



A-ISAC

Cooperating to Protect Our Skies

Faye Francy, Executive Director
Aviation Information Sharing and Analysis Center

The aviation sector plays such a critical role in the world economy that it has become an attractive target for a variety of malign actor groups. Each year, the air transportation system carries over 2.6 billion passengers and 48 million tons of freight, making it the world's greatest source of international trade, tourism, and economic progress. Aviation's global economic impact (direct, indirect, induced, and tourism catalytic) is estimated at \$2.2 trillion, or 3.5% of global gross domestic product (GDP). Aviation directly employs 8.6 million people and is estimated to support 56.6 million jobs worldwide.¹ The aviation sector includes airlines, airports, air cargo, original equipment manufacturers (OEMs), equipment suppliers, infrastructure providers, service providers, and other companies supporting aviation. These organizations represent a list of prominent targets for those hoping to disrupt, degrade, defraud, or otherwise impact the global economy and world order.

One company's detection of a potential attack may mean another company's prevention of a devastating security breach.

Sectors such as financial services, oil and gas, and electrical power have been targets of choice for organized security campaigns by individuals, criminal organizations, transnational terror groups, and even nation-states. These actor groups know they can maximize the impact of their political statements, their financial gain, and/or the intellectual property stolen if they succeed in attacking such high profile targets. In addition to the thousands of lives lost as a result of the terrorist attacks of September 11, 2001, the three years after the attack saw U.S. air carriers lose over \$44 billion in passenger revenue.² Beyond aviation, the full economic impact of the attacks was estimated to exceed \$100 billion, including consequences for infrastructure, travel, and business, among other sectors.³

Some of today's cyber threat actors conspire globally in their pursuit of technical information and intellectual property for profit and competitive purposes. Other threat activist or "hacktivist" groups specifically aim to disrupt and sabotage critical aviation sector manufacturing and operational processes. It is imperative that the aviation industry strengthen existing safeguards to ensure that appropriate protective measures are in place to address these advanced threats.

Signed in May 1998, U.S. Presidential Decision Directive/NSC-63 (PDD-63)

recognized the potential for critical infrastructures to be attacked, and asked each critical infrastructure sector to establish sector-specific information sharing organizations in order to maintain open channels of communication about current threats and collaborate to forestall potentially devastating attacks. As a result, several sectors formed what are now known as Information Sharing and Analysis Centers (ISACs). These centers strive to improve coordination and protection responses across their given sectors.

In 2003, the National Council of ISACs was formed to improve coordination amongst the ISACs and to address common issues and concerns impacting all critical infrastructures. Today there are over 18 operating ISACs within the National Council. Other critical infrastructure sectors have built their own ISACs as a means of managing risks and minimizing the disruption of cyber-attacks to their businesses. In 2012, the Aviation Sector Coordinating Council (ASCC) chartered the formation of an Aviation Information Sharing Working Group (A-ISWG) to examine the need for an Aviation Information Sharing and Analysis Center (A-ISAC). The A-ISWG charter acknowledged the international nature of aviation and included the participation of international members. There was consensus that the community needed an Aviation ISAC, so seven founding

aviation members joined together and incorporated the A-ISAC as a non-profit organization in September 2014. Understanding that widespread aviation industry participation is critical to understanding emergent threats, A-ISAC is governed by a Board of Directors composed of leaders across the global aviation community.

A-ISAC was developed in consultation with two of the most mature ISACs, the Financial Services ISAC (FS-ISAC) and the Multi-State ISAC (MS-ISAC). The A-ISAC uses sharing and detection experience from across 16 critical infrastructures to establish what is relevant for the aviation sector. ISAC-driven information sharing strategies improve the collective security posture of members: one company's detection of a potential attack may mean another company's prevention of a devastating security breach.

The A-ISAC organization enhances the ability of the aviation private sector to prepare for and respond to security threats, vulnerabilities, and incidents, and to reduce the risks and costs associated with operational disruptions due to nefarious security events. The ability to effectively provide threat intelligence to protect the aviation sector has become an operational requirement for global air transportation stakeholders.

Security is not a competitive business driver, but is essential to the health



of the aviation industry. As a trusted member-driven organization, the A-ISAC offers frequent and relevant products for dissemination. The key feature is the ability to share timely, anonymized, and actionable intelligence among participants across the global aviation industry. Trusted member sharing is conducted in a secure, private manner that fosters collaboration and communication for the mutual benefit of the aviation community. Sharing with any governmental agency or other trusted third party organization on either an anonymous basis or a “for attribution” basis is at the discretion of the member company providing the data.

The A-ISAC also works with the Department of Homeland Security (DHS) as part of their Critical Infrastructure Information Sharing and Collaboration Program (CISCP). This collaboration provides access to the National Cybersecurity Communications and Integration Center (NCCIC), a top secret facility for sharing omni-directional threat intelligence across public and private sectors. The CISCP mission is to improve the defense posture of critical infrastructure by sharing a view of current threats and vulnerabilities and providing support for risk detection, prevention, mitigation, and response efforts. The goal of the program is an effective information

sharing framework among trusted partners. The aviation community will work with the government analysts to share timely and actionable threat intelligence in aviation and to provide mitigation actions. Additionally, the Air Domain Intelligence-Integration and Analysis Center (ADIAC) in Annapolis Junction is a pilot to promote a similar activity with a myopic focus on the aviation sector. The ADIAC is hosted by the Transportation Security Administration (TSA) and sponsored by the Office of the Director of National Intelligence (ODNI).

A-ISAC is dedicated to sharing global threat information to better protect aviation companies and the sector as a whole. A-ISAC allows for the dissemination of timely, anonymized, and actionable information between member firms, enabling them to:

1. Share specific threats and/or incidents in real time as they unfold.
2. Understand how to tactically combat threats and implement mitigation strategies.
3. Enhance the aviation sector’s collective knowledge and implement best practices.

The aviation community must take steps to manage business risks and hedge against the impact of unforeseen security events. The fusion of public-private sector threat

intelligence tailored for the unique needs of the aviation community is precisely what the A-ISAC offers. 

Sources

- 1 Air Transportation Action Group (ATAG): “Aviation: Benefits Beyond Borders: When the System Stops Working.” aviationbenefits.org, March 2012. <<http://aviationbenefits.org/media/21253/When-the-system-stops.pdf>>
- 2 Morral, Andrew R., Carter C. Price, David S. Ortiz, Bradley Wilson, Tom LaTourrette, Blake W. Mobley, Shawn McKay, Henry H. Willis: “Modeling Terrorism Risk to the Air Transportation System: An Independent Assessment of the TSA’s Risk Management Analysis Tool and Associated Methods.” Rand Corporation, 2012. <http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1241.pdf>
- 3 Sanger, David E.: “The Price of Lost Chances.” The New York Times, September 2011. <<http://www.nytimes.com/2011/09/08/us/sept-11-reckoning/cost.html>>

About the Author:



Faye Francy is the Executive Director of the Aviation ISAC (A-ISAC), a non-profit organization based in Annapolis Junction, Maryland. Ms. Francy is responsible for establishing, implementing and overseeing the organization’s mission, goals, policies and core guiding principles. Ms. Francy is employed by Boeing Commercial Airplanes (BCA) and on loan to the A-ISAC. Previously, she led BCA’s Cyber ONE engineering team, which is an enterprise-wide Community of Excellence (CoE) group that collaborates across the company focused on leveraging the best of Boeing in the cyber domain.

