diligence loopholes are plugged.

The areas which raise potential problems for foreign repair stations and aviation trusts are threat countermeasures, private sector contracts, and complacency. Countermeasures must be judiciously applied using discretion and independent judgment. They cannot be arbitrary and must address the root cause, particularly with respect to employee leaks. They cannot be overzealous hip shots or they will backfire with far-reaching consequences. Private sector contracts can create potential issues as contractors may act overzealously to counter perceived threats and the tools employed may be used inappropriately. Apart from being a source of potential insider activity, use of contractors could result in mission creep. The most insidious problem is complacency as it is human nature to relax one's guard over time, thus creating new opportunities for insiders. By exercising sound judgment and educating its employees, managers, and contractors, the FAA can maintain aviation safety and security without jeopardizing its culture or undertaking draconian measures.

While the insider threat cannot be completely eradicated, the FAA can limit the opportunities of insiders to exploit foreign

repair stations and aviation trusts. The policy and statutory framework of executive orders, national security directives, and IRTPA shape the FAA's ability to combat insider threats. By understanding the history and structure of repair stations and trusts, the FAA can develop effective countermeasures. The openness which is part of FAA and aviation culture is a strength which can be leveraged to combat the insider threat through recognition and publication of successes and failures in addition to regular training and access to counsel.