Australian Government
Department of Home Affairs

Department of Home Affairs submission to the Inquiry into the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024

Parliamentary Joint Committee on Intelligence and Security

February 2025

Table of Contents

Introduction

1. The Department of Home Affairs (the department) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 (TSA Bill), and associated explanatory memorandum.
2. This submission outlines the need for amendments to the *Aviation Transport Security Act 2004*, and the *Maritime Transport and Offshore Facilities Security Act 2003*, and their supporting regulations (transport security legislative frameworks) to ensure Australia's aviation, maritime, and offshore facility sectors (the transport sector) are resilient to current and emerging threats. It also provides an overview of the TSA Bill, including industry consultation and engagement.

Threat environment

3. On 11 September 2001, al-Qaeda terrorists hijacked four commercial aircraft, deliberately crashing two into the upper floors of the North and South Towers of the World Trade Centre complex in New York City, a third into the Pentagon in Washington D.C., and a fourth into an empty field about 20 minutes by air from Washington D.C. 2,977 people from 90 nations were killed[1]
4. Despite Australia having a strong aviation and maritime safety record, September 11 brought to light how much more vigilance was needed to make the transport sector less vulnerable and more secure.
5. To mitigate acts of terrorism in Australia's transport sector, the Australian Government enacted the transport security legislative frameworks, which largely focus on physical threats, within an entity's physical boundary or geographical location.
6. Australia is not immune to terrorist attacks. In 2017, an Australian counter terrorism operation (Operation SILVES) disrupted an attempt to bring down an aircraft using an improvised explosive device. The bomb was hidden inside a meat grinder, which was set to explode mid-flight on an Etihad Airways aircraft departing from Sydney Airport. There was also evidence of plans to conduct a separate attack using a poisonous gas.[2] Two brothers in Sydney, guided by Islamic State operatives in Syria, were later charged and convicted. Their conspiracy, if successful, would have led to the loss of over 400 lives[3] and the largest terrorist attack in Australian history.
7. Over the last 20 years there have been significant shifts in the geo-strategic security environment. While traditional threats such as terrorism continue to exist and challenge Australia, the transport sector is facing new and evolving threats that have been exacerbated by rapid technological advances and issues and events that arise in both Australia and overseas.

[1] 9/11 Memorial & Museum (2024) *9/11 FAQS,* 9/11 Memorial & Museum, accessed 28 January 2025. https://www.911memorial.org/911-faqs#:~:text=Nineteen%20terrorists%20from%20al-Qaeda,the%20Pentagon%20in%20Arlington%2C%20Virginia.
[2] *R v Khaled Khayat; R v Mahmoud Khayat* (No 14) [2019] NSWSC 1817.
[3] Zammit, A (April 2020) *Operation Silves: Inside the 2017 Islamic State Sydney Plane Plot,* Combating Terrorism Center, accessed 28 January 2025. https://ctc.westpoint.edu/operation-silves-inside-the-2017-islamic-state-sydney-plane-plot/.

8. In the Australian Security Intelligence Organisation's (ASIO) Annual Threat Assessment for 2024, Mike Burgess AM, Director-General of Security, advised that the threat environment demands we dedicate more resources to countering espionage and foreign interference.[4] These threats are pervasive, multifaceted and, if unmitigated, could do serious damage to Australia's sovereignty, values, and national interest.
9. In August 2024, Mr Burgess advised that Australia's security environment is degrading and is more volatile and more unpredictable.[5] In reflection of the degrading security environment, ASIO raised Australia's national terrorism threat level to PROBABLE, which means there is a greater than fifty per cent chance of an onshore attack or attack planning in the next 12 months.[6]
10. If there is one thing of which we can be certain, it is that strategic threat environment will continue to evolve. Our regulatory frameworks must be able to evolve, too.

The time to act is now

11. The transport sector is critical in facilitating the movement of people, goods, and services; providing access to employment, education, healthcare, and other social services; and fostering social cohesion and inclusivity. A secure and resilient transport sector directly contributes to Australia's prosperity and unity by ensuring critical supply chains are not disrupted and essential services are maintained, bolstering trade networks and economic growth.
12. If a security threat materialises in Australia, it could result in loss of life, and compromise the reliability, continuity, and security of Australia's transport sector. This would have subsequent adverse impacts for Australia's prosperity and security by disrupting essential services, as well as eroding the public's confidence in government.
13. This is Australia's opportunity to be proactive, rather than reactive; to protect Australia's transport sector by enacting dynamic and modernised transport security legislative frameworks that can adapt to current and emerging threats in a flexible, risk-based and scalable way.
14. The frequency and severity of threats to the transport sector is increasing, with the security and resilience of Australia's critical infrastructure continuously being challenged. Over the past twelve months, we have seen international threats to transport infrastructure. For instance, prepositioning of state based actors on airports and seaports, international sabotage using incendiary devices and a steady pace of motivated actors breaching security-restricted areas or bringing prohibited items through airport checkpoints.
15. Recent global security incidents, such as those outlined below, have exposed and compounded security vulnerabilities within the transport sector. This has created the potential for harm and disruption across the Australian economy.

[4] Burgess, M (2024) *Director-General's Annual Threat Assessment 2024*, ASIO, accessed 28 January 2025. https://www.asio.gov.au/director-generals-annual-threat-assessment-2024.
[5] Burgess, M (2024) *National Terrorism Threat Level*, ASIO, accessed 28 January 2025. https://www.asio.gov.au/national-terrorism-threat-level-2024.
[6] Ibid.

Cyber

16. Volt Typhoon[7] were recent events involving malicious state-sponsored actors pre-positioning themselves within critical infrastructure networks, poised to use their network access for disruptive effects on the United States' communications, energy, transportation systems, and water and wastewater sectors, in the event of potential geopolitical tensions and/or military conflicts.

17. In 2024, the global CrowdStrike IT outage caused significant issues for airports and airlines, including flight cancellations and delays and impacts to internal systems. [8]

18. On 10 November 2023 Australia's second largest port facility operator, DP World, which is responsible for 40% of maritime freight in Australia, was shut down due to a cyber security incident. This impacted the movement of goods in and out of Australia and freight was unable to leave the port until operations commenced on 13 November.

19. The Optus, Medibank and Latitude Financial cyber incidents that occurred in September 2022, October 2022 and March 2023, respectively, shone a spotlight on the ongoing and credible threat to critical infrastructure. Inadequate prevention and response to cyber incidents have a devastating impact on the Australian community. Between these incidents, over 26 million records containing personal and sensitive data have been compromised.[9,10] The impacts of these incidents may be long-term, complex, and have a cascading bearing on daily life and the social and economic wellbeing of communities.

20. There is growing recognition of the extent that malicious cyber actors seek to target critical infrastructure, not just for cyber espionage or intelligence collection but also to pre-position on networks for future disruption of critical functions (likely to be initiated in the event of a major crisis or conflict).[11]

Foreign interference and sabotage

21. In 2024, a series of fires in the air cargo supply chain in Europe demonstrated how foreign interference and sabotage are real and ongoing threats to the aviation sector. While the main focus of the sabotage appears to be disruption to supply chains, there was the real risk that miscalculation could have seen packages combust while on an aircraft in flight, including on a passenger aircraft. In response to the sabotage, several countries, including Australia, introduced additional air cargo security measures to mitigate these threats.

---

[7] Australian Signals Directorate (ASD) (2024) *PRC State-Sponsored Actors Comprise And Maintain Persistent Access To U.S. Critical Infrastructure*, ASD, accessed 28 January 2025. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/prc-state-sponsored-actors-compromise-and-maintain-persistent-access-us-critical-infrastructure.
[8] Marshall, A (19 Jul 2024) *Why the Global CrowdStrike Outage Hit Airports So Hard*, Wired, accessed 28 January 2025. https://www.wired.com/story/crowdstrike-windows-outage-airport-travel-delays/.
[9] Kaye, B (23 Sep 2022) *Australia's Optus says up to 10 million customers caught in cyber attack*, Reuters, accessed 28 January 2025. https://www.reuters.com/technology/australias-optus-says-up-10-mln-customers-caught-cyber-attack-2022-09-23/.
[10] Taylor, J (1 Dec 2022) *Medibank hackers announce 'case closed' and dump huge data file on dark web*, The Guardian, accessed 28 January 2025. https://www.theguardian.com/australia-news/2022/dec/01/medibank-hackers-announce-case-closed-and-dump-huge-data-file-on-dark-web.
[11] Australian Signals Directorate (ASD) (2024) *PRC State-Sponsored Actors Comprise And Maintain Persistent Access To U.S. Critical Infrastructure*, ASD, accessed 28 January 2025. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/prc-state-sponsored-actors-compromise-and-maintain-persistent-access-us-critical-infrastructure.

Critical infrastructure

22. In 2018, the *Security of Critical Infrastructure Act 2018* (SOCI Act) was passed by Parliament[12]. Through iterations of subordinate legislation, the SOCI Act requires all hazards security of Australia's critical infrastructure. Today, critical hospitals, critical electricity assets, and even critical rail freight services have a legislative requirement to mitigate the cyber security, supply chain and natural hazards risks they are exposed to.

23. The transport security legislative framework has not kept pace with the current threat environment and the current legislative security settings for the aviation, maritime, and offshore facility sectors are not aligned with the government's broader position on the protection of critical infrastructure. This creates unnecessary vulnerabilities through inconsistent application of security settings across the economy, resulting in a reduced ability for both industry and government to respond to threats accordingly.

24. The second edition of the Australian Government's Annual Risk Review (the Risk Review) noted the existing gap in security standards between the transport sector and other Australian critical infrastructure sectors is concerning for two reasons[13]:

    a. Critical interdependencies exist between the transport sector and the healthcare and medical sector, the energy sector, food and grocery sector, and the import of geographically concentrated critical goods. Despite private efforts to protect these services from disruption, a compromised transport sector can cease their operations. The transport sector is their weakest supply link.

    b. Adversarial countries and criminals continue to conduct cyber campaigns targeting Australian critical infrastructure. Geopolitical issues are expediting a need for supply chain security and natural hazards are increasing in their frequency and severity. These events disrupt the delivery of critical services across the country, cost millions of dollars, and undermine Australian's security and prosperity.

25. The Risk Review also noted high levels of cyber incidents, ongoing foreign interference, the threat of politically motivated violence, instability in global supply chains due to global conflicts and disruption from severe weather events are the key areas of concern for security of critical infrastructure.[14] In a world where transport infrastructure is integral to the Australian way of life, there is no room for complacency.

How does Australia compare internationally?

26. The International Civil Aviation Organization (ICAO) – the United Nations specialised agency for civil aviation – has introduced standards for aviation cyber security. These require member states, including Australia, to ensure aviation regulated entities identify and protect their critical information and communications technology systems and data from unlawful interference. This Bill will make that a requirement for Australian regulated entities, allowing Australia to meet its international obligations.

[12] Federal Register of Legislation (2023) *SOCI Act 2018*, Federal Register of Legislation, accessed on 28 January 2025. https://www.legislation.gov.au/C2018A00029/2022-04-02/text.
[13] Department of Home Affairs (2024) *Critical Infrastructure Annual Risk Review Second Edition,* Department of Home Affairs, accessed on 28 January 2025. https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2024.pdf.
[14] Ibid.

27. Similarly, the International Maritime Organization (IMO) also sets maritime obligations. As a member of IMO, Australia is required to implement the International Ship and Port Security Code (ISPS Code). The ISPS Code does not outline specific obligations to counter against cyber, supply chain and natural hazards. However, IMO has developed guidance material to assist in mitigating current and emerging threats. This Bill will further support Australia meeting its international maritime security obligations.
28. Australia's transport sectors are not only interconnected to other critical sectors and the Australian economy, but are just as important in the global economy. For this reason, Australia has the responsibility to promote and uphold international standards, as the interlinked nature of international travel and trade makes globally varying security standards a risk for all nations.
29. Many of our international partners have introduced measures that contribute to mitigating all hazard security risks.
    a. **United Kingdom:** The UK's Aviation Cyber Security Strategy (2018-2022)[15] includes frameworks for understanding cyber threats, managing cyber risks, and gives incident reporting guidance and resources to assist the aviation industry in managing and preparing for cyber events. The UK's Department of Transport has an 'all-risks' approach which considers terrorism and natural hazards in addition to cyber security.
    b. **United States:** The US's Transportation Security Administration (TSA) administers cyber security requirements for its regulated entities to ensure entities improve their cyber security resilience and prevent disruption and degradation to their infrastructure. The TSA cyber security requirements align with the international standard of ISO/IEC 27001, which Australia does not currently uphold. The Maritime Transportation Security Act 2002 (US) (MTSA) requires owners and operators of MTSA regulated facilities to analyse cyber security vulnerabilities and provide cyber security mitigation procedures.
    c. **European Union:** Through the NIS 2 Directive, signed in December 2022, EU member states are required to enhance their cybersecurity capabilities for sectors of high criticality, including risk management measures, supply chain security, and mandatory cyber incident reporting.[16] The Directive in the Resilience of Critical Entities 2023 prioritises strengthening the resilience of critical entities, including the transport sector, against a range of threats including natural hazards, terrorist attacks, insider threats and sabotage.[17]

[15] UK Department for Transport and Civil Aviation Authority (2018) *Aviation cyber security strategy*, UK Department for Transport and Civil Aviation Authority, accessed 28 January 2025. https://www.gov.uk/government/publications/aviation-cyber-security-strategy.
[16] European Commission (2025) *NIS2 Directive: new rules on cybersecurity of network and information systems,* European Commission, accessed 28 January 2025. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.
[17] European Commission (2024) *Critical infrastructure resilience at EU-level*, European Commission, accessed 28 January 2025. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

d. **Canada:** In 2009, Canada released their National Strategy for Critical Infrastructure,[18] which committed to implementing an all hazards risk management approach for critical infrastructure, including transport infrastructure, which takes into account accidental, intentional and natural hazards[19]. This was followed by the 2018-2020 Action Plan for Critical Infrastructure[20], which is focused on implementing an all hazards risk management approach.[21]

30. Australia's current transport security legislation needs to keep pace with our international partners and require entities to consider cyber security risks, supply chain risks and other risks to security such as natural hazards.

Transport Security Amendment Bill

31. The TSA Bill ensures the transport sector can adapt and respond to current and emerging threats in a flexible, risk-based, and scalable way. The measures it contains have been developed in consultation with industry and contribute to the following security objectives:
    - a transport sector that is resilient to current and emerging threats
    - an effective system testing program that is risk-based and responsive to intelligence
    - compliance and enforcement frameworks that are robust and fit-for-purpose
    - modern and proportionate regulation.
32. The Bill will significantly contribute to maintaining a secure and resilient transport sector that will have positive benefits on Australia's prosperity and unity by ensuring critical supply chains are not disrupted and essential services are maintained, bolstering trade networks and economic growth, as well as the public's confidence in government.
33. The continued focus on proportionate regulation acknowledges our shared responsibility for security with industry, and ensures both proactive and reactive measures are in place for ongoing protection against current and emerging threats.
34. The department consulted extensively with industry and across government in the development of the reforms, including on the policy approach, the impact analysis, and the contents of the Bill. The department also established a cross-sectoral advisory committee to harness industry's technical and operational expertise on the development and implementation of the reforms. Industry has, on balance, been supportive of the reforms, recognising the need to strengthen Australia's transport security settings.
35. The department will continue to work closely with industry during the implementation of these legislative reforms, through the development of the regulations, and as we progress future stages of the reform agenda.
36. Further information on the measures, including industry feedback, is provided at **Attachment A**.

[18] Government of Canada (2022) *National Strategy for Critical Infrastructure*, Government of Canada, accessed 28 January 2025. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx.
[19] Ibid.
[20] Government of Canada (2018) *National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure,* Government of Canada, accessed 28 January 2025. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr-2018-20/index-en.aspx.
[21] Ibid.

Conclusion

37. A secure and resilient transport sector directly contributes to Australia's prosperity and unity. To ensure the continued reliability, continuity, and security of Australia's transport sector, Australia must strengthen its transport sector security settings to adapt and respond to the evolving and challenging threat environment.
38. The TSA Bill is Australia's opportunity to proactively protect its transport sector and reaffirm the Australian Government is committed to maintaining world-leading transport security settings.

Attachment A: Summary of Measures – Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024

Part 1—Unlawful interference

1. This measure proposes:
    - under the ATSA, unlawful interference will be expanded to include cyber security incidents that have had, is having, or is likely to have, a significant or relevant impact on an aviation asset (including sleeper software).
    - under the MTOFSA, unlawful interference will be expanded to include:
        - cyber security incidents that have had, is having, or is likely to have, a significant or relevant impact on a maritime or offshore facility asset (including sleeper software).
        - putting the safety of a ship at risk by communicating misleading information as well as false information
        - attempted acts of unlawful interference.
    - under the ATSA and MTOFSA, cyber security incidents will be required to be reported
    - under the MTOFSA, reporting requirements will no longer be restricted to acts that are, or are likely to be, a terrorist act.
    - under the ATSA and MTOFSA, the penalty for a failure to report a cyber security incident aligns with the penalty for failure to report other kinds of security incidents within the transport security legislative frameworks. This recognises the significant impact cyber security incidents could have on aviation and maritime entities.
2. The expanded security incident reporting requirements will provide the department with an enhanced ability to understand the trends in the threat environment facing the transport sector.
3. There will be no dual cyber security incident reporting obligations for entities under both the SOCI Act and the transport security legislative frameworks. IPs will only be required to report incidents under the transport security legislative frameworks, where reports will be required to be submitted to both the department and the Australian Signal Directorate's Australian Cyber Security Centre (ACSC).
4. For security incident reporting requirements, further details will be outlined as part of Aviation Transport Security (Incident Reporting) Instrument 2015 and the Maritime Transport and Offshore Facilities Security (Incident Reporting) Instrument 2018 following additional consultation with industry. These changes will be implemented within 12 months of the Bill receiving Royal Assent.

Part 2—Security assessments

5. Currently, under the transport security legislative frameworks, IPs must maintain a security program or security plan (hereafter referred to as security program) that requires them to mitigate against terrorism, and serious crime. This measure amends the transport security legislative frameworks to support the introduction of all hazards security obligations within the ATSR and the MTOFSR. This will include explicit obligations (to be set out in the regulations) for IPs to identify and mitigate risks posed by cyber security incidents, supply chain disruptions, security controlled activities and natural hazards.

6. The Bill introduces the definitions of 'operational interference' and ‘relevant interference’ to give effect to the all hazards security approach. This is essential to extend the risks IPs safeguard against to include a broader range of hazards and threats that could interfere with the availability, integrity, reliability, and/or confidentiality of an IP’s information, operations, or assets. This is intended to capture incidents that do not arise through unlawful means, and incidents that could occur due to negligence or accident, such as supply chain disruptions or natural hazards.
7. Aviation IPs will be required to undertake a security assessment that will form part of their security program. Security programs will be required to identify how the outcomes of their security assessment will be implemented. This approach will also apply to the maritime sector; however, under this measure the security assessment will replace the existing risk context assessment.
8. IPs will be required to provide a yearly statement of compliance to advise whether the security assessment, and the measures and procedures in their security program are within the IP’s agreed risk tolerance and meet the relevant transport security legislative frameworks’ requirements. The statement of compliance will initially be submitted with the security assessment and security program as an overarching assurance. Statements of compliance will then be re-submitted at least annually (within 90 days of anniversary), or when the security assessment or SP are amended, to verify they have been reviewed and are still fit-for-purpose. The Secretary may cancel the approval of a security program which is in force where the IP fails to give the Secretary a statement of compliance.
9. The requirements associated with the all hazards security obligations, security assessment and statement of compliance will be implemented following amendments to the ATSR and the MTOFSR, within 12 months of the Act receiving Royal Assent. IPs will be consulted as part of this process. It is intended for the new obligations to be outcomes-focused and principles-based, to give entities the ability to identify risks and mitigation measures appropriate to their operating environment and size.
10. The department acknowledges this measure will significantly impact security programs and will holistically conduct a review of the security program framework, to understand how we can ensure the legislative settings, policy levers, and internal processes associated with security programs and plans are fit for purpose and continue to be effective.

Part 3—Powers of security inspectors

11. Under the ATSA, system tests are undertaken to identify whether a screening point effectively detects weapons and prohibited items, preventing their carriage into a secure area or cleared zone. System tests assess the effectiveness of aviation security controls, and ensure industry meets the security requirements set out in the regulatory framework, relevant screening notices and their security program.
12. The Bill amends the MTOFSA to introduce system testing in the maritime sector, to test the effectiveness of maritime security controls, and ensure industry meets the security requirements set out in the regulatory framework and their security plan.
13. The Bill will also introduce vulnerability testing in the ATSA and the MTOFSA to fully assess the extent to which vulnerabilities exist within the aviation and maritime sectors. Vulnerability testing is a way to partner with industry to test the limits of capability by having an inspector emulate an adversary who has both the intent and capability to exploit, access, circumvent, or defeat a security system. This is an effective way to expose weaknesses in security systems and identify what improvements need to be made in relation to people, process, technology, and legislation to achieve an effective security outcome.
14. The department will develop the maritime system testing and vulnerability testing programs in consultation with industry. This will allow industry to contribute to the development and shaping of the methods, frequency, and desired outcomes of the programs.

Part 4—Charging of fees

15. This measure will align the charging fee power to issue a security identification card in the ATSA with the MTOFSA, to ensure consistent statutory authorisation.

Schedule 2

Part 1—Infrequent international vessels, dual purpose vessels

16. This measure will streamline the process and ensure regulation is proportionate for Australian ships infrequently travelling overseas in exceptional circumstances. Currently, certain Australian vessels travelling internationally require both an approved security plan and an International Ship Security Certificate (ISSC) granted by the department. This includes domestic vessels, not regulated under the MTOFSA that infrequently travel internationally. This measure will give the Secretary the power to issue the operators of certain ships a ship security plan exception certificate and an ISSC exemption certificate subject to them passing the infrequent overseas voyages test. A ship passes the infrequent overseas voyages test if each overseas voyage undertaken by the ship is undertaken in exceptional circumstances.
17. These amendments will explicitly exclude unregulated Australian vessels from the definition of a security regulated ship – provided they pass the infrequent voyages test – making it possible for unregulated Australian vessels to apply for an ISSC exemption.
18. The dual purpose vessels measure will remove the requirement for ships operating as both a ship and offshore facility to have an offshore security plan. These vessels will only be required to hold an approved ship security plan.
19. The amendments will consider a Floating Product, Storage and Offtake (FPSO) vessel and Floating Storage Unit (FSU) vessel as a security regulated ship, regardless of the function it is carrying out at any given time.

Schedule 3

Part 1—Demerit points

20. This measure will enable the demerit points scheme to be established for the air cargo sector in the ATSR, which will align enforcement options across the aviation sector.

21. Under the new amendments, air cargo entities may be subject to a demerit point system in which certain areas of non-compliance may carry specified demerit points. Accumulation of demerit points for acts of non-compliance may lead to the cancellation of an IP's approval, designation, or accreditation.

22. This allows the regulator to consider an additional scalable enforcement option to address both serious and ongoing patterns of non-compliance and encourage IPs to enhance their security measures and outcomes.

23. The department has committed to consulting with industry to develop what the scheme will look like and how it will work in practice, including:

    - how the department proposes to achieve a fair and equitable scheme given the variation in size, operation, and complexity between organisations and
    - point allocation, review/appeal options, and whether points can be restored.

Part 2—Language modernisation

24. Currently, the transport security legislative frameworks uses two main categories (male and female) to divide humans through the term 'sex.' To comply with community expectations, as well as the Sex Discrimination Act 1984, the Australian Privacy Principles and the 'Australian Guidelines on the Recognition of Sex and Gender' the Government proposes to replace the term 'sex' with the term 'gender.'

25. In practice, this amendment will require screening officers who are undertaking frisk searches, to make reasonable efforts, if practicable, to locate a screening officer of the same gender as the person to be frisk searched. The phrase 'if practicable' will oblige screening officers to make these efforts, but also allow for situations where no person of the same gender can be located.

26. The Bill will also remove reference to the word 'fax' in MTOFSA as an outdated form of communication technology, to ensure the legislation is technologically agnostic.

Part 3—Training requirements

27. This measure will align how training, qualification and other requirements can be prescribed across the aviation sector and ensure cargo examining aircraft operators, should any be approved to operate, are treated consistently with all other aviation IPs.

28. This measure does not impose any new training, qualification, or other requirements for air cargo IPs, and does not change the training requirements that already apply to aviation IPs.

Part 4—Security directions

29. Under the current transport legislative frameworks, the Secretary of the department can issue a special security direction (ATSA) or a security direction (MTOFSA) (hereto collectively referred to as an SD) in response to a defined set of security threats.

30. Currently, in the aviation sector an SD can be issued in response to a change in nature of an existing general threat of unlawful interference, and in the maritime sector, an SD can be issued in relation to a specific threat that is probable or imminent.

31. The threshold for SDs will be amended through the Bill to ensure it evolves with the definition of unlawful interference and the threat environment facing the transport sector. This includes the ability to issue an SD where a specific or general threat of unlawful interference is made or exists or if there is a change in the nature or risk of an existing general threat of unlawful interference. SDs will continue to remain a last resort power used in exceptional circumstances, as noted in the explanatory memorandum of the Bill.

Part 5—Test weapons

32. The Bill will introduce the definition of test weapon in the MTOFSA and amend the equivalent in ATSA, to be 'an item, including a weapon, which either by design or through modification, is incapable of operating as a functional *weapon*.'

33. Using a variety of test weapons that mimic potential attack pathways will ensure that a screening officer can detect a broad range of items to safeguard Australians and the travelling public against unlawful interference.

34. The Bill introduces a regulation making power to prescribe things as test weapons, to improve security outcomes by providing flexibility to include test pieces that reflect new and emerging threats. A regulation making power will reduce any unintended consequences, while allowing the department to remain agile and flexible through the inclusion of new test pieces. Similarly, it aligns with approaches undertaken by other government entities and allows the department to better comply with international obligations.

Part 6—Security regulated ports

35. This measure will amend the definition of 'port', 'security regulated port' and 'port facility' in the MTOFSA to clarify the scope of facilities, functions and capabilities that are contemplated in the definitions.

36. This change will provide clarity for both the department and IPs to ensure additional business critical or supply chain critical assets are protected from an all hazards security perspective and secured within a 'security regulated port' boundary. In recognising the uniqueness of security regulated ports, the definition will capture any other activity that is critical to ensuring the security and reliability of an asset, which reasonably includes ancillary activities such as cyber operation centres, control towers, power stations, or anything that controls operational technology equipment and assets.

37. The department has committed to individual consultation with all entities who will have the opportunity to amend their port boundaries as a result of this measure.