

Guide to Security Incident Reporting Compliance in the Transportation Sector



Explosive growth in the global and domestic transport sector

Throughout the last decade, the global transportation sector has seen explosive growth, with even greater increases forecasted.

Air travel has soared. The sector is on track to double in size over the next two decades. Just the number of employees affiliated with aviation alone is set to increase from 65 million to nearly 100 millionⁱ. Passenger and freighter aircraft is also projected to double from 23,000 to 48,000 by 2038ⁱⁱ. As for the long-term forecast for air passengers: 8.2 billion in 2037 versus 4.4 billion in 2018ⁱⁱⁱ.

Alongside passenger travel has grown air freight. Air freight tasks are expected to grow by 109 percent by 2030 on the strength of just-in-time delivery for manufacturing and mining products, medical and scientific supplies, and perishables^{iv}.

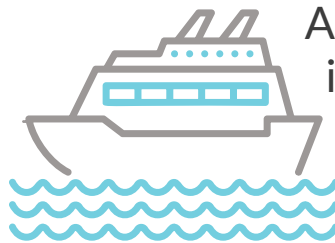
Commerce on the seas is thriving, too. Cargo volumes through Australian ports are expected to double by 2040, owing to a consistent trade in primary exports, goods, and services^v. Meanwhile, the last decade brought double-digit growth to the Australian cruise industry and projections of more growth to come^{vi}.

Number of employees affiliated with aviation alone



is set to increase from **65m** to nearly **100m**ⁱ

The last decade brought double-digit growth to the Australian cruise industry & projections of more growth to come^{vi}



Passenger & freighter aircraft is also projected to double

from **23,000** to **48,000** by 2038ⁱⁱ



Of course, the pandemic has thrown a major spanner in the works. But the most recent industry forecasts have held up. Maritime trade is expected to return to positive growth in 2021^{vii}. The long-term outlook for freight also appears bright^{viii}. And the expected widespread distribution of a COVID-19 vaccine has prompted Australian air titans to deliver optimistic outlooks for domestic operations^{ix}. Even the domestic cruise industry is expected to rebound^x.

The long-term forecast for air passengers is **8.2b** in 2037 versus **4.4b** in 2018ⁱⁱⁱ



The expected widespread distribution of a COVID-19 vaccine has prompted Australian air titans to deliver optimistic outlooks for domestic operations^{ix}



New vectors for attack

While it might be good for the bottom line, the increased patronage of global and domestic routes does create physical security challenges for the transport sector. For one, the sharp fall in consumer demand during the pandemic precipitated mass layoffs across the industry^{xi}. The expected return to record-breaking traffic to and through global airports, aircraft, ports, and affiliated facilities will certainly test the sector’s level of operational preparedness.

Indeed, high levels of domestic and international passenger growth at Australian airports had already tested the capacity of security infrastructure. Last decade, the country’s leading airports, Sydney, Melbourne, and Brisbane, each set passenger records, with the smaller hubs of Gold Coast, Perth, and Darwin seeing even larger net-growth^{xii}.

Of course, this increased passenger growth comes at a time of evolving transport security risk. The prodigious rise in the domestic cruise industry, to take one example, introduces a maritime attack vector, with crowds of passengers and close proximity to favoured targets of high-symbolic resonance^{xiii}.

The 2010s also saw a sharp increase in the number of individuals inspired to conduct small-scale, randomised acts of violence and terrorism. Unfortunately, the transport sector, well populated with civilian targets, has been a perennial favourite.

What’s made these attacks particularly challenging for law enforcement is that their mobilisation now happens with little or no direct contact with terrorist groups. Extremist propaganda has gone online. The consequence has been that threats on transportation targets present more quickly than ever, with no intelligence forewarning^{xiv}.

High-profile Australian transport facilities have already been targets. In 2017, for instance, two men linked to the Islamic State were convicted of a foiled Sydney terrorist attack against passenger aircraft^{xv}.



In 2017, two men linked to the Islamic State were convicted of a foiled Sydney terrorist attack against passenger aircraft^{xiv}

The plot failed when the overweight bag carrying the bomb could not be checked in at the airport. But would it have succeeded, prosecutors argue, 400 passengers would have been killed by military-grade explosives concealed inside a meat grinder.

Security statutes in transportation

Government responded to this foiled bomb plot by upgrading airport security and increasing police powers^{xvi}. Nevertheless, the deteriorating threat climate continues to put pressure on the transportation sector to keep its facilities, customers, employees, and publics safe. Another motivator for the industry is regulatory compliance.

Federal and state governments have long wielded regulatory levers to ensure transport security. One such federal lever is the 2004 Aviation Transport Security Act (ATSA), which creates legal mechanisms safeguarding against unlawful interference with aviation. In the main, the ATSA establishes minimum security requirements for civil aviation, imposing binding obligations on persons engaged in civil aviation related activities.

The Act specifically obligates aviation industry participants to develop and comply with aviation security programs. Another purpose of this Act is to meet Australia’s obligations under the Chicago Convention.

Matching the ATSA on the maritime front is the 2003 Maritime Transport and Offshore Facilities Security Act (MTOFSA), which creates similar legal mechanisms to safeguard against unlawful interference with maritime transport or offshore facilities. Like the ATSA, the MTOFSA establishes a regulatory framework centred around the development of security plans for ships, other maritime transport operations, and offshore facilities. Plans themselves are intended to make appropriate contributions to maritime security objectives, including:



Meeting the country’s obligations under Chapter XI-2 of the SOLAS Convention and the ISPS Code, including those with regard to the rights, freedoms, and welfare of seafarers



Reducing the vulnerability to terrorist attack of Australian ships, ports, and other ships within Australia, as well as offshore facilities



Reducing the risk that maritime transport or offshore facilities are used to facilitate terrorist or other unlawful activities








The effective communication of security information among maritime industry participants and government agencies with security responsibilities for maritime transport and offshore facilities

Mandatory security incident reporting requirements

Perhaps the most critical piece of security information that would need to be communicated among industry participants is notification of security incidents. And to that end, both the ATSA and MTOFSA have made provisions for the timely reporting of security incidents.

Part six of the ATSA imposes an aviation security incident (security incident) reporting mandate on industry participants, including airport operators, aircraft operators, aviation security inspectors, airport security guards, screening officers, and employees who become aware of aviation security incidents. Security incidents themselves represent threats or acts of unlawful interference with aviation, including:

-  Disruptive persons on-board a craft or at a port
-  Detection at a screening point
-  Prohibitive item on-board a craft
-  Communicated threat
-  Transport-related procedural failure

Once the incident is identified, a report must be made as soon as possible – **no later than 24 hours after**, with penalties of anywhere between 50 and 200 penalty units attaching to stakeholders who become aware of incidents yet fail to report. The monetary amount of a penalty unit is AUD 210 as of 1 July 2017. In cases of where payment is not received, prosecution might commence.

Further, if at the time of making the report, the industry participant does not have required information, but later attains it, that information must also be provided. So, what information must be reported, exactly? The following must be included in incident reports:

- Name, contact number, and email address for the person making the report
- Title or position held by the person making the report
- Name of the employer of the person making the report (where applicable)
- Date of the report
- Date and time the security incident commenced
- Date and time the security incident ceased
- Location of the security incident (including, where applicable, the name and address of the location where the security incident occurred)
- Industry participant or participants to whom the security incident directly relates
- Industry participant or participants who are affected as a result of the security incident
- Detailed description of the security incident, including an indication as to whether the incident was:
 - a. Threat of unlawful interference; or
 - b. Unlawful interference; and
- If the security incident was a threat of unlawful interference:
 - a. Name and contact details of the person who received the threat;
 - b. Details of the threat;
 - c. Whether the person making the report assessed the threat as genuine or as a hoax and how they made that assessment; and
 - d. Whether discovering who made the threat was successful, unsuccessful, ongoing or not attempted
- If the security incident involved an aircraft:
 - a. Aircraft type;
 - b. Flight number;
 - c. Whether or not the aircraft was in flight at the time of the security incident; and
 - d. Type of cargo on board (if applicable)

- If the security incident involved a building or other infrastructure, information sufficient to identify the building or other infrastructure, such as the building number or other identifier
- If the person making the report is aware that the security incident has previously been reported to the Department:
 - a. Approximate time and date at which the security incident was reported; and
 - b. Name or position of the person, or the name of the area in the Department, to whom the incident was reported
- If the security incident has been reported to the police, an industry participant or any other body:
 - a. Approximate time and date at which the security incident was reported; and
 - b. Name and contact information of the person the incident was reported to
- Whether the report is a result of a routine security inspection
- If the report is a result of a security incident being brought to the attention of the person making the report by a third party:
 - a. That the report is a result of notification from a third party; and
 - b. The name, and where applicable, name of employer, of the third party
- Steps the industry participant has taken, or is in the process of taking, to ensure the security incident does not occur again.

The MTOFSA hews to that basic framework. Only in this circumstance, port operators, ship masters, ship operators, port facility operators, offshore facility operators, maritime security inspectors, duly authorised officers, maritime security guards, screening officers, and employees with knowledge of an incident are all deemed persons with incident reporting responsibilities. The following scenarios constituting a security incident:



If a threat of unlawful interference with maritime transport or offshore facilities is made and the threat is, or is likely to be, a terrorist act.



If an unlawful interference with maritime transport or offshore facilities is, or is likely to be, a terrorist act.

Once a maritime transport or offshore facility security incident is identified, part nine of the Act mandates timely reporting – **no later than 24 hours**, with penalties of anywhere between 50 and 200 penalty units attaching to stakeholders who become aware of incidents yet fail to report. The information that must be included in incident reports is similar to that required by the ATSA, as well:

- Name, contact number, and email address for the person making the report
- Title or position held by the person making the report
- Name of the employer of the person making the report (where applicable)
- Date of the report
- Date and time the security incident commenced
- Date and time the security incident ceased
- Location of the security incident (including, where applicable, the name and address of the port or offshore facility where the security incident occurred)
- Industry participant or participants to whom the security incident directly relates
- Industry participant or participants who are affected as a result of the security incident
- Detailed description of the security incident, including an indication as to whether the incident was:
 - a. Threat of unlawful interference; or
 - b. Unlawful interference; and
- If the security incident was a threat of unlawful interference:
 - a. Name and contact details of the person who received the threat;
 - b. Details of the threat;
 - c. Whether the person making the report assessed the threat as genuine or as a hoax and how they made that assessment; and
 - d. Whether discovering who made the threat was successful, unsuccessful, ongoing or not attempted

- If the security incident involved a ship:
 - a. Name of the ship and its flag;
 - b. Size and type of ship;
 - c. IMO and ISSC numbers;
 - d. Type of cargo on board (if applicable)
- If the security incident involved an offshore facility or building or other infrastructure, information sufficient to identify the building or offshore facility or other infrastructure, such as the building number or other identifier
- If the person making the report is aware that the security incident has previously been reported to the Department:
 - a. Approximate time and date at which the security incident was reported; and
 - b. Name or position of the person, or the name of the area in the Department, to whom the incident was reported
- If the security incident has been reported to the police, an industry participant or any other body:
 - a. Approximate time and date at which the security incident was reported; and
 - b. Name and contact information of the person the incident was reported to
- Whether the report is a result of a routine security inspection
- If the report is a result of a security incident being brought to the attention of the person making the report by a third party:
 - a. That the report is a result of notification from a third party; and
 - b. The name, and where applicable, name of employer, of the third party
- Steps the industry participant has taken, or is in the process of taking, to ensure the security incident does not occur again.

An interesting wrinkle in both Acts is the provision for security compliance information (information relating to compliance or non-compliance), which the Secretary may require. Should the Secretary request this information, it must be given within a 14-day period, with penalties attaching for non-compliance.

Add to that, in the case of the ATSA, the Secretary may require aviation security information, an expansive category of information that might include (but is not limited to):

- Statistics relating to the screening of people, vehicles, goods or cargo for entry to cleared areas or cleared zones
- Statistics relating to the people, vehicles, goods or cargo that go through a screening process and:
 - Receive clearance as a result of going through the screening process; or
 - Do not receive clearance as a result of going through the screening process and the reason or reasons for not receiving clearance;
- Information about activities undertaken, or to be undertaken, to ensure that people, vehicles, goods or cargo that have not received clearance are not in cleared areas or cleared zones
- Information about activities undertaken, or to be undertaken, at an airport for the purposes of safeguarding against unlawful interferences with aviation
- Information about the controls that apply, or will apply, to airside areas, airside security zones, airside event zones, landside areas, landside security zones or landside event zones

Here again, the information required must be submitted within a 14-day period, with penalties attaching for non-compliance.

How integrated security incident management technology can help expedite timely incident reporting

Both the ATSA and MTOFSA lay out the same mechanisms for the mandatory reporting of incidents. Aviation/maritime stakeholders can either complete a security incident report form online, download the form then email the completed form, or phone the transport security coordination team with the required information. Easy enough? Not so fast.

For good reason, both Acts require stakeholders to collect, record, then export numerous pieces of information in a timely manner. Different stakeholders have to report this information to different entities (depending on who they are), though they all have to report to the Secretary and state/territory/or federal police. And the Secretary has the statutory authority to compel even more information.

And if that weren't complicated enough, consider the fact that security incidents themselves also happen on a broad attack plain, which growing traffic on transport routes makes all the more difficult to secure.

Industry stakeholders aren't just responsible for reporting these incidents, either. They will also have to respond to breaches or threats, either of which constitute a reportable security incident. What can industry stakeholders do? Technology holds the answer:



Easy-to-use workflows.

The sensible solution is to find a digital security incident management platform that will maintain (required) incident management reports as well as any voluntary reporting that the stakeholder chooses to do. Here, easy-to-use workflows to add and edit new incidents, screening events, and stakeholder notifications provide the key means of managing security incidents and expediting timely reporting in the same system, particularly helpful if stakeholders are compelled to send more information.



Authorised users.

It doesn't end there. Not everyone should be collating information and making reports about sensitive security incidents. To this end, the platform would only allow authorised users (based on an Active Directory) to create, update, delete, and extract information in-system.



Easy to use.

On the other hand, users (especially those in the field) once they are authorised don't need any more hurdles to report and manage incidents than those they already confront on the job. The platform can help, here, as well. Responsive design will cater to mobile devices including smartphones and tablets, in addition to desktop. The solution will also make it easy to search and filter records.



Increased visibility.

Information about security incidents doesn't just have to be easy to find for audit purposes. Once you find it, that information needs to be easy to digest for a number of stakeholders for any number of policy-related reasons. Dedicated dashboards for incident and voluntary reporting summaries, or other notable events like exempt dignitaries and unaccompanied baggage will make it easier for stakeholders to interpret relevant pieces of information and make appropriate decisions in a timely manner.

Security threats to the nation's transport sector have increased, as traffic on its transport routes has taken off. The Government has upped the ante on securing transport infrastructure. And it's also required industry stakeholders to report security incidents under threat of penalty for non-compliance.

Given the nature of transport infrastructure, complying with these regulatory requirements already isn't easy. Information management shouldn't add to your challenges. Fortunately, trusted security incident management platforms, like Noggin's, help stakeholders manage and report their security incidents, keeping them in compliance with the law.



Citations

- i International Air Transport Association: Air transport supports 65.5 million jobs and \$2.7 trillion in economic activity. Available at <https://www.iata.org/pressroom/pr/Pages/2018-10-02-01.aspx>.
- ii Mark Caswell, Business Traveller: Airbus: world's passenger fleet to double in 20 years. Available at <https://www.businesstraveller.com/business-travel/2018/07/10/airbus-worlds-passenger-fleet-to-double-in-20-years/>.
- iii International Air Transport Association, Airlines: Passenger numbers to hit 8.2bn by 2037 – IATA report. Available at <https://www.airlines.iata.org/news/passenger-numbers-to-hit-82bn-by-2037-iata-report>.
- iv Bureau of Infrastructure, Transport and Regional Economics (BITRE): Australian freight transport overview.
- v Ibid.
- vi Cruise Lines International Association Australasia (CLIA), 2015, Cruise Industry Source Market Report Australia 2015, CLIA, Sydney. Available at <http://www.cruising.org/docs/defaultsource/research/australia-market-report-2015.pdf>.
- vii United Nations Conference on Trade and Development: COVID-19 cuts global maritime trade, transforms industry. Available at <https://unctad.org/news/covid-19-cuts-global-maritime-trade-transforms-industry>.
- viii Freddie Pierce, Supply Chain Digital: Long-term outlook for freight rail appears bright. Available at <https://www.supplychaindigital.com/logistics/long-term-outlook-freight-rail-appears-bright>.
- ix Lucas Baird, Financial Review: Vaccines may beat bubbles to international travel restart: Joyce. Available at <https://www.afr.com/companies/transport/qantas-to-be-cash-flow-positive-by-2021-20201203-p56k47>.
- x Cruise Industry News: P&O Australia Expecting 'Rebound' of Local Cruise Industry. Available at <https://www.cruiseindustrynews.com/cruise-news/23740-p-o-australia-expecting-rebound-of-local-cruise-industry.html>.
- xi Makhtar Diop, World Bank Blogs: Shore up global transport to defeat the COVID-19 (coronavirus) pandemic. Available at <https://blogs.worldbank.org/transport/shore-global-transport-defeat-covid-19-coronavirus-pandemic>.
- xii Bureau of Infrastructure, Transport and Regional Economics (BITRE), 2016, Airport Traffic Data 1985–86 to 2015–16. Available at https://bitre.gov.au/publications/ongoing/airport_traffic_data.aspx.
- xiii Department of Infrastructure and Regional Development: Transport Security Outlook to 2025: Security Environment Review, 2017. Available at <https://www.homeaffairs.gov.au/transport-security/files/transport-security-outlook-2025-security-environment-review.pdf>.
- xiv Ibid.
- xv BBC: Australian brothers guilty of IS plane bomb plot. Available at <https://www.bbc.com/news/world-australia-49764450>.
- xvi Rod McGuirk, AP: Australia upgrading airport security after alleged bomb plot. Available at <https://apnews.com/article/8a8cef018e1d472bac48a11d05f7585d>.

Like what you read? Follow Noggin on social media



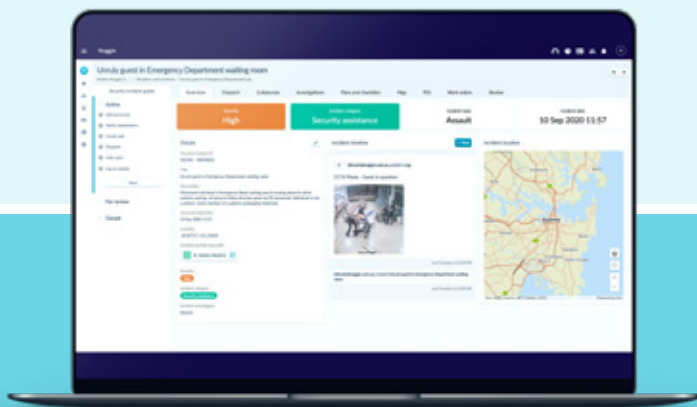
@teamnoggin



facebook.com/teamnoggin



linkedin.com/company/noggin-it



noggin for Security

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Security gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Security solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: www.noggin.io
or contact: sales@noggin.io