



Australian Government

Department of Infrastructure and Regional Development



Working together: Mitigating cyber security risks in aviation

Shona Rosengren

Office of Transport Security

This Presentation

- Understanding cyber security threats to Aviation
- The role of governments in protecting critical infrastructure from cyber attack
- The role of aviation regulators in cyber security



Aviation Cyber Security - Threats

- Few significant cyber attacks against the aviation sector to date that have endangered life or caused major disruption to aviation systems.
- But the threat landscape is constantly changing.

Aviation Cyber Security - Threats

- There are two categories of possible cyber threats to aviation:
 - Attacks that could result in loss of life or endanger the safe operation of an aircraft.
 - Criminally or politically motivated attacks that cause economic disruption to aviation businesses.

Critical Infrastructure Cyber Defence

- The primary role of governments in cyber security is to ensure public safety and the long-term availability of critical infrastructure.
- Governments will also seek to:
 - Work with the private sector to minimise the impact of cyber-criminality on the economy.
 - Prosecute cyber-criminals.
 - Protect their national interests in cyber-space.

Australia's approach to cyber-security

- The Australian Government's approach to cyber-security is outlined in Australia's Cyber Security Strategy.
- The Australian Cyber Security Centre is a government entity that supports critical infrastructure operators and other businesses to manage cyber threats.



Australia's Cyber Security Strategy

1. A National Cyber Partnership
2. Strong Cyber Defences
3. Global Responsibility and Influence
4. Growth and Innovation
5. A Cyber Smart Nation



The Australian Cyber Security Centre (ACSC)

- Is a trusted source of cyber-security advice for the public and private sector.
- Provides information to industry on cyber threats and vulnerabilities.
- Works with businesses to respond to and manage cyber attacks.
- Builds capability across the economy to manage cyber attacks.



Cyber Security in the Aviation Sector

- The aviation sector is exposed to many of the same threats and vulnerabilities as other critical infrastructure sectors.
- The industry will benefit from much of the same advice and support as other critical infrastructure sectors.
- This presents an opportunity to avoid duplication of functions across different areas of Government.

Aviation Security Regulators in Cyber Security

- The principal role of governments in relation to aviation security is to prevent acts of unlawful interference with civil aviation.
 - This mandate comes from Annex 17 to the International Convention on Civil Aviation.
 - Acts of unlawful interference include those acts that jeopardise the safety of civil aviation.
 - This should be the focus for aviation cyber security.
- For aviation security regulators, responses to cyber security threats need to be balanced with traditional threats.

Aviation Security Regulators in Cyber Security

- Aviation security regulators should work closely with cyber security authorities and regulators for other critical infrastructure sectors to avoid duplication.
- This allows aviation security regulators to leverage existing centres of expertise within government on cyber security.
- This also allows a greater focus on those aspects of cyber security unique to aviation.

Aviation Security Regulators in Cyber Security

- Key roles for aviation security regulators include:
 - Working with international partners and the aviation industry to identify specific cyber threats and vulnerabilities unique to the sector.
 - Ensure that industry has access to appropriate cyber security guidance material.
 - Monitoring the risk of an act of unlawful interference by cyber means and taking regulatory action to strengthen cyber security where necessary.

Questions?

