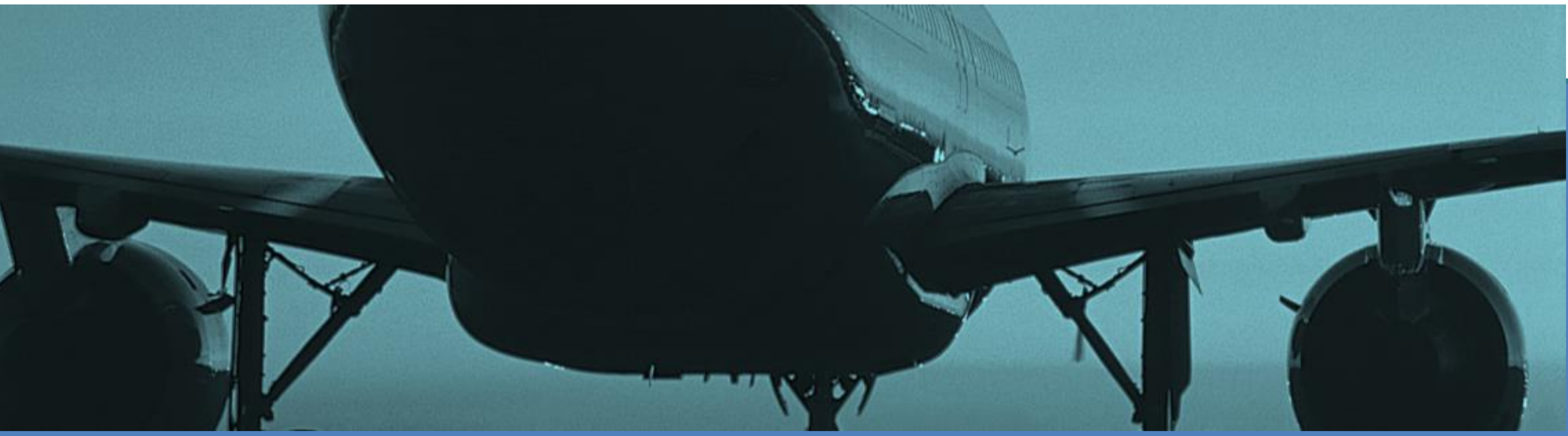
Australian Government

Department of Infrastructure and Regional Development

KNOWN CONSIGNOR SCHEME

GUIDE TO COMPLETING THE APPLICATION FORM



Contents

Known Consignor Scheme: Guide to Completing the Application Form	
Version 1.0	31/10/2016
Version 1.1	18/11/2016
Version 1.2	01/06/2017

DISCLAIMER

The Department of Infrastructure and Regional Development (the Department) makes all reasonable efforts to ensure that the information provided in this document is accurate. However, the content of this document is provided as a general guide only. The Department does not guarantee the accuracy, currency or completeness of any information contained in this document. The Department will not accept any responsibility or liability for any loss, however caused, arising from the use, or reliance upon, the content of this document.

Before relying on any information contained in this document, you should always make your own enquiries, consider your individual circumstances, seek professional advice, and check that the information is accurate and current.

INTRODUCTION

Purpose of This Guide

The purpose of this Guide is to help you complete the Known Consignor Application Form and provide you with guidance on how your business can meet the security outcomes required under the Known Consignor Scheme.

The Application Form

The Application Form asks how you ensure the security and integrity of your cargo; in particular, how you prevent an unauthorised explosive (i.e. a bomb) being inserted into cargo originating from your nominated site/s. **If you cannot provide evidence you secure your cargo and appropriately mitigate the risk of an unauthorised explosive being inserted into your cargo, you will not be able to join the Known Consignor Scheme.**

A failure to complete all relevant parts of the Application Form or provide enough detail will delay the processing time of your application. Departmental Officers may contact you to seek approval to edit your application form for clarity.

The application form, and this Guide, are divided into six parts:

- **Business Information;**
- **Part A**: Clearing Cargo and Facility Security;
- **Part B**: Personnel Security Risk Assessment and the Aviation Security Identification Card;
- **Part C**: Training;
- **Part D**: Chain of Custody; and
- **Part E**: Incident Response and Quality Assurance.

Two case studies containing sample responses for **Part A** have also been included in this Guide.

Still unsure how you should complete the form?

Email: knownconsignor@infrastructure.gov.au

Call: **1300 791 581**

BUSINESS INFORMATION

In this part of the application form, you are required to provide details of your business. To help Departmental Officers process your application faster, please provide context around your business operations and, if necessary, legal arrangements.

Business details (Q3)

The legal entity name and ACN you supply should be associated with the business undertaking Known Consignor work. For example, if you are exporting live fish for aquariums, you should supply a legal entity name and matching ACN associated with the company exporting fish, even if this business is part of a holding company associated with many different businesses. For example, if there are trust arrangements, you should list the legal entity operating the business; this may be a regulated company or a trustee that operates the business.

When providing information around your business, consider which ABN is appropriate for your application as a Known Consignor. If your site is a multi-site business and ABNs vary between sites, please specify this in your application.

PART A – CLEARING CARGO AND FACILITY SECURITY

Part A of the Application Form asks how you clear cargo and maintain facility security. Clearing cargo refers to the measures and procedures that you use to ensure that the cargo originating from your nominated site/s does not contain unauthorised explosives.

This part of the Guide addresses the following topics:

- What Is an Unauthorised Explosive?
- Outcomes Focused Security
- Multiple Sites
- Small Business
- The Cargo Clearance Process (inputs, manufacturing, packing, storage, consolidation, loading, internal movement)
- Access Controls
- Intruders, Trusted Insiders and Contractors
- Security Sensitive Information
- Proposed Measures and Procedures

What Is an Unauthorised Explosive?

All explosives must be considered as **unauthorised** unless there is a legitimate reason for their carriage on an aircraft.

In practice, an unauthorised explosive will take the form of an improvised explosive device (IED). An IED has the potential to cause catastrophic damage to an aircraft. IEDs can be designed to look like everyday items. Containers, cavities, packaging bags or boxes may also be used to conceal unauthorised explosives.

In 2010, terrorists altered two printers to contain improvised explosives and sent them via air freight from Yemen to the United States. The explosives were made using PETN concealed within printer cartridges, packed within consolidated loads. Prior to this, the terrorists had attempted several 'dry runs' to determine how long the cargo would take to reach its destination.

Terrorists go to great lengths to conceal explosives in everyday items. It is your responsibility to ensure you know what is inside the items you clear.

Outcomes Focused Security

The Department takes an ‘outcomes focused’ approach to assessing Known Consignor applications. An outcomes focused approach considers whether or not your business meets a security outcome, rather than prescribing a list of specific measures and procedures that you must have in place. This means that you have the flexibility to determine how best to meet the required security outcomes.

For example, while traditional physical security measures such as fences, locks and gates can contribute to a security outcome, the Department recognises that you may have other ways of keeping your cargo and nominated site/s secure.

On the other hand, while you might have fences, locks and gates at your nominated site/s, this does not necessarily mean that your cargo is secure. It is up to you to demonstrate how your security measures and procedures secure your cargo.

Multiple Sites

If your business exports from multiple sites, you will need to seek approval for each site that exports by air.

If all of your sites perform similar functions, and have similar security measures in place, you should complete only one application form. At each question, you should note if and how the security measures and procedures differ between sites. You can use Appendix D of the application form to provide additional information about the differences between sites.

If your sites perform very different functions, (e.g. one site manufactures products, while another site acts as a distribution centre for spare parts or returns) it may be easier to complete separate application forms.

Regardless of whether you complete one or two forms, you must identify a Nominated Contact Officer (NCO) for each site. All NCOs need to hold a valid Aviation Security Identification Card (ASICs), and undertake NCO training.

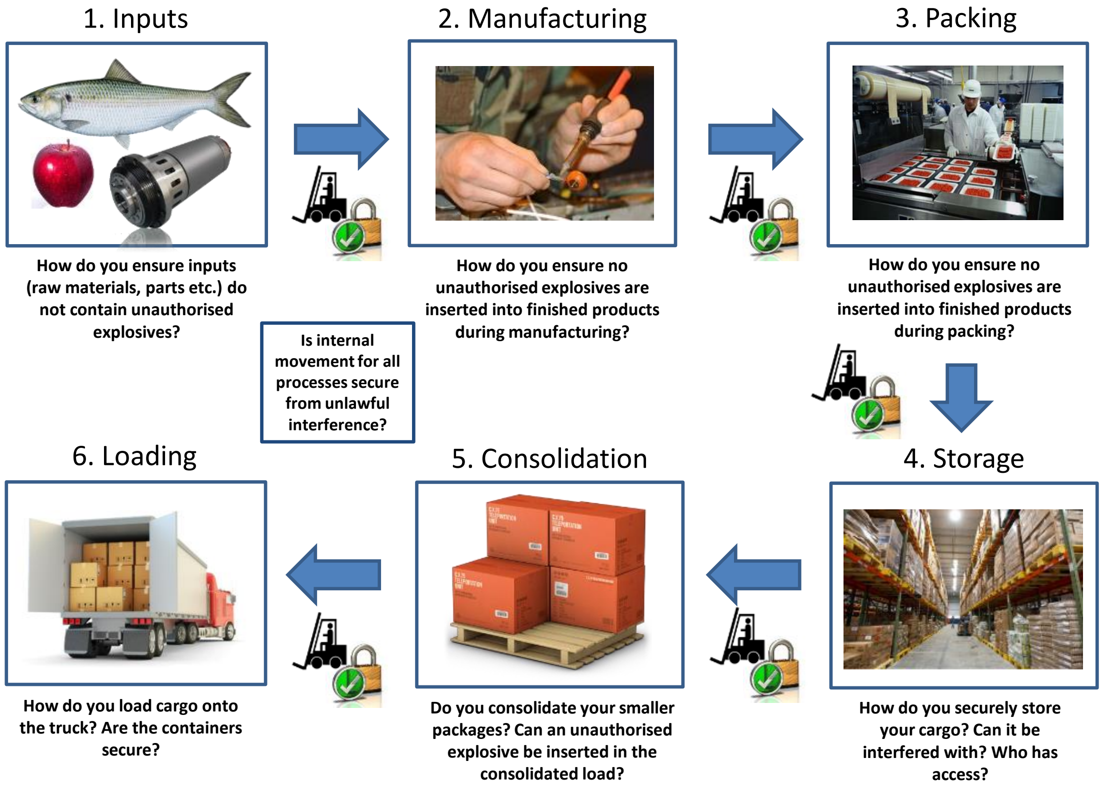
Small Business

As long as your business originates air cargo, you are eligible to apply for the Known Consignor Scheme regardless of business size. When filling out the application form, small businesses may need to think outside traditional ideas of security and quality assurance. If your business operates out of a home, for example, consider how members of your household (not involved in the business) or guests may access business assets and how you can ensure that your cargo is kept safe from interference. If your business operates in a shared warehouse space with others, consider your packaging process and whether it ensures any tampering by outsiders would be evident. Additionally, if your business is small, you may not have written procedures or formal quality assurance processes such as external audits in place, so it is important that you can demonstrate other ways of maintaining the approved processes that keep your cargo secure.

The Cargo Clearance Process

Known Consignors are authorised to originate cleared cargo from their nominated site/s. The flowchart below describes some common processes to consider when originating cargo. Not all of the processes listed below may be relevant to your business, but it is important that you still understand and address each section of the Application Form, including describing why a particular question is not applicable to your business.

Clearing Cargo Flowchart



1. Inputs

How do you ensure inputs (raw materials, parts etc.) do not contain unauthorised explosives?

2. Manufacturing

How do you ensure no unauthorised explosives are inserted into finished products during manufacturing?

3. Packing

How do you ensure no unauthorised explosives are inserted into finished products during packing?

Is internal movement for all processes secure from unlawful interference?

4. Storage

How do you securely store your cargo? Can it be interfered with? Who has access?

5. Consolidation

Do you consolidate your smaller packages? Can an unauthorised explosive be inserted in the consolidated load?

6. Loading

How do you load cargo onto the truck? Are the containers secure?

Inputs (Q8-9)

Most businesses need raw materials, machinery, parts or partially finished goods to produce a finished product. As a Known Consignor, it is your responsibility to ensure that these inputs do not contain unauthorised explosives. When discussing inputs, describe clearly whether you are purchasing pre-manufactured items from suppliers or raw materials. If raw materials, detail the form these take.

You also need to clearly describe what sorts of finished products you produce to provide context for your inputs.

Depending on the type of materials you use to manufacture goods, you will have different measures and procedures that are appropriate for securing cargo at this stage. For example, if your business manufactures machinery or equipment that requires assembling smaller components from third party suppliers, you may need to visually or physically examine each component before it is used. On the other hand, if your business deals with fresh produce, this step may not be applicable to your operations because the detection of any contaminants or foreign objects may be part of your existing operations.

A good starting point is to review your input acceptance process and determine if your business already has measures and procedures in place to ensure they do not contain unauthorised explosives.

Manufacturing (Q10-12)

Manufacturing includes any process/es your business undertakes to transform raw materials or components into finished goods. Your business must have measures and procedures in place to ensure that no unauthorised explosives can be inserted into any finished goods. You have the flexibility to implement measures and procedures that are appropriate and cost effective, as long as they achieve the desired security outcome. For example, if you assemble different components to manufacture a piece of machinery, a visual inspection during each assembly stage may suffice. Alternatively, if you produce pharmaceuticals, the insertion of an unauthorised explosive may not be possible due to the nature of the chemical processes involved.

You will need to look at your current manufacturing or production processes and determine if you have sufficient measures and procedures in place to prevent the insertion of an unauthorised explosive into your finished goods.

Packing (Q13-15)

Packing includes the process of placing finished goods inside a box, carton or other container. Your business needs to have measures and procedures in place to ensure that no unauthorised explosives can be inserted into the box, carton or container used in packaging your finished goods.

You may already have existing measures and procedures to detect and prevent foreign objects from being inserted into packaging material. For many businesses, preventing the insertion of an unauthorised explosive may be as simple as having multiple personnel working in the packing area, to look out for suspicious behaviour and prevent a **trusted insider** or an **intruder** from inserting an unauthorised explosive into cargo.

You may also want to ensure that the materials your business uses to pack your cargo are tamper proof and/or tamper evident. If you are using tamper evident tape or a similar packaging security measure, you will need to specify in your application where you store stocks of this material and how you control access to it. As a Known Consignor, you must ensure the materials you use to package your goods are secured from interference or abuse.

It is important to note that whatever measures and procedures you have in place, they must be appropriate for your operations and the type of goods your business originates.

Storage (Q16-18)

Cargo must be stored securely at all times on your nominated site/s. Your business will be required to have measures and procedures in place to prevent your inputs and cargo being tampered with. You may achieve this by having facility security measures such as cameras, swipe access or lockable gates. Additionally, you may have measures and procedures in place to prevent personnel or contractors from unauthorised entry into storage areas. If your business uses tamper evident packaging, this also enhances the security of your cargo, as any tampering can be clearly and quickly identified.

When discussing your storage arrangements in your application, you need to clearly identify differences in storage procedures for inputs that have been checked for explosives, and cargo produced from the inputs.

You also need to describe storage of packing materials and how these are secured from interference. This is particularly important if you make up packaging beforehand, such as placing inserts into boxes.

Consolidation (Q19-21)

Consolidation is generally a separate process from packing. Packing refers to the process of packaging goods into initial boxes or cartons. Consolidation refers to the process of combining these smaller boxes or cartons onto a pallet of unit load device (ULD), ready for transport. Consolidated loads are most commonly shrink-wrapped to sit tightly on a pallet. As the consolidated pallet may consist of multiple boxes or cartons, and may contain gaps, it may be possible for an unauthorised explosive to be inserted into the consolidated load. In this situation, you need to have security measures and procedures in place to ensure that no unauthorised explosive is inserted into cargo during the consolidation process.

In discussing your consolidation measures in your application, you need to state clearly where consolidation materials such as shrink wrap may be stored, and how you control access to these. As a Known Consignor, you must ensure the materials you use to consolidate your goods are secured from interference or abuse.

Loading (Q22-24)

The loading process is where cargo is finally loaded onto ground transport. Usually, this involves a business organising a transporter to come and pick up a consolidated load. You must ensure that there is no opportunity for an unauthorised explosive to be inserted into cargo during the loading process. Ideally, loading should be overseen by your personnel to ensure that cargo is not interfered with.

Internal Movement (Q25-27)

In most businesses, goods are moved between different areas during the production, packing or consolidation processes. During ‘internal movement’, there may be opportunities for a **trusted insider** or an **intruder** to insert an unauthorised explosive into cargo. For example, if goods are left unattended for long periods, they may be vulnerable to interference. You should consider whether there are any vulnerabilities in the internal movement process. This includes considering whether cargo is left in any unsecure areas, the speed of internal movement, potential bottlenecks on your nominated site/s, the oversight of people moving cargo, and how easy it is for someone involved in the moving of cargo to insert an unauthorised explosive into cargo.

In discussing internal movements in your application form, the more specific you can be, the easier it will be for Departmental Officers to process your application. Writing: “The first internal movement occurs after Stores staff receive inputs from our suppliers. Suppliers unload boxed goods at the designated loading bay and our Stores staff carry boxes by hand approximately

10 metres to the on-site Store. Where heavy goods are receipted, a Stores staff member will operate a forklift to move this item directly into the manufacturing workshop, a distance of about 15 metres. This is supervised." is preferable to writing: "We move goods from the loading bay to the store."

Access Controls (Q28-30)

Access controls include, but are not limited to: perimeter fencing, locks, gates, security guards, and electronic access cards.

When discussing access controls in your application, it is important to specify details rather than just listing measures. As an example, if discussing security cameras, state what sort of coverage they provide (eg. coverage of all external access points to the manufacturing area, but not to office areas), whether they are actively monitored, motion sensitive and details such as who has access to footage and how this is controlled.

When discussing swipe access to facilities, please provide detail around who has swipe access, whether access is recorded and whether this evidence is accessible to people in your business. If discussing physical keys to facilities, please provide detail around who holds keys, how many sets there are and whether you have a key register. Providing detail around each measure allows Departmental Officers to process your application faster.

Intruders

To prevent an intruder from inserting an unauthorised explosive into cargo, Known Consignors must implement effective access controls to deter, detect and prevent unauthorised access to their nominated site/s.

Trusted Insiders

Trusted insiders are potential, current or former personnel or contractors who have legitimate access to your nominated site/s, information, systems or people, who use that access to either intentionally or unknowingly cause harm. A trusted insider may be someone who has been radicalised and seeks to knowingly cause harm by inserting an unauthorised explosive into cargo. In another instance, a trusted insider may have been bribed or coerced to insert a package into cargo, not knowing it to be an unauthorised explosive. Because they already have access to your site/s, traditional physical security and access control measures are less effective at combating the trusted insider threat.

To analyse opportunity for trusted insiders to insert explosives into your cargo, consider at each stage of processing how many people work on a task, how closely together they are located and whether they are supervised. If any staff work alone, it is important to state this in your application and discuss measures in place to mitigate the threat of a trusted insider tampering with cargo. Including this information in your application is important to enable Departmental Officers to process your application faster.

In 2016, three staff working at the TNT Melbourne Airport depot were discovered to be supporters of the five men charged in the “tinnie terror” case. A TNT employee recognised them on television footage of the case and contacted the National Security Hotline, leading to the removal of the three from freight-handling roles. Without the vigilance of this employee, these men would have continued to have access to air cargo and may have had opportunity to tamper with it.

People may become radicalised before or after they begin working at your business, and it is your responsibility to ensure you and your staff remain vigilant and respond to suspicious behaviour appropriately.

Contractors

Known Consignors are also required to consider whether any contractors, with legitimate access to their nominated site/s, may have the opportunity to insert an unauthorised explosive into cargo. Contractors most likely to have this opportunity include cleaners, delivery personnel, electricians or maintenance crew. You will need to think about both how contractors are managed and supervised during normal business hours and how you deal with cargo security outside of these hours, when contractors may have unescorted access to cargo.

Security Sensitive Information (Q31-32)

Known Consignors are required to protect security sensitive information. Security sensitive information includes, but is not limited to: information on cargo flight and carrier details; cargo handling procedures; visitor access passes and logs; security notices; and Security Programs and directions issued by the Department. Generally, businesses already have information security protection procedures in place to prevent the disclosure of sensitive commercial information.

You should review your current information technology security or paper-based filing systems to ensure that security sensitive information is protected from unauthorised access. For example, you may need to review who has access to the cargo manifest details: is access based on a need to know basis, or can everyone within the nominated site/s access this information through a common login? If security sensitive information can be accessed by a large number of people, then you may need to look at measures to restrict access, in order to mitigate the risk of trusted insiders using that information in a way that might undermine aviation security. Measures you may consider implementing include:

- using lockable containers to hold hard copy information;
- using password protected IT system and/or restricted access to certain folders;
- using a firewall; and/or
- maintaining a register to record the release of security sensitive information.

Proposed Security Measures and Procedures (Q33)

As you review **Part A** of the Application Form, It is important for your business to consider any potential vulnerabilities in your security that your existing security measures and procedures may not cover. The presence of security vulnerabilities does not automatically disqualify your business from approval as a Known Consignor. However, you will need to think about how to address these vulnerabilities in a way that is suitable for your business.

Part A: Case Study 1 – Manufacturer (Q8-33)

The following text is a sample response to Part A of the Application Form by a manufacturer.

Clearing Cargo and Facility Security

*Please describe the steps (where applicable) in how your business clears cargo. If any of the steps are **not applicable**, please provide the reasons.*

Inputs

Q8.Describe the inputs that you use to manufacture or produce your cargo:

We source batteries, LEDs and circuit boards from overseas suppliers, as well as metal frames from a distributer in Sydney. We use these to manufacture electrical equipment.

Q9. How do you ensure that inputs, such as raw materials, parts, or other products, do not contain unauthorised explosives? Describe how you inspect, physically examine, or use other means to ensure that inputs do not contain unauthorised explosives:

Most of our inputs are small and cannot contain unauthorised explosives due to their size. Two staff members work together to conduct visual inspections of circuit boards for unauthorised explosives. We do not check the inside of the batteries as the cases are sealed however the battery is manufactured with very little spare space in the case, so any foreign object inserted there would prevent the battery from functioning. Batteries that do not function correctly are returned to the supplier as defective stock. As we always test our electrical equipment's functionality, this test would pick up on any foreign objects inserted in the battery.

Manufacturing

Q10. Describe how you manufacture or produce your cargo:

Our staff combine batteries and circuit boards in our workshop, integrating them into metal frames to become completed electrical equipment. There are around 20 personnel working on the manufacturing floor at any time, with additional staff engaged as required. There are two supervisors present at all times, responsible for ensuring manufacturing takes place in accordance with our company protocols and OH&S requirements. The equipment is assembled and quality inspected on the workshop floor.

Q11. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the manufacturing process?

We have strong perimeter security, with a high perimeter fence, swipe access gates at the entrance, and another set of swipe access doors into the building. Swipe access is granted on a needs basis with manufacturing staff unable to access office areas unescorted and vice versa.

Our personnel are trained to pick up on any intruders roaming around the site. Our equipment and our intellectual property are of high value and staff have a security conscious attitude because of this. All personnel must wear uniforms, which makes strangers more visible.

We also do not allow couriers or contractors to roam freely. Contractors are required to sign in at the front office and work only on their assigned jobs in the presence of supervision by a company employee.

Outside of working hours, our facility is equipped with motion sensor alarms with back to base monitoring.

Q12. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the manufacturing process?

All of our manufacturing is done by personnel working closely together. No staff have lone access at this stage. All staff work within line of sight of each other and two supervisors roam the floor and carry out random inspections of products, adding another layer of security. Having people work closely together means any suspicious behaviour will be noticed quickly. Our company's security awareness training encourages staff to speak up when they see something they don't believe is right so the person engaging in suspicious behaviour will be confronted.

We also conduct referee checks on our personnel and interview them extensively to assure us of their character.

As a final safeguard, we functionally test and visually inspect all of our electrical equipment. This will pick up any foreign objects inserted during the manufacturing process as there is little space within the equipment and inserting a foreign object will cause electronic signals to fail. If a product fails inspection, a supervisor pulls it apart for inspection, thus detecting the foreign object. If it is a battery that fails inspection, it is replaced by a functioning unit in the final product and the non-working battery is returned to the supplier as faulty stock.

Packing

Q13. Describe how you pack your cargo:

As soon as the electrical equipment is manufactured and quality checked, a packing staff member uses a forklift to move it to the packing line, located in the next room. There is not enough time for this person to tamper with the equipment when moving it as equipment is sealed and any tampering around seals will be evident when packing staff visually inspect it. Two people work in the packing room and are overseen by roaming supervisors.

These workers remove Styrofoam inserts from boxes and check for any tampering before inserting the equipment. Packing staff then use company branded tape to seal all box edges and place company seals across each edge.

Q14. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the packing process?

See our response to manufacturing. We use the same measures and procedures to prevent the entry of intruders.

Q15. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the packing process?

We use two packers at all times, who have oversight of each other. If one of these packers is away, the other is not allowed to pack alone and will be supervised.

Storage

Q16. Describe how you store your cargo. Note down where your cargo is stored, what state it is stored in (sealed or unsealed cartons), and ease of access (e.g. is access to the storage facility restricted?)

We store the boxed cargo in a storage room, which can be accessed by ladders and forklift. The cartons are stacked in this area according to their serial numbers. The storage room is not locked off from the main area.

Q17. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the storage process?

See our response to manufacturing. We use the same measures and procedures to prevent the entry of intruders. As the storage room must be accessed from the main manufacturing floor, it would be unlikely for an intruder to break into the facility during working hours and not be noticed and confronted by staff. Outside of working hours, our facility is equipped with motion sensor alarms with back to base monitoring.

Q18. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the storage process?

We store cargo in tamper evident packaging and spare packaging materials are locked away outside of normal business hours. We also forklift our cargo to above-ground shelves in the storage room so this cargo is only accessible by forklift. These measures prevent unlawful interference.

Consolidation

Q19. Describe how you consolidate (if at all) your cargo:

We shrink wrap our cartons onto a pallet once we finalise the shipment. We manually do the shrink wrapping a day before the truck arrives to pick it up. Shrink wrapping is done at the cargo storage area by a single person.

Q20. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the consolidation process? In particular, how do you prevent the insertion of an unauthorised explosive into the packing material, such as in shrink wrapping, or hidden inside a consolidated load?

See our response to manufacturing. We use the same measures and procedures to prevent the entry of intruders.

Q21. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the consolidation process? In particular, how do you prevent the insertion of an unauthorised explosive into the packing material, such as in shrink wrapping, or hidden inside a consolidated load?

We currently only have one person doing the shrink wrapping. We have identified this as a potential vulnerability in our security. As a mitigation measure, we will have this staff member acquire an ASIC to allow him to continue shrink wrapping by himself. We have provided his details at Part B – Personnel Security Risk Assessment and ASIC.

Loading

Q22. Describe how you load your cargo onto a transport vehicle:

We use two freight forwarders. When a truck arrives at our facility for a pick-up, we always check the truck driver's identity and ensure they know where they are delivering our cargo. After this, one of our logistics staff uses a forklift to lift palleted goods onto the truck and a supervisor ensures no goods are added or removed from the pallet while this is taking place. The supervisor and logistics staff member check the truck driver locks the truck securely.

Q23. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the loading process?

See our response to manufacturing. We use the same measures and procedures to prevent the entry of intruders.

Q24. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the loading process?

At this stage, cargo is shrink wrapped and there are company seals across box edges so any tampering will show up. The loading process is also supervised by both a member of our personnel and the truck driver. No one can unlawfully access the cargo during loading without the driver or our staff noticing and confronting the person.

Internal Movement

Q25. Describe how you internally move your cargo (e.g. moving your cargo from packing to storage):

We receive most goods, boxed, at the warehouse loading bay area. Stores staff inspect boxes for damage and accept them if no damage is visible. They then carry them by hand about 10 metres into the on-site store where they open the boxes and check contents against the purchase order for quantity. They then deliver boxes to

Manufacturing staff by hand, a distance of about 10 metres. Where heavy goods are receipted, stores staff operate a forklift and are supervised while doing so.

Internal movement also occurs when finished goods are moved by workshop personnel to the packing area. Most goods are placed on trolleys and trolleys are pushed by hand however if finished goods are heavy, a manufacturing staff member will move them using a forklift. This is supervised.

Additionally, once cargo is packed into cartons in the packing area, it is moved by the packers by hand or by forklift into the storage area. If using a forklift, this is supervised. We pick the cartons from the storage area to go on the consolidated pallet. Once we have finalised the shrink wrapping, pallets are stored and then moved to the loading bay.

Q26. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the internal movement process?

As we have a small site, cargo is moved rapidly from one area to the next under close supervision. An intruder would not have the opportunity to insert an unauthorised explosive into cargo without being noticed. We also use our own company tamper evident sticky tape on our cartons, which means that our personnel can pick up any tampering with the cargo after it has been packed.

Q27. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the internal movement process?

As above for intruder.

Access Controls

Q28. How do you prevent an **intruder** from accessing your nominated site/s? Describe the controls you have in place to deter, detect and prevent access to your nominated site/s, including during after-hours, weekends or holidays:

See our response to manufacturing. We use the same measures and procedures to restrict access to our nominated site/s, including during after-hours, weekends and holidays.

Q29. Do any **contractors** have legitimate access to your nominated site/s, particularly after-hours (e.g. contractors, cleaners or electricians)?

We have the following contractors that enter our nominated site/s at different times. They are:

- Maintenance and electricians - These contractors enter our nominated site/s during work hours and must report to reception and be signed in. They are limited to accessing the relevant areas of their work.
- Cleaners - Cleaners enter our nominated site/s after hours and have access to the entire site.

Q30. How do you prevent these **contractors** from accessing your cargo? Describe the controls you have in place to deter, detect and prevent access to your cargo, including during on-hours and after-hours (e.g. do you restrict cleaners to certain areas, or keep cargo areas locked?):

For our maintenance contractors and electricians, we check their credentials and maintain some supervision over their activities. As these contractors are on site during work hours, their actions are monitored.

For our cleaners, we do not currently monitor their access or have oversight of their activities. However, they will now be required to apply for and obtain ASICs.

Security Sensitive Information

Q31. How do you ensure that security sensitive information (see glossary) is protected from unauthorised access by an **intruder**? Describe the measures and procedures you currently use in your business to restrict access to and distribution of any information that could be used by an intruder to compromise the security of your cargo:

In our offices, access to cargo and logistic information is stored in digital form on computers secured with Windows BitLocker encryption, and on similarly encrypted company servers. Computers require a password to be inputted after five minutes of inactivity, and passwords are required to be changed every three months. For physical documents, staff are trained to shred documents containing sensitive information (including shipping information, customer details, financial records) once they are no longer required.

On the product floor, shipping information is printed daily and only contains details of that day's shipments. This information does not directly identify the customer. Only floor managers have this information on hand, however there is a risk that the information could be left unattended. Labels on goods ready for shipment identify the customer and their address, so we require and train our personnel to be vigilant at all times and identify and confront suspected intruders.

Q32. How do you ensure that security sensitive information (see glossary) is protected from misuse by a **trusted insider**? Describe the measures and procedures you currently use in your business to restrict access to and distribution of any information that could be used by a trusted insider to compromise the security of your cargo:

Beyond what has been mentioned above, the company takes precautions to ensure that sensitive information is only available on a need-to-know basis. Computer access to sensitive information is restricted (through user restricted folders on the company computer network) to those individuals with direct responsibility for this information, and a record is kept of who has access to what information. For example, sales and client relations staff do not have access to shipping schedules, and staff biographical information is only available to our office administrator. Detailed logs are kept on the computer access of staff. Physical files are kept in lockable cabinets. Only the general manager has broad access to all security sensitive information.

On the product floor, the measures to prevent intruders accessing security sensitive information would also partially prevent a trusted insider from compromising our security. However, given that some of our shipments happen at regular intervals, it would be possible for a determined trusted insider to piece together the shipping profile for some of our customers. We rely on other strategies, such as having multiple people present during the packing process, to prevent a trusted insider from placing an unauthorised explosive into our export cargo.

Proposed Security Measures and Procedures

Q33. Are there any security measures and procedures that you are proposing or currently in the process of implementing, which are not yet available? Please describe:

We will obtain ASICs for any employee who has lone access to cargo.

Part A: Case Study 2 – Food Exporter (Q8-33)

The following text is a sample response to Part A of the Application Form by a seafood exporter.

Clearing Cargo and Facility Security

*Please describe the steps (where applicable) in how your business clears cargo. If any of the steps are **not applicable**, please provide the reasons.*

Inputs

Q8.Describe the inputs that you use to manufacture or produce your cargo:

Our company fishes in waters around Queensland and exports fresh fish.

Q9. How do you ensure that inputs, such as raw materials, parts, or other products, do not contain unauthorised explosives? Describe how you inspect, physically examine, or use other means to ensure that inputs do not contain unauthorised explosives:

Once fish are caught, they are kept in the cooler on the boat. Fishermen on the boat do have access to the cooler however as we later gut and examine the fish for its appropriateness for sale as food, it is not possible a foreign object inserted would not be picked up at that stage. When the boat docks at shore, three of our staff transport the fish, on trays, to the processing room. During processing, we make sure that nothing foreign is hidden inside the fish.

Manufacturing

Q10. Describe how you manufacture or produce your cargo:

Our fishing boat docks close to our processing room. Three staff place fish on trays, which are then pushed by these staff to the processing room, a distance of around 20 metres. This process is supervised. Around 6 staff gut the fish and place them on the processing line. One staff member at the end of the processing line packs these fish into boxes with ice.

Q11. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the manufacturing process?

We are located on a pier and locked facility doors prevent an intruder from easily accessing the processing and packing areas. Additionally, we are a family run business where everyone knows everyone else. We have about 10 staff on site at a time and can easily spot an intruder.

Importantly, processing staff work closely together and the whole process is supervised, up to and including when the shipments are loaded onto a truck.

Q12. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the manufacturing process?

All of our processing is done by personnel working closely together, with multiple people present. This will pick up any suspicious behaviour. No staff have lone access at this stage.

Our company policy also requires staff to leave all personal items, such as wallets and phones, outside the processing room for hygiene reasons. We also have a supervisor watching the gutting and packing of fish.

Packing

Q13. Describe how you pack your cargo:

Once the fish is gutted, we pack the fish with ice in a polystyrene box. This is immediately packed under a strapping machine, which seals the carton and company branded tape is applied across the carton edge. The straps are tamper evident, and the carton cannot be opened without it being evident that the straps have been cut. We store stocks of the company branded tape in a locked cabinet. Keys to this cabinet are held by a supervisor responsible for unlocking and locking the facility each day.

Q14. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the packing process?

See our response to manufacturing. We use the same measures and procedures to prevent the entry of intruders.

Q15. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the packing process?

We have multiple eyes on the packing machine and the person responsible for packing. There is a shift supervisor who has oversight of the whole process. The quick turnaround means that there is almost no time for someone to insert an unauthorised explosive into cargo.

Storage

Q16. Describe how you store your cargo. Note down where your cargo is stored, what state it is stored in (sealed or unsealed cartons), and ease of access (e.g. is access to the storage facility restricted?)

We don’t store any cargo overnight in our freezers. It is all packed and shipped on the same day. Packing staff hand carry the boxes of fish around 5 metres from the strapping machine to the shrink-wrapping machine adjacent to the loading bay, where we store them until they are picked up by our freight forwarder. They are not shrink-wrapped until the freight forwarder’s truck arrives.

We assemble cartons each day to pack the day’s fish into for export. These assembled cartons are kept in the corner of the processing room, in sight of the processing line workers. They do not contain any packaging inserts that could hide an explosive.

Q17. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the storage process?

See our response to manufacturing. We use the same measures and procedures to prevent the entry of intruders.

Q18. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the storage process?

There is no reason for pre-prepared cartons to be handled until packing, and no reason for packed and strapped cartons to be touched until shipment, so anyone doing so would be questioned. Furthermore, the cartons are strapped, and there is only one strapping machine which is in line of sight of all staff in the processing room. It is impossible to remove the strapping without this being noticed by our staff.

Consolidation

Q19. Describe how you consolidate (if at all) your cargo:

We shrink wrap our cartons in the loading bay once the pickup truck comes. We stack 20 cartons on each pallet. They are packed tightly together and we shrink wrap the consolidated load in clear wrap.

Q20. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the consolidation process? In particular, how do you prevent the insertion of an unauthorised explosive into the packing material, such as in shrink wrapping, or hidden inside a consolidated load?

See our response to manufacturing. We use the same measures and procedures to prevent the entry of intruders.

Q21. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the consolidation process? In particular, how do you prevent the insertion of an unauthorised explosive into the packing material, such as in shrink wrapping, or hidden inside a consolidated load?

We have a single person doing the shrink wrapping. However, the process is visible to others on the processing line and is supervised by a supervisor. We don’t think someone could insert an unauthorised explosive without being noticed.

Loading

Q22. Describe how you load your cargo onto a transport vehicle:

We sometimes load our own van, or have our freight forwarder come and pick up the cargo. Because of the high value of our goods, our supervisor always checks the identity of the truck driver. He and the general manager also oversee the loading process to ensure that it runs smoothly.

Q23. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the loading process?

See our response to manufacturing. We use the same measures and procedures to prevent the entry of intruders.

Q24. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the loading process?

The general manager will always oversee any loading activities. Loading also occurs in the presence of the freight forwarder. We will pick up any suspicious behaviour as our cargo is highly valued and so we are aware of the potential for theft.

Internal Movement

Q25. Describe how you internally move your cargo (e.g. moving your cargo from packing to storage):

As discussed above, internal movement occurs from the time inputs (fish) are received at the business to the time the final consolidated and packaged products are loaded into the freight forwarder's truck. These internal movements are covered above in the relevant sections. Workshop personnel move fish on trolleys to the packing area. Once cargo is packed into cartons, it is moved to the corner of the processing room. The cartons are then placed on the consolidated pallet. Shrink wrapping occurs directly adjacent to the loading bay.

Q26. How do you prevent an **intruder** from inserting an unauthorised explosive into cargo during the internal movement process?

As we have a small site, cargo is moved rapidly from one area to the next under close supervision. An intruder would not have the opportunity to insert an unauthorised explosive into cargo without being noticed. We also use our own company tamper evident sticky tape on our cartons, which means that our personnel can pick up any tampering with the cargo after it has been packed.

Q27. How do you prevent a **trusted insider** from inserting an unauthorised explosive into cargo during the internal movement process?

As above for intruder. We have a very quick and short internal movement process. Fish is taken off the boat, delivered by a forklift or carried into the processing facility. Processing, packing and temporary storage all occurs in the one location. Once a pallet is shrink wrapped, it is moved to the loading bay.

Access Controls

Q28. How do you prevent an **intruder** from accessing your nominated site/s? Describe the controls you have in place to deter, detect and prevent access to your nominated site/s, including during after-hours, weekends or holidays:

See our response to manufacturing. Doors/gates to the site are locked after business hours, on weekends and holidays.

Q29. Do any **contractors** have legitimate access to your nominated site/s, particularly after-hours (e.g. contractors, cleaners or electricians)?

We do not use any contractors or cleaners. All cleaning is performed by our personnel. The only instances of contractors entering the site are for emergency repairs.

Q30. How do you prevent these **contractors** from accessing your cargo? Describe the controls you have in place to deter, detect and prevent access to your cargo, including during on-hours and after-hours (e.g. do you restrict cleaners to certain areas, or keep cargo areas locked?):

As our site is small, any contractor on site is monitored by our personnel. Contractors only attend our business during business hours. If a contractor was required to attend our business outside of operating hours, we would ensure a staff member accompanied the contractor and supervised the contractor's work.

Security Sensitive Information

Q31. How do you ensure that security sensitive information (see glossary) is protected from unauthorised access by an **intruder**? Describe the measures and procedures you currently use in your business to restrict access to and distribution of any information that could be used by an intruder to compromise the security of your cargo:

As a small business, we hold very little security sensitive information. What information we do hold is stored on password protected computers and is accessible only to the general manager. Our office is effectively paperless, but the documents we do print are stored in a locked cabinet (the general manager has the key) and shredded before being disposed of. We are not privy to the flight details of cargo (this is handled by our freight forwarder), and what information we do have is only distributed on a need to know basis. The general manager has access to security sensitive information. No other personnel have access to the company computer. This prevents security sensitive information from being exploited by trusted insiders.

Q32. How do you ensure that security sensitive information (see glossary) is protected from misuse by a **trusted insider**? Describe the measures and procedures you currently use in your business to restrict access to and distribution of any information that could be used by a trusted insider to compromise the security of your cargo:

As above. Only the general manager has access to security sensitive information, and she does not have lone access to cargo. If she was to use this information to interfere with cargo, this will be picked up by our staff.

Proposed Security Measures and Procedures

Q33. Are there any security measures and procedures that you are proposing or currently in the process of implementing, which are not yet available? Please describe:

None.

PART B – PERSONNEL SECURITY RISK ASSESSMENT AND ASIC

In **Part A** of the Application Form, you will have outlined various measures and procedures you use to prevent the trusted insider and the intruder threat. **Part B** of the Application Form asks you to identify the broader personnel security risks in your business, and how you might mitigate those identified risks. It also asks you to identify the key personnel within your business who must be hold a valid Aviation Security Identification Card (ASIC) because of their role within your organisation.

This part of the Guide addresses the following topics:

- Why Are There Personnel Security Requirements?
- What Are the Personnel Security Requirements for Known Consignors?
  - Establishing the Risk Context
  - Identifying the Roles That Require a Person to Hold an ASIC
- How to Identify Personnel Requiring an ASIC, and What Are Suitable Mitigation Measures?
- How Do I Get an ASIC?
- ASIC Adverse Findings

Why Are There Personnel Security Requirements?

Personnel security is a critical component of the Known Consignor Scheme. Personnel security requirements are designed to address the risk of a **trusted insider** using their access rights to insert an unauthorised explosive into cargo.

Trusted insiders are potential, current or former personnel or contractors who have legitimate access to the nominated site/s, information, systems or people, who use that access to either intentionally or unknowingly cause harm. A trusted insider may be someone who has been radicalised and seeks to knowingly cause harm by inserting an unauthorised explosive into cargo. A trusted insider could also be someone who has been bribed or coerced to insert a package into cargo, not knowing it to be an unauthorised explosive.

The risks posed by trusted insiders can be mitigated through the implementation of well thought out personnel security measures and procedures. Personnel security is best described as **a system of policies and procedures** which seek to manage the risk of personnel exploiting their legitimate access for illicit gain, or to cause harm. A key part of personnel security is background checking, but it is not the only part.

What Are the Personnel Security Requirements for Known Consignors?

Establishing the Risk Context (Q34-35)

The first step of **Part B** requires you to provide a general overview of the personnel security risk context in your business. This captures key external and internal factors that may impact on your personnel security measures. For example, if you plan to hire several casual workers during harvest season in summer, this will affect your business's ability to manage the insider threat.

There may be a variety of ways in which you can manage the influx of casual workers to keep your site secure. For example, you may restrict access of casual workers to certain areas; heighten your supervision of new workers; prevent casual workers from carrying any personal belongings into cargo packing areas; or increase inspections or scrutiny of packed cargo.

Other factors that could be relevant to your personnel security risk context include:

- plans to upsize/downsize the business;
- budgetary constraints;
- organisational restructuring;
- major changes to business practices;
- internal attitudes to security; and/or
- operational factors (e.g. high number of contract personnel/turnover/redundancies etc.)

The Department does not prescribe the measures and procedures your business needs to put in place to manage these external or internal factors. However, you do need to think about how you can deal with potential large changes to your personnel structure, and how you can manage these changes to mitigate the insider threat.

Identify the Roles That Require a Person to Hold an ASIC (Table, p13)

Key personnel within your organisation must hold a valid ASIC. at a minimum, the Nominated Contact Officer must hold an ASIC.

In addition, where a person has **unescorted access to cargo** or **special access to security sensitive information**, they must hold a valid ASIC unless measures are in place to mitigate against this threat.

How Do I Identify Personnel Requiring an ASIC, and What Are Suitable Mitigation Measures?

The personnel security flowchart on page 31 can assist you to identify the personnel that require an ASIC (in addition to the Nominated Contact Officer).

If your business already has other measures in place that mitigate the insider threat, this may reduce the number of Personnel required to hold an ASIC. For example, measures and procedures that may be effective in mitigating the insider threat include:

- live monitored security cameras;
- multiple personnel working together to pick up on suspicious behaviour;
- constant supervision of production lines or packing areas;
- rigorous quality assurance processes on final consignments; and/or
- the business's general approach towards security, incident reporting, hiring and training.

Ultimately it is a business and operational decision as to how you address the insider threat. For example, you may want to consider the cost of obtaining an ASIC versus the cost of changing work practices. You will also need to consider, and detail in your application, how you will adapt your business practices when ASIC holders are away and another person must undertake that individual's regular tasks.

Whatever your personnel security arrangements are, they must be documented in your Application Form. The sample response on the following page will give you an idea of the information required.

The Department will not make the decision for your business as to how many personnel should obtain an ASIC. The Department's role is to validate your site to ensure that security outcomes are met. During validation, the Department will look at your existing measures and see whether they contribute to the personnel security outcome.

Sample Completed Table, p13.

Role with access to cargo or information	Full name(s) of individuals in that role	ASIC required/ not required	Reason (including mitigation measures if ASIC not required)
The contact officer nominated at Q4.	John Lee	Must obtain an ASIC.	The Nominated Contact Officer must obtain an ASIC, in order to assure the Department that the person responsible for implementing the Known Consignor Security Program has been appropriately background checked.
Security manager	Sally Barnes	Required	Security manager has 24-hour access to all areas of our building.
Production line workers	Various	Not required	We do not propose ASICs for our production line workers. We will mitigate the insider threat by having production line workers work in teams, with supervision at all times. See response in Part A for further detail.
Cleaners	Annie Short Eric Knox	Required	Cleaners have unsupervised access to cargo. It is not practical to change our operations to prevent them from accessing storage areas.
Export manager	Eleanor Wazowski	Required	While our export manager does not have unsupervised access to cargo, she has access to all cargo consignment information, as well as information about the security procedures associated with our export consignments.

How Do I Get an ASIC?

To obtain an ASIC, an individual must apply to an approved issuing body. Individuals performing functions for a Known Consignor should apply for a role-specific ‘white’ ASIC. Not all issuing bodies issue white ASICs. For a list of issuing bodies that will issue to Known Consignors, and more information on applying for a card, visit the Department’s website: https://infrastructure.gov.au/asic.

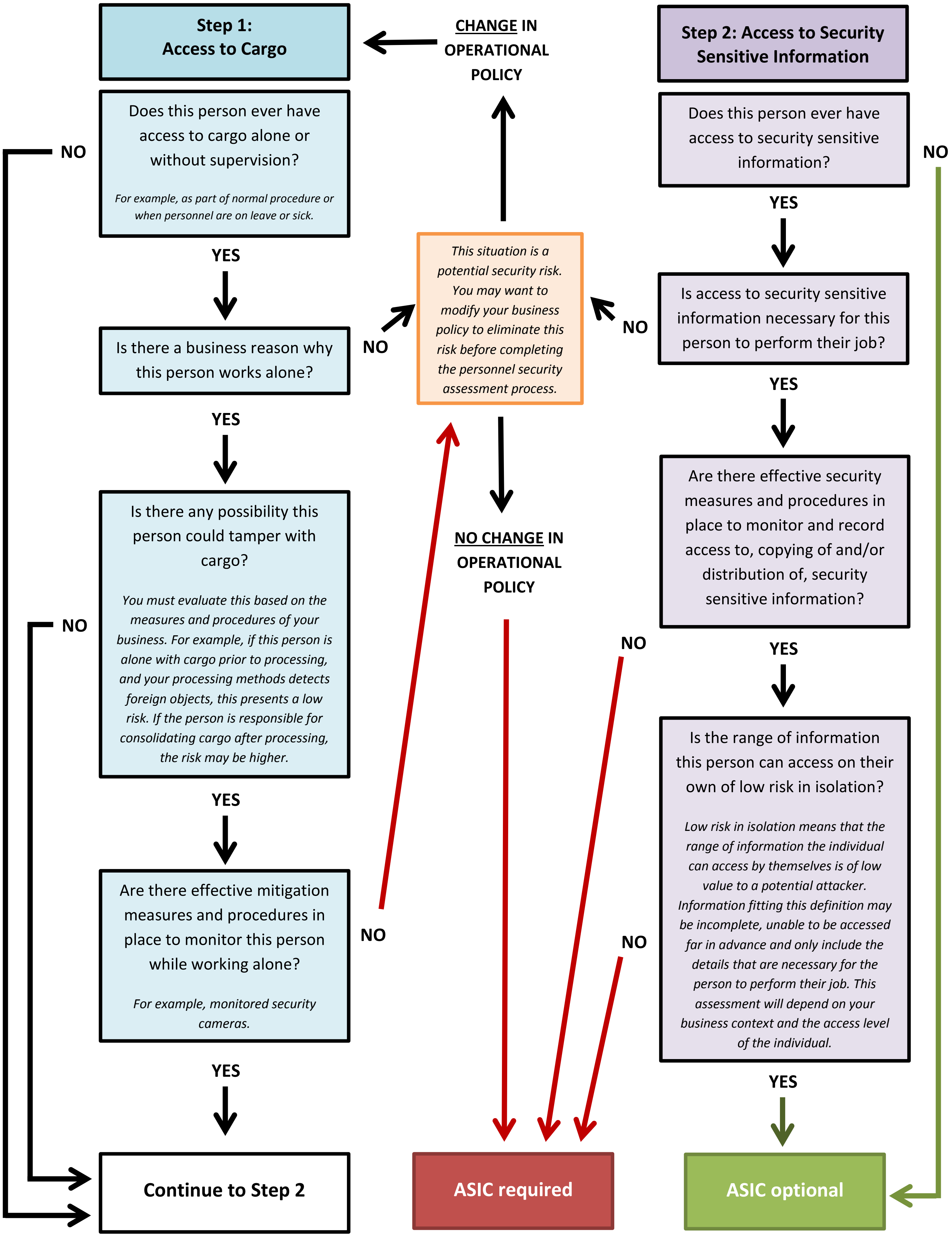
Issuing bodies typically take up to 6 weeks to process an application, so it is important to take this into account when applying to the Known Consignor Scheme. Additionally, remember that applying for ASICs does not guarantee approval as a Known Consignor.

If you have further questions on the ASIC application process, email knownconsignor@infrastructure.gov.au.

ASIC Adverse Findings

A criminal record does not necessarily prevent an individual from working in a role which grants them access to cargo or security sensitive information. Only when a background check returns an adverse criminal record, containing aviation security relevant offences as defined in the Aviation Transport Security Regulations 2005, would an application for an ASIC be denied. In this instance, your business would not be expected, nor required, to terminate the individual’s employment. However, you may wish to make holding an ASIC a condition of employment for new personnel in a particular role. Existing employment laws still operate in relation to unfair dismissal. In the event of an adverse finding, you need to show how your business will mitigate the risks posed by that individual (i.e. reassigning them to a new role, revoking access to cargo or information etc.). If your business fails to implement mitigation measures, your Known Consignor approval may be withheld or revoked.

Personnel Security Flowchart – Who Needs an ASIC?



Step 1: Access to Cargo

Does this person ever have access to cargo alone or without supervision?

For example, as part of normal procedure or when personnel are on leave or sick.

YES

Is there a business reason why this person works alone?

YES

Is there any possibility this person could tamper with cargo?

You must evaluate this based on the measures and procedures of your business. For example, if this person is alone with cargo prior to processing, and your processing methods detects foreign objects, this presents a low risk. If the person is responsible for consolidating cargo after processing, the risk may be higher.

YES

Are there effective mitigation measures and procedures in place to monitor this person while working alone?

For example, monitored security cameras.

YES

Continue to Step 2

NO

NO

NO

NO

CHANGE IN OPERATIONAL POLICY

This situation is a potential security risk. You may want to modify your business policy to eliminate this risk before completing the personnel security assessment process.

NO CHANGE IN OPERATIONAL POLICY

ASIC required

Step 2: Access to Security Sensitive Information

Does this person ever have access to security sensitive information?

YES

Is access to security sensitive information necessary for this person to perform their job?

YES

Are there effective security measures and procedures in place to monitor and record access to, copying of and/or distribution of, security sensitive information?

YES

Is the range of information this person can access on their own of low risk in isolation?

Low risk in isolation means that the range of information the individual can access by themselves is of low value to a potential attacker. Information fitting this definition may be incomplete, unable to be accessed far in advance and only include the details that are necessary for the person to perform their job. This assessment will depend on your business context and the access level of the individual.

YES

NO

NO

NO

NO

ASIC optional

PART C – TRAINING

Required Training

Security Awareness Training (Q36)

As a minimum**, all individuals with access to cargo or security sensitive information** must receive **security awareness training** that meets **the Department's specified learning outcomes**.

All Individuals with Access to Cargo or Security Sensitive Information

This includes all personnel and contractors involved in all stages of processing your cargo (e.g. manufacturing, packing and loading), as well as cargo delivery drivers, administrative personnel with access to security sensitive information, and managerial personnel with oversight of business processes.

Security Awareness Training Options

To meet this training requirement, you can either:

1. use the Department's free online eLearning module;
2. design and deliver your training in-house; or
3. use training delivered by a third party.

The Department's free online eLearning module is the recommended way to meet this training requirement if you do not already deliver similar training. If you elect to use the Department's free online eLearning module, you will be provided access to the module once the Department has assessed your application.

However, if your business already has training or induction packages (either delivered in-house or by a third-party), you may instead choose to incorporate content into these packages that meets the Department's specified learning outcomes. You will be provided guidance on developing training once the Department has assessed your application.

Learning Outcomes

Upon completion of the security awareness training, individuals should be able to:

1. describe the current threat context to aviation and air cargo;
2. explain the roles played by industry and government in protecting air cargo;
3. follow and apply their workplace procedures to protect the security of air cargo;
4. identify suspicious activities, behaviour and cargo;
5. respond to and report suspicious activities, behaviour and cargo; and
6. keep cargo secure through basic facility, information and personnel security measures.

The security awareness training must also specifically address how to identify improvised explosive devices and trusted insiders.

At validation and during future compliance audits, the Department may ask you to provide evidence that the security awareness training you use meets these learning outcomes.

Nominated Contact Officer Training (Q37)

In addition to security awareness training, the **nominated contact officer** in your business is **required** to undertake more detailed training regarding the security outcomes of the Known Consignor Scheme.

You will have to develop your own nominated contact officer training. You will be provided guidance on developing training once the Department has assessed your application.

Learning Outcomes

Upon completion of the nominated contact officer training, the individual should be able to demonstrate an awareness of, and the capacity to comply with:

1. your business's general responsibility to contribute to the maintenance of aviation security;
2. your business's approach to managing aviation security within its organisation;
3. the Aviation Transport Security Regulations 2005; and
4. the Known Consignor Security Program (issued to your business on approval as a Known Consignor).

At validation and during future compliance audits, the Department may ask you to provide evidence that the security awareness training you use meets these learning outcomes.

Role-specific Training (Q38)

It is **recommended** that Known Consignors also deliver **role-specific training** to individuals with specific security duties. These security duties will differ according to how you structure your business.

You will be provided guidance on developing training once the Department has assessed your application.

While the Department does not prescribe specific learning outcomes, as a guide you should ensure that:

- personnel transporting secure cargo via road transportation know how to keep cargo secure;

- personnel who dispatch or receive goods know how to ensure the security of cargo; and
- security managers or supervisors know how to respond to security incidents, and how to set and review company security policies effectively.

In this part of the Application Form, you should detail the specific security duties undertaken by individuals in your business, and the training they receive. The following is an example:

Security Duties/Roles	**Training Topics/Details**
Cargo delivery drivers	Securing company trucks Securing transfer of cargo
Security manager	Basic audit training Identifying trusted insider training Company security policy training

Alternatively, you may indicate that no further role-specific training is required due to the nature of your operations.

PART D – CHAIN OF CUSTODY

Chain of custody concerns the security of cargo along the supply chain. The Department requires Known Consignors to be aware of, and implement, measures and procedures to ensure there is a secure chain of custody for cargo leaving their nominated site/s. For many businesses, measures and procedures already in place to prevent theft and contamination may go a long way to meeting the security outcomes outlined below.

Ground Transport (Q39)

When you fill out this section of the Application Form, you should tick the relevant boxes. More than one applicable box may apply to your business.

Depending on whether you transport your cargo yourself, use a RACA or an AACA, or use an unregulated entity, there may be additional requirements on your business to ensure the security of your cargo in transit.

I Will Transport My Cargo Myself

If you intend to use your own vehicle/s and driver/s to transport your cargo, in Q40, in addition to describing the measures and procedures you will have in place to secure your cargo from interference while it is in transit, you will need to describe the **measures and procedures you will have in place to secure the vehicle/s (both on site and in transit)**.

I Will Use a RACA or an AACA to Transport My Cargo

If you intend to engage a RACA or an AACA to transport your cargo, you must provide the details of the RACA or AACA at **Appendix A**. The Department directly regulates RACAs and AACAs and it is their regulatory responsibility to keep cargo secure once it is in their possession.

In Q40, in addition to describing measures and procedures you will have in place to secure your cargo from interference while it is in transit, you will need to describe **how you verify the AACA/RACA status of your transport provider, including verifying the identity of the driver/s.**

For a list of RACAs and AACAs, visit https://infrastructure.gov.au/security/regulatory-guidance/index.aspx.

I Will Enter into a Signed Undertaking with an Unregulated Entity to Transport My Cargo on My Behalf

If you intend to enter into a signed undertaking with an unregulated entity to transport your cargo on your behalf, in Q40, in addition to describing the measures and procedures you will have in place to secure your cargo from interference while it is in transit, you will need to describe the **measures and procedures you will have in place to secure the vehicle/s (both on site and in transit)** and **how you verify the identity/employment status of the unregulated entity's drivers.**

If you intend to use an unregulated entity to transport your cargo, you and the Department must be confident that the unregulated entity can keep your cargo secure. You must provide the unregulated entity with an undertaking, using the form at **Appendix B**, which must be signed by both you and the unregulated entity. It is your responsibility, not the unregulated entity's, to ensure that the undertaking is adhered to.

Any unregulated entity used to transport your cargo must:

- have a signed undertaking with your business;
- make a copy of the signed undertaking available to the Department when requested;
- be covered under your Known Consignor Security Program;
- understand their responsibilities under your Known Consignor Security Program;
- be identifiable as working for your business (e.g. issued with company ID, contractor ID); and
- be subject to the same training requirements as described in **Part C** above.

This provides confidence to the Department and your business that the unregulated entity will maintain the security of your cargo.

If you are not comfortable accepting liability for the consequences of any interference with your cargo while it is in transit with the unregulated entity, the Department advises you discuss with them the option of becoming a RACA or an AACA. More information can be found at https://infrastructure.gov.au/security/air-cargo/

Security of Cargo (Q40)

All Known Consignors have a responsibility to ensure that the security of cargo leaving their nominated site/s is maintained. This section of the Application Form asks you to identify measures and procedures you will have in place to secure your cargo from interference while it is in transit.

Possible measures and procedures to secure your cargo from interference while it is in transit include:

- locking a vehicle's cargo compartment in such a way that makes it inaccessible to the driver and intruders (such as transmitting a combination lock code to the next business along the supply chain or using a keyed padlock for which only the known consignor and the next business along the supply chain have keys);
- requiring the driver to hold a valid ASIC;
- measures and procedures to secure vehicles in transit (such as tamper-evident compartment seals, vehicle alarms, a direct service agreement, no stopping during journeys, vehicle escorts, remote monitoring, or conducting a post-transport check for any tampering of cargo);
- sealing cargo with plain tape and using a unique stamp across the tape or signing across it, using company tape, using one-time numbered seals, or using other tamper-evident tapes or seals;
- engaging a RACA or an AACA to transport your cargo; or
- other factors (such the distance/time taken to travel from your nominated site/s to the next business along the supply chain, or the nature of your cargo).

As Known Consignors are responsible for issuing Security Declarations for cleared cargo, there is also an increased expectation that they are aware of and verify that the security measures and procedures that their ground transport provider uses are effective.

More than one of the possible measures and procedures described above may be used in combination to secure your cargo. If you choose not to use these, you must be able to demonstrate other measures and procedures you will have in place to secure your cargo.

PART E - INCIDENT RESPONSE AND QUALITY ASSURANCE

Incident Response and Reporting (Q41-42)

Known Consignors are required under the *Aviation Transport Security Act 2004* to report security incidents. Your incident response and reporting procedure requirements are documented in the Application Form.

Quality Assurance (Q43)

Once approved, Known Consignors are also required to implement quality assurance activities to ensure that all security measures and procedures remain effective and relevant. While your security measures and procedures in place today may be effective, this can change due to changes in operations, personnel, or the wider security environment. As such, it is important that your security measures are reviewed in a formalised way, on a regular basis.

If you have existing quality assurance procedures in place, you may choose to supplement these with a security review component. Examples of quality assurance activities include internal and external audits and reviews.

Some businesses may have memberships in industry associations which require them to operate to certain standards. If you are one of these businesses and you are regularly subjected to an audit for your accreditation or membership, provided that the audit covers aspects of security that you have outlined in your Application Form, you can use this to demonstrate that you meet this requirement.

The approval of Known Consignors can be for a period up to a maximum of five years. Known Consignors must undertake an audit and/or review of their security measures and procedures at least once during their approval period. More reviews may be required if your business undergoes significant operational changes during your Known Consignor approval period. Known Consignors must also keep records of these activities including corrective actions taken.

DECLARATION

The Department cannot begin assessing your Application Form until you complete the declaration.

APPENDICES

You must also provide sufficient information in either **Appendix A** or **Appendix C** on the ground transport entities that you use to transport your cargo.

Appendix D is where you may enter any further information which you believe will assist your application. If you have included attachments with your Application Form, this is where you can detail what is included in those attachments, and why you have included them.

Still unsure how you should complete the form?

Email: knownconsignor@infrastructure.gov.au

Call: **1300 791 581**