CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

TSA CYBERSECURITY AND PATH FORWARD

Carissa VanderMey, Cyber Coordinator

- TSA & CYBERSECURITY

WE DON’T DO IT ALONE

- Achieving cybersecurity for critical infrastructure and transportation providers requires a collaborative effort between government and industry.
- In the U.S., TSA works closely with the Cybersecurity & Infrastructure Security Agency to increase resiliency in the Transportation Systems Sector.
- TSA also works with our industry partners to understand cyber risks and develop practical solutions to reduce risk.

Aviation Cyber Initiative

STRATEGIC OBJECTIVES

- Identify, assess, and analyze cyber threats, vulnerabilities, and consequences within the Aviation Ecosystem through research, development, testing, and evaluation initiatives.
- Engage with Aviation Ecosystem stakeholders on activities for reducing cyber risks.
- Seek potential improvement opportunities and risk mitigation strategies.

- The Aviation Cyber Initiative is a tri-chaired task force chartered by the Department of Defense, the Department of Homeland Security, and the Department of Transportation.
  - The DHS chair position was recently transferred from the Cybersecurity and Infrastructure Security Agency to TSA.
- The ACI Community of Interest is comprised of stakeholders from across the aviation ecosystem including U.S. Federal partners, and industry and international partners.

INTERNATIONAL ENGAGEMENT

- ICAO Cybersecurity Panel – TSA participated in the first meeting of the Cybersecurity Panel and will participate in, along with the FAA who is the head of the USG delegation, in the Panel's two groups – Working Group on Threat and Risk as well as Working Group on Guidance Material – that will advance the Panel's work.
- TSA continues to serve as an observer to European Civil Aviation Conference (ECAC), maintaining a presence in the ECAC cybersecurity meetings and providing input to various working papers.
- Bi-lateral engagements with states on cybersecurity-related best practices and capacity building through engagements with the U.S. Department of State.

Photo Credit: Shutterstock

TSA’s approach to Cybersecurity

- ✓ TSA has authority to “take action the Administrator considers necessary” to carry out security-related responsibilities. This includes authority to prescribe regulations, standards, and procedures, and to issue orders.

- ✓ As such, TSA is building a regulatory framework and is implementing comprehensive strategies aimed at enhancing the cybersecurity posture of all modes of transportation.

- ✓ Over the past several years, TSA has issued Surface Security Directives (SDs) and Aviation Program Amendments requiring actions of certain high-risk transportation owners and operators.

- ✓ In addition to SDs and Program Amendments, TSA also issues Information Circulars (ICs) recommending lower risk owners and operators take similar steps.

Cybersecurity Incident Reporting

UNAUTHORIZED ACCESS

Unauthorized access to an Information Technology (IT) system or Industrial Control System (ICS) that disrupts operations and is the responsibility of the operator to operate and maintain.

DISCOVERY OF MALICIOUS SOFTWARE

Discovery of malicious software on IT systems or ICS that disrupts operations and is the responsibility of the operator to operate and maintain.

OPERATIONS DISRUPTIVE ACTIVITY

Activity resulting in a denial of service to any IT system or ICS **that disrupts operations and** is the responsibility of the operator to operate and maintain.

INCLUDED INFORMATION FOR MANDATED REPORTING

- The name of the **reporting operator entity** and call back number
- A description of the **threat**/incident/suspicious activity
- Actions and/or **mitigation efforts** taken in response
- **Impact** to operator entity or operations

WHAT ARE WE SEEING?

HUMAN ELEMENT

□ Social Engineering
□ Insider Threat

MALWARE

□ Viruses
□ Ransomware
□ Worms
□ Zero Days
□ Trojan Horses
□ Information Stealing

OTHER ATTACK TYPES

□ DDOS
□ Spoofing
□ Cyber Sabotage
□ Supply Chain Compromise

MITIGATION EFFORTS?

Employee Training/Assessments

Access Control

Cyber Supply Chain Risk Management

Vulnerability Management

Authenticate and Encrypt Data in Transmission

Secure Boundaries Between Systems

TSA CYBERSECURITY ROADMAP: CYBERSECURITY IS SECURITY

- The TSA Cybersecurity Roadmap provides a framework for how TSA can operate within the cyber environment, ensure the protection of its data and information technology systems, and ensure the protection and resilience of the Transportation Systems Sector.

- The Cybersecurity Roadmap covers a five-year period and is currently being reviewed to better align TSA's cybersecurity activities in the new regulatory environment post the Colonial Pipeline ransomware attack.

TSA is charged with securing the nation's transportation systems from all threats, which involves **protecting against both cyber and physical attacks**.

The **TSA Cybersecurity Roadmap** aligns with both the **National Cyber Strategy** and the **DHS Cybersecurity Strategy**.

Focus is on the incorporation of cyber threats into the risk assessments for the **Transportation Systems Sector** and increased information sharing among all stakeholders.

TSA CYBERSECURITY ROADMAP

WHAT IS THE GOAL?

TSA will develop and maintain a leadership role, collaborating with international partners as well as other federal departments and agencies, the private sector, and other stakeholders to ensure:

- Cybersecurity risks are effectively managed
- Critical networks are protected
- Vulnerabilities are mitigated
- Cyber threats are reduced and countered
- Incidents are responded to in a timely manner
- Cyber environment is secure and resilient across the Enterprise and the Transportation Systems Sector

FOUR GOALS FOR ACTION

RISK IDENTIFICATION

Goal 1.1: Assess and prioritize evolving cybersecurity risks to TSA and the Transportation Systems Sector.

VULNERABILITY REDUCTION

Goal 2.1: Protect TSA information systems.
Goal 2.2: Protect Transportation Systems Sector Critical Infrastructure.

CONSEQUENCE MITIGATION

Goal 3.1: Respond effectively to cyber incidents.

ENABLE CYBERSECURITY OUTCOMES

Goal 4.1: Strengthen the security and resilience of the cyber environment.
Goal 4.2: Improve management of TSA and TSS cybersecurity activities.

TRANSPORTATION SECURITY ADMINISTRATION

What's next in the U.S. & TSA

- TSA is working on more permanent regulations for pipelines, railroads, and rail transit agencies.
- Evolving nature of cyber threats will require continued information sharing with transportation operators and critical infrastructure owners.
- Investment in secure technologies and human resources to reduce vulnerabilities and increase resiliency.
- Cyber Incident Reporting for Critical Infrastructure Act of 2022
  - Develop and implement in coordination with the interagency, reporting requirements
  - Development of National Cyber Incident Response Plan
  - Coordinate ongoing nationwide campaign against ransomware attacks

THANK YOU