NATIONAL STRATEGY FOR AVIATION SECURITY

of the United States of America

DECEMBER 2018

THE WHITE HOUSE

WASHINGTON, DC

My fellow Americans:

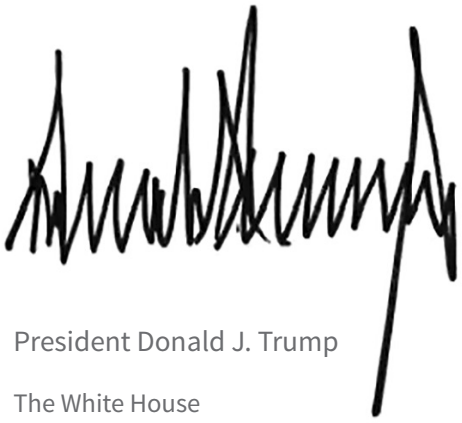
Since 2007, the National Strategy for Aviation Security (NSAS) has been the overarching framework for implementing a comprehensive and integrated approach to protecting the aviation domain, and enabling aviation-related activities to remain a vital component of our Nation's economy. Our enemies, however continue to view aviation as a key target, and the Aviation Ecosystem faces a multitude of threats and ever changing tactics that are challenging to overcome. The past decade has seen the rise of technologies that generate economic and social benefits, but also may be used to challenge the safety and security of the Aviation Ecosystem. The use of "disruptive technologies," such as cyber connectivity and unmanned aircraft, in reckless or malicious ways, along with the constant evolution of terrorist threats to manned aviation, requires a fresh, whole-of-community approach.

Consistent with the President's National Security Strategy, this new NSAS focuses first on protecting the United States and its interests. It broadens the scope of potential threats to, or disruption of, the Aviation Ecosystem beyond the previous more narrow focus on terrorist groups, criminals, and hostile nation states to also include insiders, foreign intelligence activities, and the spread of infectious disease via air travel.

The new NSAS directs a holistic and adaptive approach to securing the Aviation Ecosystem that prioritizes enhanced domain awareness, collection of anticipatory information, augmentation and sustainment of layered security measures, improved system resilience, and effective engagement with government and private-sector partners. The NSAS underscores the importance of, and recognizes the interdependent roles of, Federal, State, and local authorities, the private-sector, and international partners to securing the system and facilitating aviation safety and commerce.

This NSAS aims to enhance the safety and security of the Aviation Ecosystem, preserving the freedom of operations for legitimate pursuits and facilitating American prosperity. To accomplish this objective, the United States must execute a coordinated, integrated, and layered effort to protect the American people and the homeland while enabling American economic dynamism.

Sincerely,



President Donald J. Trump

The White House
December 2018

Table of Contents

Introduction

The threat landscape has changed significantly since NSPD-47/HSPD-16 directed the development of the NSAS. The past decade has seen the rise of emergent technologies, including cyber, unmanned aircraft, and spectrum-dependent systems that generate economic and social benefits, but also challenge the safety and security of the Aviation Ecosystem. While safety can be built into the system by conscious design to prevent accidents or errors, security exists within an ever-changing competition with those who intend to do harm to the system. These evolving "disruptive technologies," along with on-going traditional threats, require a new concerted approach from the Global Aviation Community of Interest[1] to ensure the safety, security, and prosperity of the Aviation Ecosystem.

Aviation-related activities currently represent approximately 5 percent of our Nation's gross domestic product (GDP) and are forecasted to grow with the advent of advanced technologies.[2] This dynamic landscape requires the United States to develop and sustain a persistent, layered methodology to protect this vital resource. Furthermore, the Aviation Ecosystem supports public sector, homeland security, and continuous and on-demand military air operations to defend and prevent disruption to the Nation.

The Aviation Ecosystem faces a complex and diverse set of threats, and our adversaries seek to exploit the Aviation Ecosystem for nefarious purposes. Terrorists, criminals, and hostile nation-states understand well the importance of aviation to our domestic economy and they will continue to view aviation as a key target. Aviation is a particularly desirable target for terrorists, as an attack on a manned aircraft is a dramatic event that can harm or kill large numbers of people and garner terrorists the notoriety they seek. Since the attacks of September 11, 2001, the world has witnessed numerous terrorist attacks and attempted attacks that employ diverse methods that challenge our ability to detect and react with a timely response.

1 The Global Aviation Community of Interest (GACOI) includes: the Intelligence Community (IC); Federal, State, Local, Tribal, and Territorial (FSLTT) departments and agencies; law enforcement; international partners; private sector; and academia. *Unifying Intelligence Strategy for Aviation Issues (UIS-A), 2017*.

2 Advanced technologies include: global positioning service-based technology, system-wide information management programs, unmanned aircraft systems, and flight tracking.

Vital United States National Interest

The United States priority interests in aviation security are to 1) protect the homeland, the American people, and the American way of life; and 2) promote American prosperity.

Desired End-State

A safe and secure Aviation Ecosystem that preserves the freedom of operations for legitimate pursuits and promotion of American prosperity is the desired end-state. The United States operates a coordinated, integrated, and layered system to anticipate, detect, deter, prevent, and defeat the threat to the Aviation Ecosystem, and respond when necessary.

Assumptions

The United States confronts a diverse collection of adversaries that continually seek to exploit the Aviation Ecosystem for their nefarious purposes.

As the United States prospers from the advancement of emerging technologies such as cyber connectivity and unmanned aircraft systems, our Aviation Ecosystem will enjoy new opportunities and face new vulnerabilities that will require a continuously adaptive and holistic approach to mitigation and resilience.

No single mitigation effort is invulnerable to exploitation by our Nation's adversaries, but a well-coordinated, layered, whole-of-community approach will help mitigate threats and ensure a resilient Aviation Ecosystem.

Because of the complexity and global nature of the Aviation Ecosystem, responsibility for preventing, responding to, and, if necessary, recovering from attacks extends across all levels of government, and private and public sectors.

Obstacles and Challenges

The size and complexity of the Aviation Ecosystem generates a variety of threat vectors that our enemies can and do manipulate.

The threat posed by terrorists to the Aviation Ecosystem will continue to change in form and intensity as terrorists' intentions and capabilities evolve. In response to countermeasures, terrorists adapt their techniques, including modality of planning, complexity of attack, and style of execution.

Emerging threats, including malicious cyber actors, threats from insiders, malicious or reckless use of unmanned aircraft and other Non-Traditional Aviation Technologies (NTAT)[3], sophisticated explosives, and transnational criminals, pose the greatest challenge to the entire Aviation Ecosystem.

Current Environment

Examples of attempts to bring down airliners include the underwear bomber (2009)[4], the printer cartridge bomb plot (2010)[5], the

3 NTAT are defined as low-altitude and slow-speed aerial vehicles, including small unmanned aircraft systems, and ultralights that may be purpose-built or commercially available and typically do not require licensed pilots to operate.
4 The underwear bomber attempted to detonate an improvised explosive device (IED) hidden in his underwear while on board Northwest Airlines Flight 253 from Amsterdam to Detroit in December 2009.
5 The printer cartridge bomb plot involved shipment of two packages containing IEDs concealed in printer cartridges bound from Yemen to the United States, which were discovered in route in October 2010.

thwarted underwear bomb plot (2012)[6], the Khorasan Group's development of explosive small electronics (2014)[7], and the personal electronic device threat (2017)[8]. Transnational criminal organizations (TCOs) also exploit the Aviation Ecosystem to traffic in drugs, weapons, humans, and other contraband, while aviation insiders have facilitated some of the successful attacks on aviation such as the attacks on Daallo Airlines (2016)[9] and MetroJet (2015).[10]

While the cyber realm has yet to be fully exploited by terrorists and other non-state actors, the United States continues to see their interest in the systems and networks associated with the Aviation Ecosystem. Nation-states have already conducted cyber attacks and cyber espionage against Aviation Ecosystem targets. Executive Order (E.O.) 13800, of May 11, 2017, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, calls for departments and agencies to use available authorities and capabilities to support the cybersecurity risk management effort of the owners and operators of the Nation's critical infrastructure, including aviation infrastructure.

Attacks from users within the Aviation Ecosystem continue to pose an ongoing threat. The potential use of an aircraft for hijacking and as a weapon remains a danger, as does the prospect of using civil aviation as a delivery system for chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) weapons. In addition to taking advantage of aviation security gaps, bad actors will continue attempts to exploit the legal governance features of the aviation system that facilitate legitimate travel and commerce for nefarious purposes.

Threats

The Aviation Ecosystem faces a complex and diverse set of threats. Globalization, the potential malicious or reckless use of unmanned aircraft systems (UAS), CBRNE materials, malicious cyber activity, terrorist ideology, and the growing phenomenon of Homegrown Violent Extremism (HVE) have enabled threats to the Aviation Ecosystem to extend in reach and impact. There are six main originators of threats in the Aviation Ecosystem:

Terrorists

Terrorists have demonstrated clear intent and capability to harm the United States and its global interests and remain a severe threat to aviation. Terrorists' continued interest in attacking the Aviation Domain has been demonstrated by the al-Shabaab attack on Daallo Airlines (2016) and the attack on MetroJet Flight 9268 in Egypt (2015), for which ISIS claimed responsibility. Both of these attacks were assessed to be the work, in part, of radicalized insiders. Additionally, the catastrophic attacks at Brussels and Istanbul airports (2016) demonstrate terrorists' intent and capability to attack public areas of airports, which could influence Homegrown Violent Extremists to select similar targets.

Terrorists are taking advantage of the same

6 The thwarted underwear bomb plot of 2012 was intended to destroy a United States-bound airliner using an underwear bomb similar to that used in 2009.
7 The Khorasan Group plotted in 2014 to develop explosive small electronics intended to bring down a commercial airliner.
8 The personal electronic device (PED) threat of 2017 involved terrorist intent to target commercial aviation through explosives placed in PEDs.
9 The attack on Daallo Airlines Flight 159 from Mogadishu, Somalia to Djibouti in February 2016 involved a bomb detonated on board the aircraft, a plot which was facilitated by airport insiders.
10 MetroJet Flight 9268 from Sharm El Sheikh, Egypt to Saint Petersburg, Russia in October 2015 disintegrated in flight following detonation of a bomb, a plot which was facilitated by airport insiders.

tactics, techniques, and procedures (TTPs) pioneered by criminals to counter immigration, customs, and border security measures to move people and materiel. Globally, terrorists also use unsecured aviation transportation routes to transport arms, explosives, money, or operatives clandestinely to safe havens, training sites, or attack-staging locations. Ultimately, terrorists could use these access points and routes to transport more dangerous cargo, including weapons of mass destruction (WMD) and their associated components.

Hostile Nation-States

While most countries have an explicit interest in being able to operate safely, effectively, and reliably in the Aviation Domain, some pose threats due to hostile acts that cause intentional or unintentional consequences (e.g., 2014 downing of Malaysia Air Flight 17 over Ukraine). Some countries directly sponsor international terrorism by providing training, funding, supplies, and materials that could be used to manufacture WMD and related components and operational direction to terrorist surrogates. Nation-states also wittingly or unwittingly provide safe havens for terrorists to plan, prepare, or facilitate attacks, or deploy illicit materiel or operatives through the Aviation Ecosystem. Further, both Iran and North Korea operate airlines that have been identified by the United States for their roles in terrorism and/or proliferation.

Additionally, some nation-states present a military threat to the United States or may seek to exploit the Aviation Domain for intelligence collection purposes. Nation-states are increasingly viewing offensive cyber capability as a means for advancing military, political, and economic objectives. These capabilities have been used for cyber espionage against United States targets, including those in the Aviation Ecosystem. Some nation-states may create a direct or indirect risk to civil aviation by not adequately de-conflicting civil and military activity, such as from test missile launches, GPS interference, or operations in support of combat.

Criminals

Recent disruptions of criminal organizations smuggling weapons and drugs through our Nation's airports with the assistance of insiders reveal the need for continued vigilance. Transnational Criminal Organizations (TCOs) and other criminal affiliates routinely seek out the assistance of sympathetic or willing aviation insiders to facilitate the movement of illicit goods or people. It is possible that TCOs could unwittingly work with terrorist organizations despite the potential negative impact to or disruption of their facilitation networks. However, the vulnerabilities exposed through the actions of aviation insiders who are involved in criminal activities may also be exploited by individuals affiliated with terrorism.

Criminals have employed cyber techniques to target aviation-related companies to commit financial crimes and employed UAS for smuggling and Intelligence Surveillance and Reconnaissance. Criminals who commit cybercrimes have targeted aviation-related networks and websites. The capabilities and motivations of these types of actors make it hard to predict their targets and the impact of their activity. Moreover, the anonymity of cyber criminals makes attribution of their activities extremely difficult.

Insiders

Insiders pose a particular threat because of their proximity to and knowledge of the Aviation Domain. An insider is an individual with access or insider knowledge that can be exploited or

that would allow them to exploit the vulnerabilities of the Aviation Ecosystem. Insiders include personnel employed by governments, airports, airlines, and other aviation stakeholders, including vendors, suppliers, and sub-contractors that may have unescorted access to aircraft or secure areas in airports or in sensitive locations off airports. The Transportation Security Administration estimates there are approximately 1.8 million workers with access to secured areas and other security identification display areas, sterile areas, or air operations areas at United States airports. Additionally, foreign and domestic airport authorities are uncovering radicalized individuals with authorized access to aircraft and other flight operation nodes which presents potential security concerns.

In the international environment, terrorist groups such as ISIS, al-Qa'ida in the Arabian Peninsula, and al-Shabaab have used aviation insiders to carry out attacks against targets. These attacks heighten concern about the viability of such tactics and the need for the development of adaptable mitigation strategies.

Foreign Intelligence Activities

Hostile or suspect nation-states and other foreign intelligence entities are developing insights into the workings and vulnerabilities of the Aviation Ecosystem because of its complexity, relative openness, and the challenges of enforcing existing requirements. This growing capability enables them to collect information on the Aviation Domain. Hostile nation-states and other intelligence entities use the Aviation Ecosystem to conduct intellectual property theft that costs untold sums of money and creates profound threats to our national security.

The Spread of Infectious Disease via Air Travel

Recent international outbreaks of Zika (2016), Ebola (2015), and pandemic H1N1 influenza (2009) demonstrate that fast transportation creates an extensive diffusion route for communicable disease. Indeed, epidemiologists consider transportation, and particularly air transportation, a disease vector because the structure of the Aviation Domain can shape how far and how quickly disease can spread. The Centers for Disease Control and Prevention, in coordination with other United States Government stakeholders and as appropriate with the private sector[11], and the 2013 National Strategy for Pandemic Influenza provide guidance to the aviation sector on travel health measures with the potential to slow the spread of communicable diseases. Nonetheless, responsible governmental authorities and other aviation actors around the globe apply varying degrees of rigor in the enforcement of and compliance with public health measures, including special procedures related to infectious diseases.

Emerging Disruptive Technology/Risk

Cyber Connectivity within the Aviation Ecosystem

The aviation industry, like all business sectors, is working to enhance efficiency by increasing the connectivity of its networks and operations, but this consequently increases the vulnerabilities of its systems. The aviation industry is delivering network-based services such as broadband communications access and in-flight entertainment and Wi-Fi to customers. Industry is also connecting aircraft systems, such as communications and navigation; airport systems, such as screening equipment, physical security

11 The private sector is defined as entities and persons, including for-profit and non-profit, that are not part of any government. *DHS Instruction 2464-01-013*.

controls, electronic maintenance manuals and flight bags, and passenger information displays; and airline business networks, such as reservation systems and on-line check-in websites. In addition, UAS frequently operate through command and control systems that could potentially be vulnerable to hacking and cyber attack.

Increasing Reliance on Radio Frequency (RF) Spectrum and Ability to Degrade Use

Aviation infrastructure depends on the availability of a broad range of spectrum used for communications, position finding/navigation, timing, and surveillance. Further, as the air navigation system (ANS) moves away from traditional land-based navigation systems to rely on space-based technologies such as GPS, the Aviation Ecosystem may become more vulnerable to purposeful interference. Aviation infrastructure involves command and control, and communications systems. The RF spectrum is one common component for each of the four domains in most traditional aircraft: air-to-air, ground-to-air, air-to-ground, and ground-to-ground. Given the centrality of the RF spectrum to aviation operations, the United States Government must take steps to safeguard its use, including physical security measures and technical measures to prevent jamming and spoofing and to enable authentication, as well as cybersecurity considerations. Moreover, the increased use of computer and RF spectrum-dependent systems in the Aviation Ecosystem opens opportunities for degradation of systems and interoperability issues as well as adversarial attacks upon those systems.

Proliferation of Unmanned Aircraft Systems

The dramatic growth of UAS use globally can be traced to a few factors: low cost, ease of use, and practical utility. The Federal Aviation Administration (FAA) forecasts annual United States sales of hobbyist and commercial small UAS to be 7 million units annually by 2020 – and by 2024, the FAA estimates annual domestic sales will top $9 billion. Bloomberg Technologies estimates that by 2020 the global UAS market will be $127 billion. From both a recreational and commercial perspective, UAS applications will grow along with the technology. As manufacturers improve the capability of their systems to operate beyond line of sight (BLOS), which is also known as beyond visual line of sight (BVLOS), enhance their power, payload, cargo configuration, increased weight enhancements, endurance, and perfect autonomous pre-programmed operations, their applications will be limited only by the user's imagination.

While most of the operators of these systems are engaged in legitimate activity, the risk of an irresponsible or malicious actor using the system is increasing. UAS have been used to fly drugs, money, and weapons over our Southern border and smuggle contraband into prisons. Reports of unauthorized UAS operating near airports are also on the rise, potentially creating a hazard to manned aircraft. Small UAS can be controlled from a handheld terminal, a mobile phone, or a laptop computer; can perform precision pre-programmed flight routines; and can hold position, orbit, swarm, or follow waypoints autonomously. They can be modified to carry an explosive payload, as effectively demonstrated by certain terrorists overseas on the battlefield. UAS also provide effective platforms to conduct illicit surveillance and to infiltrate nearby computer networks via the cyber domain. UAS can pose additional security concerns to include vulnerabilities from command and control messaging to/from the UAS and transport and communication of data from the UAS, such as streaming video or sensor data.

Strategic Objectives

In keeping with the principles from NSPD-47/HSPD-16 and other National strategies, and in accordance with the values enshrined in applicable law, the following four objectives will guide the Nation's aviation security activities:

1. Protect the United States and its Global Interests in the Aviation Ecosystem

The United States and its global interests must be protected through the detection, deterrence, and prevention of terrorist, criminal, and hostile acts, whether by physical, spectrum-based or cyber means across the Aviation Ecosystem. The security of the United States depends on the security of the Aviation Ecosystem's critical infrastructure, including physical, spectrum-based and cyber networks. Beyond the immediate casualties, the consequences of an attack on a node of critical infrastructure may include disruption of entire systems or significant damage to the economy. Parts of the Aviation Ecosystem's critical infrastructure also function as critical defense infrastructure, the availability of which must be constantly assured for deployment of military forces and for national security operations worldwide. Protection of infrastructure networks must address individual elements, interconnecting systems, and their interdependencies in both the physical and cyber domains.

2. Maximize Aviation Ecosystem Security while Maintaining Aviation Safety and Balancing United States Economic Impact

The Aviation Ecosystem demands extremely high standards of security be implemented in an efficient manner. Security measures should be balanced with the safe and efficient movement of cargo and people, economic and market-based factors, and protection of individuals' privacy and civil liberties. Maintaining transparency in the planning effort and promoting dialogue will help increase the effectiveness of risk mitigation actions and reduce burdens on the private sector. The United States must ensure the safety and security of the Aviation Ecosystem while maximizing prosperity related to the growth of technologies such as unmanned aircraft and spectrum-based systems.

3. Enhance Resilience, Mitigate Damage, and Expedite Recovery

The United States must take actions to mitigate damage and expedite recovery from an attack on the Aviation Ecosystem. Exercising and strengthening national mitigation and recovery plans while simultaneously maximizing coordination within the Aviation Ecosystem are the keys to effective recovery. The United States must develop scalable response options to ensure a resilient and quickly recoverable transportation infrastructure that minimizes adverse security and economic effects (e.g., isolation of particular portions of the Aviation Transportation System (ATS)).[12] When an incident occurs, FSLTT

12 The term "Aviation Transportation System" is defined as, "U.S. airspace, all manned and unmanned aircraft operating in that airspace, all U.S. aviation operators, airports, airfields, air navigation services, and related infrastructure, and all aviation-related industry." *NSPD-47/HSPD-16*.

departments and agencies along with private sector entities should be prepared to implement contingency procedures to ensure continuity of operations, essential public services, and the resumption or redirection of civil aviation activities, including the prioritized movement of cargo to mitigate the larger economic, social, and potential national security effects of an incident.

The Federal Emergency Management Agency (FEMA) coordinates the Federal Government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror. The National Cyber Incident Response Plan and other applicable policies will guide response to a cyber incident.

4. Effectively Engage International, Domestic, and Private Sector Partners

Ensuring the safety, security, and prosperity of the Aviation Ecosystem requires active engagement among FSLTT departments and agencies, the private sector, and international stakeholders. Transparency, open dialogue, and intelligence and information sharing are vital for success. Effective coordination will engender support for improved global aviation security while furthering United States Government policies and goals. Through these domestic and international efforts, the United States can encourage implementation of appropriate physical and cyber safety standards and security measures, maximize collaborative planning, and coordinate operational responses to incidents throughout the global aviation community.

Strategic Actions

In order to maintain a safe, secure, efficient, and prosperous Aviation Ecosystem, the United States will:

1) Maximize Domain Awareness

Maximizing Aviation Domain awareness is critical to deterring and preventing terrorist attacks, protecting the United States and its global interests in the Aviation Ecosystem, and mitigating the effects of an attack. The United States must integrate air surveillance data, all-source intelligence, law enforcement information, and relevant open-source data from the public and private sectors, including from international partners. Domain awareness is heavily dependent on advanced information collection, analysis, and sharing of that information. Domain awareness requires unprecedented cooperation and action among the public and private sectors while ensuring adherence to laws and policies protecting privacy and civil liberties. The United States Government will maximize its capability to detect, identify, classify, track, and engage where necessary aviation threats from large commercial aircraft to low-altitude, low-observable manned or unmanned aircraft operating to, from, or within the United States and its territorial airspace, or in other airspace of national security interest to the United States.

2) Anticipate Threats and Assess Vulnerabilities to and from the Aviation Ecosystem

A lack of anticipatory intelligence and process inconsistency led to varying responses to aviation events such as the printer cartridge bomb plot (2010), attempted underwear bombers (2009 and 2012), and the insider attack on Daallo Airlines

(2016). The United States Government will anticipate and identify threats, vulnerabilities, and emerging capabilities and will generate a unified response through a standardized process, including through the Aviation Operational Threat Response supporting plan, well in advance of a crisis. The United States Government will identify intelligence and information gaps and will develop courses of action to close or mitigate the impact of those gaps. The United States will also identify gaps in existing crisis management frameworks and develop and implement appropriate solutions to close them. Finally, the United States Government will improve intelligence and collection analysis support and dissemination to domestic and international aviation stakeholders.

3) Strengthen Layered Aviation Security

Using diverse and complementary security methods, public and private sector entities must act in concert rather than relying on a single-point solution. Together, as one integrated system, risk-based security measures create resilience against expected and unexpected risk. This layered security deters attacks by continually disrupting an adversary's deliberate planning process. The implementation of a new security layer must strike a balance between cost and risk, both in absolute terms and relative to other possible measures. It also must comply with applicable law and protect individual's privacy and civil liberties.

The United States Government will further integrate and align aviation security activities into a risk-based, cohesive national effort. These initiatives will include enhancing capability and procedures to detect, interdict, deter, and defeat threats to the Aviation Ecosystem, including through: technological enhancements to screening of passengers and cargo; measures to combat insiders with malicious intent; enhancing capacity to identify and respond to cyber vulnerabilities and threats; enhancing risk-based screening and vetting of passengers and crew; and improving coordination to address security challenges associated with the reckless or malicious use of UAS in the National Airspace System.

4) Ensure Continuity and Promote Resilience of the Aviation Domain

The United States will be prepared to maintain vital commerce and defense readiness in the aftermath of a physical or cyber attack or other similarly disruptive incident that may occur within the Aviation Ecosystem. Threats to and from the Aviation Ecosystem are dynamic and adaptive; therefore, prevention and protection efforts cannot be relied upon to prevent all attacks and other disruptive incidents. The United States Government will update existing contingency plans for responding to, recovering from, and reconstituting after an attack or other disruptive incident and will develop new plans to address emerging threats, as necessary. Such plans will include identification of the steps necessary to prevent the recurrence of a similar event and will address any recovery gaps to ensure a comprehensive and integrated national effort. The United States Government will also enhance emergency preparedness, including through pre-staging of resources as necessary and coordinating exercises.

5) Enhance International Cooperation

Enhancing international cooperation is a critical enabler for protection of the United States and the Aviation Ecosystem against terrorist attacks and criminal or hostile acts. The United States will work with foreign partners to improve

global aviation security equal with or exceeding United States standards. The United States will cooperate with foreign partners to enhance international standards and best practices, and to align regulation and enforcement measures. This will include initiatives pursued through international organizations that include private sector participation. The United States Government will enhance information sharing and collaboration on aviation threats and risk mitigation planning. The United States Government will also promote implementation of systems for the use of advance passenger information, passenger name records, watchlisting, and biometrics.

Tasked Supporting Plans

The NSAS articulates the Nation's aviation security strategic objectives and actions, while the supporting plans provide additional details and context for achieving those objectives pursuant to the legal authorities and missions of the departments and agencies charged with implementing the Strategy. Consistent with roles outlined in NSPD-47/HSPD-16, the plans have designated agencies responsible for the administrative management and coordination of the plans, including monitoring implementation. These agency designations have been updated to correspond better with current department and agency roles and responsibilities. These agency designations do not confer a lead role with respect to operational activities under the plans.

Aviation Operational Threat Response Plan (AOTR)

The AOTR directs the coordination of the United States Government response across the aviation operational response spectrum, from emerging, specific, and credible threats, to immediate incident response, to post-incident review and lessons learned.

Departments and agencies with administrative responsibility: Department of Homeland Security (DHS) and Department of Justice (DOJ)

Other agencies: Department of State, Department of Defense (DOD), Department of Transportation (DOT), Department of Energy (DOE), Office of the Director of National Intelligence (ODNI), and DHS SLTT

Aviation Transportation System Security Plan (ATSS)

The ATSS builds upon the existing scalable, flexible, and adaptable aviation security system through clear delineation of departmental roles and responsibilities and by directing specific actions using a well-coordinated approach to enhance security systems.

Department with administrative responsibility: DHS

Other agencies: State, DOD, DOJ, DOT, DOE, and ODNI

Aviation Transportation System Recovery Plan (ATSR)

The ATSR defines a suite of strategies to mitigate the operational and economic effects of an attack on the Aviation Ecosystem as well as measures that will enable the Aviation Transportation System (ATS) and other affected critical government and private sector aviation-related elements to recover from an attack or incident as rapidly as possible.

Departments with administrative responsibility: DHS and DOT

Other departments and agencies: State, the Department of the Treasury, DOD, DOJ,

Department of Commerce (DOC), and ODNI

Aviation Domain Awareness and Intelligence Integration Plan (ADAII)

The ADAII serves to enhance the United States Government's capacity to obtain effective knowledge of the threats to the United States and its global interests in the Aviation Domain, including the ability to detect and collect information on aviation threats, integrate and analyze that data in conjunction with associated intelligence and information, and disseminate the resulting understanding.

Departments and agencies with administrative responsibility: ODNI and DOD

Other departments: State, DOJ, DOT, and DHS

International Man-Portable Air Defense System (MANPADS) Threat Reduction Plan (IMTR)

The IMTR addresses as its main priority the immediate threat posed by MANPADS that are already out of government control and either in the possession of terrorists and other non-state actors of concern or readily available via illicit (e.g., black market) sales.

Department with administrative responsibility: State

Other departments and agencies: Treasury, DOD, DOJ, DOT, DHS, ODNI, and the National Counterterrorism Center (NCTC)

Domestic Outreach Plan (DO)

The DO outlines a comprehensive engagement strategy that ensures the interests of FSLTT departments and agencies, nongovernmental organizations, and private sector partners are considered in aviation security policy actions, as appropriate.

Departments and agencies with administrative responsibility: DOT and DHS

Other departments and agencies: State, DOD, DOJ, DOC, and ODNI

International Outreach Plan (IO)

The IO sets forth a strategy to promote close cooperation with foreign partners, international and regional organizations, and the private sector to solicit international support for an improved global aviation security framework.

Departments and agencies with administrative responsibility: State and DHS

Other departments and agencies: DOD, DOJ, DOC, DOT, and ODNI

APPENDIX A: ROLES AND RESPONSIBILITIES

The entities below have roles and responsibilities that fulfill executive orders or statutory responsibilities for Aviation Domain activities. Given the unique operating environment of the Aviation Domain, any of these entities may need to perform a specific lead or supporting functional role based on the threat scenario and the outcome desired by the United States Government. In determining whether a specific entity is suitable to perform this role, the following criteria will be considered:

- Applicable law;
- Nature of the threat or incident;
- Desired outcome;
- Response capabilities required;

• Asset availability; and

• Authority to act.

To the maximum extent feasible and appropriate, Federal departments and agencies must coordinate their activities with State, local, tribal, and territorial (SLTT) departments and agencies as well as law enforcement and emergency response agencies, including private sector entities.

Department of Homeland Security (DHS)

In accordance with National Security Presidential Directive-47/Homeland Security Presidential Directive-16 (NSPD-47/HSPD-16), DHS is responsible for closely coordinating United States Government activities encompassing the national aviation security programs, including by identifying conflicting procedures, identifying vulnerabilities and consequences, and coordinating corresponding interagency mitigation actions. Additionally, Presidential Policy Directive(PPD)-21 assigns responsibility to DHS and the Department of Transportation (DOT) to coordinate infrastructure protection activities for the Transportation Systems Sector as Co-Sector Specific Agencies. DHS has assigned Sector Specific Agency responsibility to the Transportation Security Administration (TSA) and the United States Coast Guard (USCG). Other DHS components with related roles include United States Customs and Border Protection, the Science and Technology Directorate, the United States Secret Service, the United States Immigration and Customs Enforcement, the Federal Emergency Management Agency, the Countering Weapons of Mass Destruction Office, the Cybersecurity and Infrastructure Security Agency, and the Office of Intelligence and Analysis. Components that encounter a threat during routine security or law enforcement operations will continue to take those actions within their capacity and authority to control, resolve, or defeat an aviation threat. Per PPD-41, DHS, through the National Cybersecurity and Communication Integration Center and TSA with Sector-specific expertise, is the Federal lead for asset response activities in response to significant cyber incidents. As required by law, DHS, including TSA, will consult with the Federal Aviation Administration (FAA) before taking any action that might affect aviation safety, air carrier operations, aircraft airworthiness, or the use of airspace.

Department of Transportation

The DOT has a wide-range of aviation-related responsibilities. The FAA is a component agency of DOT and is the country's civil aviation authority and air navigation services provider (ANSP). The FAA is responsible for the safety oversight of much of the Aviation Ecosystem, including airlines, other operators, and airports. In its capacity as the Nation's ANSP, the FAA provides a wide range of operational services, including air traffic management and airspace management that enable air traffic operations in United States territorial and delegated international airspace. The FAA is also responsible for the safety of United States operators (including but not limited to air carriers), United States-registered civil aircraft, and FAA-certificated airmen worldwide. In general, the operation of Unmanned Aircraft System (UAS) within the

National Airspace System (NAS)[13] is regulated by the FAA. Under PPD-21, DOT and DHS share responsibility to coordinate infrastructure protection activities for the Transportation Systems Sector as Co-Sector Specific Agencies.

Department of Justice (DOJ)

The Attorney General is the chief law enforcement officer of the United States. In the Aviation Ecosystem, the Attorney General is responsible for prosecuting and, acting generally through the Federal Bureau of Investigation (FBI), investigating all federal crime within the jurisdiction of DOJ, including crimes aboard aircraft. The FBI is also the lead investigative authority for terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. As such, in cooperation with other Federal departments and agencies engaged in activities to protect national security, the Attorney General, generally acting through the FBI, coordinates the activities of other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States, including ground-based tactical response to resolve hijacking, air piracy, and hostage negotiations. Under the supervision of the Attorney General, the FBI is also responsible for intelligence collection, counterintelligence activities, weapons of mass destruction (WMD), cyber investigation, and foreign intelligence sharing under guidelines established in statute and policy. Per PPD-41, DOJ, acting through the FBI and National Cyber Investigative Joint Task Force is the Federal lead agency for threat response activities to significant cyber incidents.

Department of Defense (DOD)

The Secretary of Defense, operating through the Commanders, United States Northern Command (USNORTHCOM), United States Indo-Pacific Command (USINDOPACOM), and North American Aerospace Defense Command (NORAD), is responsible for conducting the defense of the United States (including all United States territory); DOD forces may be directed to engage, using deadly force, of airborne civil aircraft presenting an imminent threat to the United States. Commander NORAD and Commander USINDOPACOM may direct implementation of Emergency Security Control of Air Traffic (ESCAT) in accordance with CFR Title 32, Part 245, to meet emergent threat situations.

Interagency Planning Office (IPO)

The IPO is a joint effort between the DOD, DOJ, Department of Commerce (DOC), DOT, DHS, FAA, Office of Science and Technology Policy, and National Aeronautics and Space Administration in cooperation with the private sector. The FAA established the IPO in May 2014 to coordinate actions across the Federal government to advance the modernization of our nation's air transportation system.

Department of State

State is responsible for coordinating United States Government initiatives that involve foreign governments and international organizations, including regional aviation security cooperation and capacity building. Additionally, State provides foreign policy guidance on the United

13 The National Airspace System is defined as, the common network of United States airspace; air navigation facilities, equipment and services, airports or landing area; aeronautical charts, information and services; rules, regulations and procedures, technical information, and manpower and material. Included are system components shared jointly with the military. *FAA, Pilot/Controller Glossary, April 27, 2017, p.PCG N-1.*

States response to actual or potential airborne threats to the United States. It also conducts global diplomatic outreach and coordination with foreign states to obtain required authorizations for operations and to facilitate United States Government assistance to operational threat response activities within the jurisdiction of those states, when requested. State, in joint coordination with DOT, also has responsibilities with respect to negotiating, approving, and interpreting international agreements, including with respect to aviation security. State engages in diplomatic outreach to press foreign governments and international organizations to raise global aviation security standards and to meet those standards. As outlined in the International Coordination Support Annex of the National Response Framework, State leads coordination and consultations with foreign governments and international organizations following domestic incidents.

Federal Communications Commission (FCC)

FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and United States global territories. An independent United States Government agency overseen by the Congress, FCC is the Federal agency responsible for implementing and enforcing America's communications laws and regulations. It is also charged with regulating and authorizing the use of increasing reliance on radio frequency (RF) spectrum by non-Federal users. This includes, but is not limited to, use of spectrum for UAS and the provision of communications services to commercial passengers, as well as regulating and authorizing the use of RF spectrum, in coordination with the National Telecommunications and Information Administration (NTIA), to avoid or mitigate the risk of interference to Federal users.

Department of Energy (DOE)

DOE plays an important and multifaceted role in protecting national security, including work against the proliferation of WMD. Its national labs provide both subject matter expertise and personnel with unique skills to help understand a wide array of threats and vulnerabilities to the Aviation Domain. Additionally, the National Nuclear Security Administration (NNSA) is the United States Government's primary capability for radiological and nuclear emergency response and for providing security to the Nation from the threat of nuclear terrorism. NNSA coordinates with other agencies whose roles include nuclear or radiological emergency response functions.

Department of Commerce

DOC has broad responsibilities for providing aviation industry and trade policy expertise in interagency policy development efforts and international negotiations, and economic and industry analysis of the impact of domestic regulations (including security-related regulations) and international trade agreements. DOC also administers the United States Export Control System, which governs export of dual-use items, including critical materials and technologies to international aviation suppliers and vendors, and those necessary for aviation security as described under this policy. The export control system also carries out missile technology and WMD counter-proliferation through multilateral agreements. DOC also administers the Defense Priorities Allocations System regulation that ensures timely performance of contracts supporting United States military, homeland security, and emergency preparedness programs. DOC

engages in cooperative efforts on aviation trade and security issues in numerous international bodies and fora, including the International Civil Aviation Organization (ICAO), and the Asia Pacific Economic Cooperation (APEC) forum. DOC also provides the scientific and technical expertise necessary to measure and verify that devices, equipment, and technologies meet or exceed the requirements necessary to maintain and advance the security of the Aviation Domain. DOC provides weather forecast and analysis services integral to the operations of the Aviation Transportation System (ATS). DOC also manages RF spectrum allocation among Federal agencies, including for emergency situations. As part of DOC, NTIA is responsible for regulating and authorizing the use of RF spectrum by Federal users (including Federal UAS operations). NTIA coordinates Federal spectrum uses with FCC to avoid or mitigate the risk of interference to non-Federal users.

Department of the Treasury

The Treasury's Office of Terrorism and Financial Intelligence marshals Treasury's unique financial intelligence, expertise, and authorities to disrupt and disable terrorists, WMD proliferators, and other national security threats to the United States. The Treasury's Office of Foreign Assets Control (OFAC) is responsible for administering and enforcing financial sanctions. As part of this effort, OFAC, in collaboration with partner agencies including the Intelligence Community (IC), investigates for designation or civil enforcement action, individuals or entities that assist in the evasion of United States sanctions, including activities relevant to aviation security. The Treasury's Office of Intelligence and Analysis (OIA) works closely with IC partners to provide intelligence assessments on the acquisition of aircraft, parts, and consumables used by sanctioned entities both domestic and foreign. OFAC and Treasury's Office of Terrorist Financing and Financial Crimes (TFFC) track this activity and work with interagency counterparts to determine appropriate disruption actions. TFFC engages with interlocutors at ministries of finance and intelligence, as well as with law enforcement and export authorities, to share information and urge countries to take action against designated airlines by implementing their own designations; preventing the export of aircraft and parts; detaining shipments meant for designated airlines; and disrupting payments to and from designated airlines. In close coordination with DOC, OFAC also issues licenses authorizing the sale or provision of critical material to international aviation suppliers and vendors. As Administrator of the Bank Secrecy Act, the Financial Crimes Enforcement Network analyzes financial intelligence and alerts appropriate intelocutors about indicators of illicit and suspicious transactions involving aircraft purchases.

Department of the Interior (DOI)

DOI has a role in aviation security through its National Park Service (NPS), the United States Fish and Wildlife Service (USFWS), and the Bureau of Land Management, each of which have cognizance over land that is contiguous with much of the United States northern and southern borders as well as territories such as the Virgin Islands. The NPS Aviation Program provides leadership at the national, regional, and park levels to ensure safe and efficient use of aviation resources. NPS also has extensive security responsibilities for the National Capital Region. DOI's Bureau of Indian Affairs deals with aviation security on tribal reservations as part of its law enforcement responsibilities on trust lands covering approximately 57 million acres, much of

which is along the United States border, as does the Bureau of Land Management and the USFWS.

Office of the Director of National Intelligence

The Director of National Intelligence (DNI) is the head of the IC, principal intelligence advisor to the President, and manages the National Intelligence Program. The DNI:

- Oversees IC analytic efforts to counter threat originators, in coordination with the law enforcement community and international partners;

- Oversees and directs intelligence assessments of pending attacks or other similar disruptions against the aviation ecosystem; and

- Conducts and shares strategic analysis on how threat originators are adapting so that more comprehensive protection efforts can be taken.

As directed by the DNI, the National Aviation Intelligence Integration Office is designated as the National Intelligence Manager for Aviation (NIM-Aviation) in accordance with Intelligence Community Directive 900 and Intelligence Community Policy Guidance 900.2. The NIM-Aviation:

- Leads IC efforts to identify and analyze threats and vulnerabilities to the Aviation Ecosystem, complement surveillance to detect actual threats if and when they materialize, and support other unique missions that promote aviation security;

- Coordinates with FSLTT departments and agencies, the private sector, and international partners to promote a seamless aviation intelligence enterprise architecture;

- Provides IC management on aviation issues, develops and maintains a Global Aviation Community of Interest, works to improve intelligence and information integration throughout that community, and advocates for intelligence priorities while leveraging science and technology to identify new threats, vulnerabilities, and opportunities to strengthen the safety and security of the Aviation Ecosystem; and

- May be directed by the DNI as a National Intelligence Crisis Manager for intelligence integration during an emerging, specific, and credible aviation-related threat stream or post action incident response/lessons learned.

SLTT Departments and Agencies and Law Enforcement

Much of the Nation's aviation infrastructure and law enforcement is owned and operated by SLTT departments and agencies. State governors or homeland security advisors, in addition to local and tribal departments, hold leadership positions to address specific aviation security needs or issues and response. During extraordinary circumstances, the United States Government may assume lead security responsibility. Typically, except for cross-border traffic and matters for which the United States Government has primary or exclusive jurisdiction under applicable law, lead responsibility will remain with SLTT departments and agencies. Specific responsibilities of SLTT departments and agencies are discussed in the National Infrastructure Protection Plan and corresponding Transportation Systems Sector Specific Plan. SLTT departments and agencies must routinely work with the United States Government to identify critical transportation assets, conduct the necessary vulnerability assessments, and develop or revise security plans to protect those assets. The same is required for SLTT

response and recovery capabilities to address terrorist attacks and other disruptive incidents, and to meet the National Preparedness Goal.

Private Sector

Substantial segments of the Nation's aviation transportation infrastructure are owned and operated by private sector entities. As such, an effective national aviation security strategy must be supported by a private sector that internalizes a strong security culture, embedding best practices and government requirements into day-to-day operations. It is the responsibility of private sector owners and operators to conduct and execute business continuity planning, integrate security planning with disaster recovery planning, and to actively participate with FSLTT departments and agencies to improve security in the aviation sector. The United States Government will implement initiatives to build partnerships with the private sector to ensure information sharing, identification of vulnerabilities, and development of strategies to achieve continuous improvement of the Nation's security posture throughout the Aviation Ecosystem.

APPENDIX B: AVIATION ECOSYSTEM

The term "Aviation Ecosystem" refines the term "Aviation Domain" and is intended to include all aspects of Airports, Airlines, Aircraft, Airlift, Actors, and Aviation Management. This term is a more holistic, robust description of the reality of modern aviation and more fully captures the global scope and complexity of the industry and the economic impact it generates. The term underscores the vast, interconnected systems that comprise domestic and international aviation, including civil (both commercial and general) and public aviation. The Aviation Ecosystem Six As (6As) include:

Airports

In the United States, there are more than 19,000 airports of varying sizes, while globally there are nearly 44,000. They can include helipads, commercial air taxi services, logistics hubs, and hubs for package delivery. Generally categorized as civil (commercial and general/private), military, or combinations thereof, airports fulfill specialized functions such as domestic and/or international travel, freight movement, flight training and maintenance/repair/overhaul. In addition to the officials who run an airport, the larger aviation enterprise often consists of an extensive number of vendors who employ a substantial number of people to provide goods and services.

Every airport differs in size, physical layout, and organizational structure, which creates distinct challenges and opportunities to enhance its safety and security. But, while every airport is unique, they all have in common the characteristics of accessibility and public area openness. While these qualities facilitate the movement of people, cargo, and commerce, they also make airports soft targets for nefarious actors.

Airlines

Globally, there are roughly 5,000 airlines with International Air Transport Association (IATA) codes. Some of these airlines are worth billions of dollars, while others operate on a limited budget. They are generally categorized as domestic or international. Moreover, in addition to its aircraft, an airline consists of all the operations, line, and maintenance personnel, as well as the networked systems that enable them to manage their operations and communicate with their aircraft, internally, and with the public. How an airline is managed has an

impact on its safety and the security of the Aviation Ecosystem. Likewise, public and military operators manage substantial daily activities that directly impact aviation safety and security.

Aircraft

Daily, there are more than 2.5 million passengers on nearly 24,000 commercial flights over the United States, not including general aviation and other category flights. Increasingly capable and connected with each successive generation, these aircraft can be aggregated into three general categories: commercial, general/private, and government (including, but not limited to, military). The term "unmanned aircraft" is defined in statute as "[a]n aircraft that is operated without the possibility of direct human intervention from within or on the aircraft."[14]

Airlift

The global economy depends on airlift. The intricate movement of people and a wide array of manifested cargo and mail are critical to the developed and developing worlds alike. According to IATA, air cargo alone accounts for $6 trillion worth of goods, which equals approximately 35 percent of world trade by value. Moreover, commercial airlift is becoming the primary method of transport for deployment of troops and fulfills a vital national security role.

Actors

Actors are people or entities who operate, maintain, or utilize any aspect of the Aviation Ecosystem. The overwhelming majority of actors within the ecosystem are capable, professional, and trustworthy. However, given that the ecosystem generates trillions of dollars annually, it attracts nefarious actors. Nefarious actors may also seek to exploit other, unwitting actors to further their ends.

Aviation Management

Aviation Management encompasses all aspects of the national and international regulation, operations, and administration of the Aviation Ecosystem. Aviation Management is complex, with many stakeholders that service the operation of various sectors in the Aviation Ecosystem to facilitate the safe, open, legitimate freedom of movement and free flow of commerce.

Aviation Management also includes Air Navigation Services, which are the suite of operational services that the United States and other countries provide to aircraft to enable safe and efficient flight from one destination to another. These operational services range from air traffic management, including Air Traffic Control, used to prevent collisions and expedite the orderly flow of air traffic, to enabling networks of communications, navigation, surveillance, and automation critical infrastructure.

14 "Unmanned aircraft" is defined in section 331(8) of the Federal Aviation Administration (FAA) Modernization and Reform Act of 2012, P.L. 112-95 (2012), as "[a]n aircraft that is operated without the possibility of direct human intervention from within or on the aircraft." Section 336(c) of the Act defines model aircraft as "unmanned aircraft."