

## **EXPLANATORY STATEMENT**

(Issued by the Authority of the Minister for Infrastructure and Transport)

Subject – *Aviation Transport Security Act 2004*

*Aviation Transport Security Amendment (Cargo) Regulation 2016*

The *Aviation Transport Security Act 2004* (the Act) and the Aviation Transport Security Regulations 2005 (the Principal Regulations) establish a regulatory framework to safeguard against unlawful interference with civil aviation in Australia. To achieve this purpose, the Act establishes minimum security requirements for civil aviation in Australia by imposing obligations on persons engaged in civil aviation related activities. This includes persons engaged in the handling and transport of air cargo. The Act and the Principal Regulations also give effect to Australia's obligations under Annex 17 to the Convention on International Civil Aviation (the Chicago Convention).

Subsection 133(1) of the Act provides that the Governor-General may make regulations prescribing matters required or permitted by the Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

On 26 November 2015, Parliament passed the *Aviation Transport Security Amendment (Cargo) Bill 2015*, establishing the legislative framework for the *Aviation Transport Security Amendment (Cargo) Regulation 2016* (the amending Regulation).

The purpose of the amending Regulation is to amend the Principal Regulations to establish the regulatory arrangements for the Australian export and freight forwarding industry to meet United States domestic legislation security requirements on air cargo bound for the United States.

From 1 July 2017, 100 per cent of United States bound air cargo originating from Australia and carried on a prescribed aircraft must be examined at the piece level to ensure that it does not contain unauthorised explosives. This means that each individual box, carton or other item in a shipment must be examined by technology or physically inspected before it is loaded onto a United States-bound aircraft. Currently, United States-bound air cargo may be examined following a degree of consolidation under the specifications of an Air Cargo Examination Notice issued under the Principle Regulations. From 1 July 2017, cargo will need to be examined by a designated Regulated Air Cargo Agent (RACA) at the piece level before it can be loaded onto an aircraft destined for the United States.

The amendments will provide for cargo to be cleared by an approved known consignor as an alternative to piece level examination using technology or physical examination. This will provide an effective and efficient means of recognising whole of supply chain security arrangements where industry can demonstrate appropriate security measures.

Under the known consignor scheme, approved businesses will need to demonstrate controls which ensure the security of air cargo from a facility that originates air cargo. This requires

goods to be produced, packaged, stored, transported and handled in a manner that ensures their integrity, and protects them from unlawful interference from their point of origin right through to loading onto an aircraft. Businesses wishing to become known consignors will need to apply to the Secretary and demonstrate that their facility can securely originate cargo.

The cargo clearance provisions in the Principle Regulation have been changed to enhance security outcomes and provide clarity for industry. Cargo may only receive clearance and be cleared under three circumstances, these include: if cargo was examined under a notice issued by the Secretary; if cargo originated from a known consignor; or if cargo does not require examination under a notice issued under paragraph 44B(2)(b)(i) of the Act. The previous option of clearing cargo under a Transport Security Program (TSP) will no longer be an acceptable form of clearance, as this does not subject cargo to a sufficient level of security scrutiny. This change provides industry and the regulator with a clear point to identify where cargo has received clearance. The amending Regulation also strengthens the role that security declarations play in indicating cargo's cleared status. Security declarations can only be issued for cargo that has undergone examination by a RACA (examined under a notice issued by the Secretary) or that has originated from a known consignor.

The current arrangements for TSPs in the supply chain have been removed to reduce administrative burden for industry. TSPs have been replaced by approved security programs for known consignors, RACAs and Accredited Air Cargo Agents (AACAs). The new security program framework allows the programs to be more responsive to changes in operations or security risk and aligns their duration to the regulatory accreditation period of the regulated business.

The amending Regulation also replaces previous references to suspect cargo with high risk cargo. This change will increase security outcomes by removing any uncertainty for aviation industry participants about how high risk cargo should be identified, handled and treated, ensuring that Australia's air cargo security regulatory framework continues to align with international standards and obligations under the Chicago Convention.

Transitional provisions are provided for in the amending Regulation to transition eligible RACAs to AACAs, ensuring better identification of when cargo is cleared and reducing administrative burden for industry.

Industry and government stakeholders have been consulted on the amending Regulation through:

- The Cargo Working Group (CWG), chaired by the Department of Infrastructure and Regional Development (the Department) - The CWG includes airlines, general and express freight forwarders, exporters and government agencies. A discussion paper was circulated to members of the CWG in May 2015, outlining proposed regulatory responses to meet United States air cargo security requirements. Subsequently, the Department chaired two CWG meetings to discuss these policy proposals and sought feedback on the proposed changes.

- Public consultation - the Department conducted public consultation sessions for the freight forwarding and export industries in Brisbane, Melbourne, Sydney, Adelaide, and Perth from August to September 2016 to seek feedback on the amending Regulation. The Department also released the exposure draft on the Department's website and sought comments from the wider public.
- Inter Departmental Committee (IDC) meetings - the Department consulted with other Government agencies on strengthening United States-bound air cargo arrangements through regular IDC meetings. The IDC consists of the Treasury; the Department of the Prime Minister and Cabinet; the Department of Foreign Affairs and Trade; the Department of Immigration and Border Protection; the Department of Agriculture and Water Resources; and the Department of Industry, Innovation and Science.

The exposure draft of the amending Regulation received six submissions. The submissions generally related to questions about how the known consignor, RACA and AACA schemes will be administered and how cargo will maintain its cleared status throughout the supply chain. In response, the Department will continue to work closely with industry bodies to provide further clarification on the operation of the amending Regulation and guidance materials.

The Statement of Compatibility with Human rights is set out in [Attachment A](#). Details of the amending Regulation are set out in [Attachment B](#).

The Office of Best Practice Regulation was consulted and the Regulation Impact Statement (Part II) is set out in [Attachment C](#). Part I of the Regulation Impact Statement can be found in the Explanatory Memorandum for the *Aviation Transport Security Amendment (Cargo) Bill 2015*.

The Act does not specify any conditions that need to be satisfied before the power to make the amending Regulation is exercised.

The amending Regulation is a legislative instrument for the purposes of the *Legislative Instruments Act 2003*.

The amending Regulation contains two commencement dates. Sections 1-4 and Schedule 1 commence on 1 November 2016. Schedule 2 commences on 1 July 2017.

Authority: Subsection 133(1) of the *Aviation Transport Security Act 2004*

**Statement of Compatibility with Human Rights**

*Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011*

**Aviation Transport Security Amendment (Cargo) Regulation 2016**

This Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

**Overview of the Legislative Instrument**

The Legislative Instrument amends the Principal Regulations to ensure Australia's air cargo security arrangements align with international standards and United States requirements for inbound air cargo. The amendments also introduce a substantive known consignor framework for exporters to originate cleared cargo, streamline cargo clearance provisions and establish a transitional arrangement for Regulated Air Cargo Agents (RACAs) to Accredited Air Cargo Agents (AACAs).

**Human rights implications**

*Presumption of innocence*

The presumption of innocence is affected by this instrument as it creates, updates and removes strict liability offences in the Principle Regulations. The strict liability offences engage the right to the presumption of innocence, which is a fundamental principle of the common law and is contained in article 14(2) of the International Covenant on Civil and Political Rights.

In relation to the creation of new strict liability offences, these are under regulations 4.41F, 4.41H and 4.41ZG. The offence under regulation 4.41F requires known consignors and RACAs to appropriately clear cargo when issuing a security declaration. The offence under subregulation 4.41F(5) also penalises persons who are not RACAs or known consignors issuing a security declaration. The integrity of the security declaration system and the wider supply chain will be undermined if persons who are not regulated as RACAs or known consignors are issuing security declarations. The consequence of this may lead to cargo that has not received clearance to be loaded onto aircraft.

Regulation 4.41H relates to the new requirement of keeping security declaration records. It is important that RACAs and known consignors keep records of their security declarations for 90 days to provide evidence that they have cleared cargo and to assist the regulator in compliance and investigative activities. This is not a significant burden as industry will

already have the systems in place to keep records of its export or freight forwarding information.

Regulation 4.41ZG relates to a known consignor's obligation to comply with a security program in force for the known consignor. This requirement ensures that known consignors, who originate cleared cargo, comply with the security measures under their program.

The defence of reasonable excuse for AACAs under Subregulation 4.51G(3) has been removed. The defence of reasonable excuse was not aligned to similar offences for RACAs and known consignors in not complying with their security program. By removing this defence, the amending Regulation creates a uniform strict liability offence framework for AACAs, RACAs and known consignors.

While these offences engage the right to the presumption of innocence, there are several elements that demonstrate the imposition on this right is reasonable and necessary.

The objective of these above offences is to ensure the secure transport of Australia's air cargo. Unlawful interference with aviation, such as a successful attack via explosives inserted in air cargo, could severely impact Australia and Australian interests. Including a provable fault element would likely undermine the government's objective to safeguard against unlawful interference with aviation, as it would be difficult to prove fault in most instances. The strict liability offences ensure that they are an effective deterrent to contraventions of the air cargo security framework created in this Legislative Instrument.

This Legislative Instrument puts systems in place that will be a necessary requirement for any regulated business wishing to originate, examine or handle cargo. The offences created by this Legislative Instrument relate to the proper implementation of these systems. As such RACAs, AACAs and known consignors could be reasonably expected to know these obligations because of the regulatory regime governing the industry. The security programs issued to RACAs, AACAs and known consignors place these regulated businesses on notice in relation to the requirements they must comply with. Safeguards are also placed in the amending Regulation to enable these businesses to amend their security programs so that they accurately reflect their operations.

The new strict liability offences are not severe. They are limited to 100 penalty units for regulation 4.41ZG, subregulation 4.41F(1), 4.41F(2), 4.41F(3) and 4.41F(4), and 50 penalty units for regulation 4.41H and subregulation 4.41F(5). They also do not include imprisonment. The offences will be committed by the regulated business and not employees of the regulated business.

Furthermore, a regulated business that breaches any strict liability provisions may be issued with an infringement notice under regulation 7.04 of the Principle Regulations. This means the Department of Infrastructure and Regional Development (the Department) has available, a variety of enforcement measures to ensure compliance with the provisions in the amending

Regulation. For example, this could allow authorised persons to issue an infringement notice in lieu of a charge for a criminal offence for minor breaches of the relevant strict liability provisions.

The offences under regulations 4.41G, 4.41K, 4.46G, 4.46H and 4.51J are updates for offences under previous regulations 4.41F, 4.41H, 4.41K, 4.46 and section 14 of the *Aviation Transport Security Act 2004* (for RACAs not complying with their transport security program). As such, these are not new offences, but they have been updated in accordance with the amending Regulation.

The strict liability offences under previous regulations 4.41G, 4.45A and 4.51H have been removed. There is no longer a regulatory requirement for regulated businesses to issue chain of custody statements under previous regulation 4.41G. Furthermore, RACAs and AACAs do not need to notify the Secretary of changes to their application form under the previous regulations 4.45A and 4.51H.

The Department has consulted with the Attorney-General's Department on each of these strict liability provisions and they accord with policies contained in the Attorney-General's Department's *A Guide to Framing Commonwealth Offences*.

### **Conclusion**

This Legislative Instrument is compatible with human rights because to the extent that it affects human rights in relation to the presumption of innocence, those effects are reasonable and necessary to safeguard against unlawful interference with aviation.

DARREN CHESTER

Minister for Infrastructure and Transport

**Details of the *Aviation Transport Security Amendment (Cargo) Regulation 2016***

**Section 1 – Name**

This section provides that the name of the amending Regulation is the *Aviation Transport Security Amendment (Cargo) Regulation 2016*.

**Section 2 – Commencement**

This section provides that the amending Regulation has a split commencement date. Sections 1 to 4 and Schedule 1 will commence on 1 November 2016. Schedule 2 will commence on 1 July 2017. The purpose of this split commencement is to enable the known consignor scheme to come into effect on 1 November 2016, along with new clearance requirements. This will assist industry to adjust to the new requirements before specific requirements for United States bound cargo are changed on 1 July 2017.

**Section 3 – Authority**

This section provides that the amending Regulation is made under the *Aviation Transport Security Act 2004*.

**Section 4 – Schedules**

This section provides that the *Aviation Transport Security Regulations 2005* are to be amended as set out in the Schedules to the amending Regulation.

**Schedule 1—Amendments commencing 1 November 2016**

**Part 1—Amendments**

***Aviation Transport Security Regulations 2005***

**Item [1] – Regulation 1.03 (definition of AACA security program)**

This item omits “regulation 4.49” and substitutes “regulation 4.51F” to ensure that the definition of an AACA security program is accurate.

**Item [2] – Regulation 1.03 (definition of chain of custody statement)**

This item repeals the definition of a chain of custody statement. Under the amending Regulation, chain of custody statements will no longer be required. However, this does not prevent regulated businesses from using the chain of custody statement or similar documentation for commercial or other practical reasons. Cargo will need to be kept securely throughout the supply chain by regulated businesses under their security programs.

### **Item [3] – Regulations 1.03 (definition of class of regulated business)**

This item adds the origination of cargo as one of the functions of a regulated business.

### **Item [4] – Regulation 1.03**

This item moves the definition of international cargo from previous regulation 4.41C and places it in the definitions under regulation 1.03.

This item defines a known consignor security program in the definitions. A known consignor security program is a program which is provided under regulation 4.41Z by the Secretary of the Department (the Secretary) and also includes such a security program as varied under the Aviation Transport Security Regulations 2005.

This item defines the term originate in relation to regulation 1.03A.

This item defines a RACA security program as a security program provided by the Secretary to the RACA under regulation 4.46, and includes such a security program as varied under the amending Regulation.

### **Item [5] – Regulation 1.03 (after paragraph (b) of the definition of regulated business)**

This item provides for a known consignor to be a regulated business under the amending Regulation.

### **Item [6] – Regulation 1.03**

This item inserts definitions for a regulation 4.41J and 4.41JA notice, as well as clarifying security programs in relation to a known consignor, a RACA, an AACA and an aviation industry participant who is an operator of a security controlled airport, an operator of a prescribed air service or Airservices Australia.

This item also provides for the definition of an unauthorised explosive. The definition encapsulates all forms of explosives and explosive devices, except where the explosives are authorised under a notice issued by the Secretary under subparagraph 44B(2)(b)(i) of the Act.

### **Item [7] – Regulation 1.03**

#### *1.03A Meaning of originate in relation to known consignors*

This item defines what is meant by originating cargo for known consignors. Under paragraph 1.03A(a) cargo originates with a known consignor in the circumstances where the known consignor makes, manufactures, assembles or otherwise produces the goods, which are, or reasonably likely to become cargo. In these circumstances, the cargo may be goods that ordinarily undergo some form of processing to become the finished product. For example, paragraph 1.03A(a) may include cargo such as beef, pharmaceutical products, machinery or fish, which fall under the circumstances of cargo that originates with a known consignor.



Under paragraph 1.03A(b), cargo may also originate from a known consignor even under circumstances where the known consignor has not processed or manufactured the goods. This subparagraph captures the circumstances where the known consignor has control of the goods and may conduct repackaging or consolidation of the goods into cargo for export purposes. For example, paragraph 1.03A(b) may include circumstances where cargo originates with a known consignor if the known consignor acts as a removalist company, a food treatment company that does not make the goods but treats the goods to meet phytosanitary requirements, or a third party logistics company that repackages or consolidates cargo for export.

#### **Item [8] – Regulation 2.03**

This item removes the requirement for RACAs to have a transport security program (TSP). However, this does not make any changes to the requirement for other aviation industry participants under the Act and Airservices Australia under the Principle Regulations to have a TSP.

#### **Item [9] – Regulation 2.41(5)**

This item removes references to suspect cargo under an aircraft operator’s transport security program under the Principle Regulations and replaces them with high risk cargo.

#### **Item [10] – Division 2.4**

This item repeals Division 2.4 in the Principle Regulations to remove the previous regulatory requirements for RACA TSPs. The new requirements for RACA security programs are prescribed under regulation 4.46.

#### **Item [11] – Regulations 4.41C to 4.41H**

Item 11 removes regulations 4.41C to 4.41H and replaces them with a new clearance framework.

##### *4.41C When cargo that has not been examined may receive clearance*

Under regulation 4.41C, cargo may receive clearance without being examined under certain circumstances. Under this amendment, cargo that originates with a known consignor does not need to be examined to receive clearance and subsequently be cleared. This construct provides known consignors with the ability to originate cleared cargo. Secondly, cargo that falls under a notice issued by the Secretary under subparagraph 44B(2)(b)(i) of the Act may also receive clearance without being examined.

##### *4.41CA Requirements for cargo to receive clearance*

Under regulation 4.41CA, for cargo to receive clearance it must go through one of two channels. The first channel of clearance is for cargo to be examined by a RACA in accordance with a notice issued under regulation 4.41J or regulation 4.41JA and that the RACA has handled that cargo in accordance with requirements under its security program.

Under this channel, the cargo must also have a security declaration and not contain any explosives. This means that cargo that is to receive clearance through examination cannot contain any explosives. In order for explosives that are not classified as unauthorised explosives to receive clearance, it must go through the second channel of clearance under subregulation 4.41CA(3).

The second channel of clearance provides for cargo that originates from a known consignor or cargo that is prescribed under a written notice issued by the Secretary under subparagraph 44B(2)(b)(i) of the Act to receive clearance. As additional requirements to receive clearance, the cargo must be handled by either the known consignor or a RACA in accordance with a security program in force, has a security declaration and not contain unauthorised explosives. For example, this subregulation may be used to provide for certain types of dangerous goods (which meet dangerous goods handling requirements and are authorised by the Secretary under a notice issued under subparagraph 44B(2)(b)(i)) to receive clearance without examination.

#### *4.41D Meaning of security declaration*

Under regulation 4.41D the format of the security declaration is aligned to international standards and could be used in a paper or electronic format.

The notation in regulation 4.41D clarifies that cargo may only be examined by a RACA, and that for cargo to receive clearance, it must have received clearance and subsequently been handled in accordance with the regulations. Requirements to handle cargo securely can be found under the security programs of RACAs, AACAs and known consignors.

Regulation 4.41D does not preclude any further information from being inserted or annotated in the security declaration, as long as it does not compromise the requirements prescribed under regulation 4.41D.

#### *4.41F Offence—issuing a security declaration in certain circumstances*

Under subregulation 4.41F(1), a known consignor commits an offence of strict liability if it issues a security declaration for cargo and the cargo did not originate with the known consignor or was not included in a notice issued by the Secretary under subparagraph 44B(2)(b)(i) of the Act. This offence is designed to capture instances where a known consignor issues a security declaration for cargo that it has not originated, such as instances where a known consignor issues a security declaration for another company or person. The offence is of strict liability as it is intended to capture acts of fraud or negligence, where a known consignor is engaged in issuing false declarations. The penalty of 100 penalty units is consistent with section 44C(4) of the Act and is appropriate given the nature of the offence. The security declaration is critical to determining whether cargo has received clearance and any deliberate falsification or negligent error in issuing the declaration has the potential to enable cargo that has not received clearance to be uplifted onto aircraft. This could severely undermine industry confidence in the supply chain and potentially lead to catastrophic consequences if an unauthorised explosive was inserted into cargo.

Under subregulation 4.41F(2), a known consignor commits an offence of strict liability if it issues a security declaration for cargo and the known consignor has not treated the cargo in accordance with its security program in force. The imposition of the strict liability offence is consistent with the principles in *A Guide to Framing Commonwealth Offences*. This is a specific offence which has strict criteria. Requiring proof of fault in this instance would undermine deterrence. It would be particularly difficult to prove fault in these circumstances as extensive documentation regarding the origination and handling of cargo would be required to establish the fault elements of the regulated business. Under the known consignor security program, known consignors are placed on notice to guard against the possibility of any contravention under this subregulation. If fault was required for this offence, significant resources would be needed for enforcement and this would significantly impact on the resources available to ensure the security of the air cargo supply chain. The penalty of 100 penalty units is consistent with section 44C(4) of the Act and is appropriate given the nature of the offence. The security declaration is critical to determining whether cargo has received clearance. Any deliberate falsification or negligent error in issuing the declaration has the potential to enable cargo that has not received clearance to be uplifted onto aircraft. This could severely undermine industry confidence in the supply chain and potentially lead to catastrophic consequences if an unauthorised explosive was inserted into cargo.

Under subregulation 4.41F(3), a RACA commits an offence of strict liability if it issues a security declaration for cargo and the cargo was not examined by the RACA in accordance with a notice issued under 4.41J or a notice issued under 4.41JA, or cargo that was not included in a notice issued by the Secretary under subparagraph 44B(2)(b)(i) of the Act. This offence captures instances where a RACA issues a security declaration for cargo that it has not examined (where the cargo required examination to receive clearance). The offence is of strict liability as it is important that RACAs do not issue false security declarations for cargo which has not been examined under a notice issued under regulation 4.41J or 4.41JA. Under the RACA security program, RACAs are also placed on notice to guard against the possibility of any contravention under this subregulation. If fault was required for this offence, significant resources would be needed for enforcement and this would significantly impact on the resources available to ensure the security of the air cargo supply chain. The penalty of 100 penalty units is consistent with section 44C(4) of the Act and is appropriate given the nature of the offence. The security declaration is critical to determining whether cargo has received clearance. Any deliberate falsification or negligent error in issuing the declaration has the potential to enable cargo that has not received clearance to be uplifted onto aircraft. This could severely undermine industry confidence in the supply chain and potentially lead to catastrophic consequences if an unauthorised explosive was inserted into cargo.

Under subregulation 4.41F(4), a RACA commits an offence of strict liability if it issues a security declaration for cargo and the RACA has not treated the cargo in accordance with the RACA's security program. This offence puts a RACA on notice that they must treat cargo in accordance with their security program. For example, these measures and procedures may require RACAs to keep cargo secure after it has been examined. The imposition of the strict

liability offence here is consistent with the principles in *A Guide to Framing Commonwealth Offences*. This is a specific offence which has strict criteria. Requiring proof of fault in this instance would undermine deterrence and impact upon industry and the general public's confidence in the way cargo is examined. It would be particularly difficult to prove fault in these circumstances as extensive documentation regarding examination and handling of cargo would be required to establish the fault elements of the regulated business. If fault was required for this offence, significant resources would be needed for enforcement and this would significantly impact on the resources available to ensure the security of the air cargo supply chain. The penalty of 100 penalty units is consistent with section 44C(4) of the Act and is appropriate given the nature of the offence. The security declaration is critical to determining whether cargo has received clearance and any deliberate falsification or negligent error in issuing the declaration has the potential to enable cargo that has not received clearance to be uplifted onto aircraft. This could severely undermine industry confidence in the supply chain and potentially lead to catastrophic consequences if an unauthorised explosive was inserted into cargo.

Under subregulation 4.41F(5), a person commits an offence of strict liability if the person purports to issue a security declaration for cargo and the person is not a known consignor or a RACA. This offence is intended to deter persons who are not known consignors or RACAs from issuing security declarations. Under subregulation 4.41F(5), security declarations could only be issued by RACAs and known consignors. This offence is of strict liability as it is required to maintain the validity of security declarations and the integrity of the secure supply chain. The imposition of the strict liability offence here is consistent with the principles in *A Guide to Framing Commonwealth Offences*. Regulated businesses (excluding RACAs and known consignors) are also placed on notice to guard against the possibility of any contravention. If fault was required for this offence, significant resources would be needed for enforcement and this would significantly impact on the resources available to ensure the security of the air cargo supply chain. The security declaration is critical to determining whether cargo has received clearance. Any deliberate falsification or negligent error, especially from unregulated persons in issuing the declaration has the potential to enable cargo that has not received clearance to be uplifted onto aircraft. This could severely undermine industry confidence in the supply chain and potentially lead to catastrophic consequences if an unauthorised explosive was inserted into cargo.

#### *4.41G Offence—loading cargo on aircraft if the cargo does not have a security declaration*

Regulation 4.41G replaces previous regulation 4.41H. Under subregulation 4.41G(1), a regulated business commits an offence of strict liability if it loads cargo onto a flight bound for an international flight on a prescribed aircraft and the regulated business does not have a security declaration for the cargo. This offence removes the need to have a chain of custody statement for loading cargo under previous regulation 4.41H. This offence is of strict liability to ensure that only cargo that has been cleared by a RACA or a known consignor with a security declaration can be loaded onto an aircraft. The consequences of an unauthorised explosive being loaded onto an aircraft makes this strict liability offence appropriate. The strict liability offence serves as a deterrent, to prevent regulated businesses loading cargo that

has not been cleared. Regulated businesses are put on notice to only load cargo to which a security declaration has been issued. The penalty of 100 penalty units for regulated businesses that are not AACAs and 50 penalty units for AACAs is consistent with section 44C(4) of the Act and is appropriate given the nature of the offence. At the final point of loading, cargo must be checked to see if it has received clearance. Loading cargo that does not have a security declaration could severely undermine industry confidence in the supply chain and potentially lead to catastrophic consequences if an unauthorised explosive was loaded onto an aircraft.

#### *4.41H Offence—failing to keep records of security declaration*

Under regulation 4.41H, it is an offence for a regulated business to not keep a record of the declaration for 90 days after issuing the declaration. The offence is a strict liability offence as keeping security declaration records is an important part of maintaining a secure air cargo supply chain and also serves investigatory and compliance functions. The imposition of the strict liability offence here is consistent with the principles in *A Guide to Framing Commonwealth Offences*. This is a specific offence which has strict criteria. Requiring proof of fault in this instance would undermine deterrence. Regulated businesses are placed on notice to guard against the possibility of any contravention. The penalty of 50 penalty units is appropriate given the critical need to maintain information on cargo's clearance status in the supply chain.

#### **Item [12] – Regulations 4.41J and 4.41K**

This item replaces previous regulations 4.41J and 4.41K to clarify that there are now two types of examination notices for the air cargo security supply chain.

#### *4.41J Notice for examination of cargo—examination requirements under this regulation*

Under regulation 4.41J, the Secretary may issue a written notice that sets out the requirements for examination of cargo. A notice made under regulation 4.41J may include one or more of the following: the types of cargo that must be examined; the records that must be kept; the methods, techniques and equipment that a RACA must use for examining cargo; who may examine cargo; procedures for dealing with cargo that has been examined; and any other matters the Secretary might consider relevant.

The notation under 4.41J explains that cargo may require examination in accordance with other requirements under regulation 4.41JA. Both 4.41J and 4.41JA provisions are designed to transition industry from 1 November 2016 to 30 June 2017. Once Schedule 2 commences, regulation 4.41J in Schedule 2 will become the new provision for examination of cargo for category 2 destinations.

#### *4.41JA Notice for examination of cargo—examination requirements under this regulation*

Under regulation 4.41JA, the Secretary may issue a written notice that sets examination requirements for the examination of cargo. While both 4.41JA and 4.41J provisions appear similar in Schedule 1, this construct provides a transitional phase to prepare industry for the

commencement of schedule 2 provisions. The notation under regulation 4.41JA provides context as to when the interim 4.41JA notice is used, and that it is to provide for examination requirements for countries that require certain inbound cargo examination requirements. Once Schedule 2 commences, regulation 4.41JA in Schedule 2 will become the new provision for examining cargo for category 1 destinations.

#### *4.41JB Revocation of notice issued under this Subdivision*

Regulation 4.41JB provides for a revocation mechanism of the notice issued under regulation 4.41J and 4.41JA. This is to clarify the administration of the notices and when they may be revoked by the Secretary.

#### *4.41K Offence—examination of cargo otherwise than in accordance with notice*

Under this sub-item, previous regulation 4.41K is modified to require RACAs to comply with the notice issued under 4.41J or 4.41JA in its entirety, rather than the previous limitation in relation to the examination of cargo in accordance with the notice. This strengthens the regulatory oversight for the examination of cargo, as examination plays a key part in enabling the clearance of cargo for uplift on to an aircraft. The penalty of 100 penalty units is consistent with previous regulation 4.41K and the strict liability used for this offence is appropriate. Not complying with the notice could severely undermine industry confidence in the supply chain and potentially lead to catastrophic consequences if an unauthorised explosive was inserted into cargo.

Furthermore, notices are documents that are highly technical in nature, referring to specific industry practices, equipment requirements and change regularly. It is appropriate to sub-delegate the offence to the notice as the Secretary needs to ensure industry can comply with highly technical requirements. These requirements would be impractical to list in the amending Regulation and would negatively impact security as the methods, equipment and techniques under a notice (should it be in the public domain) may be exploited by persons intending to circumvent these measures.

#### **Item [13] – After subdivision 4.1A.1A**

This new subdivision provides a framework for approving known consignors. Under regulation 4.41L, a known consignor is a person that carries on the business of originating cargo, which is defined under regulation 1.03A, and is also approved as a known consignor under regulation 4.41N.

The process of applying for approval as a known consignor is set out in regulation 4.41M. A person may apply to the Secretary to be approved as a known consignor if they carry out a business that originates cargo or intends to originate cargo. This enables persons that intend to originate cargo, but which have not yet started to originate cargo, to apply. Subregulation 4.41M(2) requires that the application be made on the application form approved by the Secretary and include the information required by the form.

After the form is lodged, the Secretary may request the applicant to provide further information in relation to the application, or agree to access for inspection one or more of the applicant's sites to gather further information. Subregulation 4.41M(3) enables the Department to inspect the applicant's site in order to validate information on the application form or gather any other information that is necessary in relation to the application. Requests made under subregulation 4.41M(3) must be in writing and specify the period within which the further information or access is to be provided.

Subregulation 4.41M(5) provides that an inspection may be conducted by an Australian Public Service (APS) employee, a person who is engaged as a consultant or contractor to perform services for the Department, or a law enforcement officer. The operation of this subregulation allows other APS employees, such as those trained in export or quality control (for example, customs officers, veterinary officers or quarantine officers), to conduct an inspection of an applicant's site.

The category of persons able to conduct an inspection is set to be broad to capture a variety of different government inspectors. This is appropriate under the circumstances due to:

- the need to meet the potential demand of known consignor applications to ensure that Australia's exports to the United States are not disrupted;
- the diversity of businesses applying to be approved as known consignors will require the Department to leverage off other agencies and their expertise;
- the non-intrusive nature of the inspections will limit the power of APS employees. That is, the persons conducting the inspections will not have any powers to enter premises or take information without agreement from the business;
- limiting the classification of APS employees would not be appropriate as the inspection may be conducted by staff from different classifications;
- limiting the category of APS employees may prevent APS employees from certain agencies from conducting an inspection, where that agency has expertise in inspecting a particular industry; and
- the dispersed nature of exporters in Australia will potentially require inspectors to be sourced from regional offices where the broad pool of Commonwealth employees is required to efficiently conduct inspections.

Furthermore, contractors or consultants engaged by the Department may also be able to conduct an inspection on behalf of the Secretary. This will provide the Department with flexible options to meet the demand for inspections and reduce the risk of delay in approving known consignors.

While the inspection is upon request by the Secretary, under subregulation 4.41M(6), if an applicant does not provide access, the Secretary may refuse to consider the application any further. This refusal also applies to circumstances where the applicant does not provide further information as requested by the Secretary.

The decision on application is governed by regulation 4.41N. In making a decision, the Secretary may take into account anything submitted in the application and any further information obtained as a result of a request for further information or information obtained during an inspection. As cargo may be cleared without examination if it originates from a known consignor, the standard of security expected is high. Subregulation 4.41N(2) also provides for the Secretary to consider any other information relevant to make a decision on the application. For example, this framework allows the Secretary to consider the holistic security situation for an application. The Secretary may refuse to approve an application even if the application was filled out correctly. It may be that the inspection resulted in new information that highlighted new risks that were not evident in the application form.

Under subregulation 4.41N(3), the Secretary's decision on the application must be made in writing. This decision must be made within 90 days of the application being made. However, the 90 day rule is subject to "stopping the clock", which is covered under subregulation 4.41N(6).

If the Secretary does not make a decision under subregulation 4.41N(1) within 90 days of the application being made, the Secretary is taken to have refused to approve the applicant as a known consignor at the end of that period. Subregulation 4.41N(3) will also need to take into account the stop clock mechanism in the next paragraphs.

The stop clock under subregulation 4.41N(6) operates in two circumstances: where the Secretary has requested further information under paragraph 4.41M(3)(a), or requested access for inspection under paragraph 4.41M(3)(b). Once the Secretary has made a request in these circumstances, the stop clock is activated for each request that is made. The stop clock halts the 90 day decision period until further information under paragraph 4.41M(3)(a) is given or an inspection under paragraph 4.41M(3)(b) is conducted. The end period may also be given a date within the written notice under paragraph 4.41M(3)(a) or 4.41M(3)(b). The stop clock mechanism provides time, where necessary, for the Department to review further information or to conduct inspections.

For example, the stop clock mechanism is worked through below for a fruit exporter. At the beginning, the fruit exporter applies to become a known consignor. The Secretary may ask the known consignor applicant about additional security measures relating to personnel security at the fruit packing facility. Once this request is provided in writing, the 90 day decision period is immediately halted on the day on which the written notice is given. It may take the fruit exporter two weeks to provide this information, and the two weeks do not count towards the 90 day decision making period. When the applicant provides the requested information, the 90 day decision period begins to countdown again. At the 45 day mark, the stop clock may be triggered again by the Secretary requesting an inspection to the applicant's site. Due to seasonal factors, an inspection may not be possible until summer, which is when the fruit is actually processed. This means that the stop clock can last for several months before the Department can conduct an inspection of the site. Once the inspection is completed, the 45 day countdown starts again, and if there are no further requests for



inspections or information, the Secretary will have 45 days to make a decision whether to approve or refuse the approval of the applicant.

#### *4.41P Duration of approval*

The duration of approval is governed under regulation 4.41P. Subregulation 4.41P(1) provides that the known consignor's approval commences on the day specified in the notice of approval under subregulation 4.41N(3). The day specified in the notice must also take into account whether the applicant is originating cargo or not. A known consignor's approval does not begin until it is carrying on a business that originates cargo. Under subregulation (3), the approval continues until the end of the period specified in the notice or when the approval is revoked. The period specified in the notice must be at least 12 months, but not more than 5 years, after the day on which the approval commences. Flexibility is required to allow the Secretary to take into account a variety of aviation security relevant factors in setting out the approval period. For example, if a business is deemed as higher risk, it may be subject to a shorter approval duration, which provides the Secretary with a degree of increased oversight of that business.

#### *4.41Q Action by Secretary in relation to approval*

Regulation 4.41Q provides for the Secretary to issue a written notice if there is a change to a known consignor's operations resulting in the known consignor no longer carrying on a business in accordance with the requirements of its known consignor security program. The notice may propose one or more of the following actions:

- that the known consignor agree to restrict its activities to those that are in accordance with the known consignor security program provided to it by the Secretary. For example, this may be used to restrict a known consignor from conducting any actions or operations that conflict with the measures and procedures in the known consignor security program;
- that the known consignor agree to the Secretary imposing a condition on the known consignor's approval as a known consignor relating to activities that are not in accordance with the known consignor's security program. For example, this may be used by the Secretary to place conditions on the activities of a known consignor that are not in accordance with the security program. This notice may be proposed where it is more practicable to have conditions imposed on a known consignor, rather than to place restrictions on the known consignor;
- that the known consignor agree to comply with a different known consignor security program. The situations that may warrant this include a known consignor agreeing to comply with a known consignor security program for a particular industry, which may be a model program, such as a security program for beef exporters. This option will provide additional administrative flexibility by allowing the Secretary to issue a written notice to have a known consignor comply with a different known consignor security program, without having to vary the program for the known consignor or direct to vary the program; and/or

- that the known consignor's approval as a known consignor be revoked. The known consignor must accept the action before it is taken to have requested a revocation under subregulation 4.41V(1). That is, this proposal does not revoke the known consignor's status without agreement.

#### *4.41R Application for re-approval*

This regulation sets out the process for a known consignor to apply for re-approval as a known consignor. The application cannot be made until it is within the last 12 months of a known consignor's approval period. Like the approval process, the re-approval application must be in the form approved by the Secretary and include the information required by the form. The Secretary may request in writing additional information in relation to the application or request access for inspection of one or more of the known consignor's sites to gather further information in relation to the re-approval application.

#### *4.41S Decision for re-approval application*

Under regulation 4.41S, the process for re-approval is the same process for the approval of known consignors.

#### *4.41T Approval continues until decision on re-approval application*

Regulation 4.41T deals with the approval duration of a known consignor during its re-approval application process. A known consignor's approval is effectively renewed if the Secretary re-approves the known consignor as a known consignor under subregulation 4.41S(3).

A known consignor's approval is also taken to continue during the re-approval application process until a decision has been made by the Secretary to refuse the application.

#### *4.41U Duration of re-approval*

Similar to the approval duration, the known consignor's re-approval commences on the day specified in the notice of re-approval under subregulation 4.41S(3) and continues in force until the end date specified in that notice or until the re-approval is revoked. Similarly, the duration of the re-approval period is between 12 months to 5 years.

#### *4.41V Revocation of known consignor approval*

If the known consignor has requested a revocation in writing under regulation 4.41V, the Secretary must revoke the approval of the known consignor.

#### *4.41W Revocation of known consignor approval to safeguard against unlawful interference with aviation*

The Secretary may revoke a known consignor's approval if the Secretary is satisfied that doing so is in the interest of safeguarding against unlawful interference with aviation. To ensure that Australia and Australian interests are protected, this revocation power is exercised based on intelligence and/or an assessment of risk. For example, the Secretary may revoke a known consignor if intelligence or an inspection visit noted potential threats to aviation security which will pose a threat to the integrity of the secure air cargo supply chain. This revocation must also be accompanied by reasons for the revocation.

#### *4.41X Revocation of known consignor approval on other grounds*

Regulation 4.41X sets out the other grounds on which the Secretary may revoke the approval of a known consignor. These grounds include a variety of situations where the known consignor may have gone out of business, may have provided false or misleading information, may have not complied with a known consignor security program or has not accepted an action in a notice under regulation 4.41Q. Before the Secretary decides to revoke a known consignor's approval, the known consignor is provided with a written notice of the proposed revocation and its reasons. This provides the opportunity for the known consignor to make a submission as to why the approval should not be revoked. The known consignor must make the submission within the response period, which is a minimum of 14 days commencing on the day the notice is given. The Secretary must consider the submission and notify the known consignor in writing of the decision and the reasons for decision. If the Secretary does not provide a notice of decision within 28 days after the response period, then the Secretary is taken to have decided to revoke the known consignor's approval.

Under regulation 8.03A, the known consignor may appeal to the Administrative Appeals Tribunal for a review of the decision by the Secretary on this matter.

#### *4.41Y Secretary's list of known consignors*

This regulation requires that the Secretary must keep a list of persons approved as known consignors. The Secretary may also publish the list.

#### *Subdivision 4.1A.1C—known consignor security programs*

#### *4.41Z Secretary must provide known consignor with security program*

The known consignor security program must set out the following requirements under subregulation 4.41Z(2). The requirements are consistent with international arrangements and are organised into six pillars. These are:

1. measures and procedures to ensure security of the known consignor's facilities. This may be tailored for individual businesses that have different ways of keeping their facility secure. For example, the security program may be based on relevant facility security measures in place at the business, such as access controls, fencing or locks;

2. measures and procedures to ensure security of the known consignor's personnel. This is aimed at preventing instances of a trusted insider using their access rights to place an unauthorised explosive into cargo. For example, the security program may contain details of background checks as well as how the business aims to mitigate the trusted insider threat, such as having multiple people working together to reduce the instances of a lone individual gaining access to cargo;
3. training requirements and procedures for the known consignor's personnel. For example, training requirements may specify a particular training course that the known consignor's personnel must take, such as security awareness training or set out procedures on how personnel may be trained to handle cargo;
4. measures and procedures for clearing cargo. This covers the ways cargo can be handled and cleared in accordance with the regulations. For example, the clearing cargo component in a known consignor's security program may detail the processes of how goods are processed, manufactured, packed, stored and loaded onto transport and what security measures are applied at each stage.
5. measures and procedures to ensure the chain of custody for cargo. Chain of custody covers the security of cargo as it leaves a known consignor's premises. These measures may require the known consignor to check the identity of the road transporter and ascertain the regulatory status of the road transporter; and
6. measures and procedures for oversight of the measures, procedures and requirements for paragraphs 4.41Z(2)(a) to (e), including quality assurance and incident response. Once approved, known consignors are required to implement quality assurance measures and procedures to ensure that all security measures and procedures implemented remain effective and relevant during their approval period. Examples of quality assurance measures and procedures will include internal and external audits and reviews.

Subregulation 4.41Z(3) and subregulation 4.41Z(4) provide that the Secretary may provide a person who is re-approved as a known consignor under regulation 4.41S with a known consignor security program. However, if there is already a security program in force for the known consignor, then the original security program remains in force. This is to remove the need to reissue security programs upon re-approval, which reduces administrative burden for industry.

#### *4.41ZA When a known consignor security program is in force*

A known consignor's security program comes into force as specified in the security program. Subregulation 4.41ZA(3) provides that the security program for the known consignor remains in force for so long as the known consignor is approved as a known consignor.

#### *4.41ZB Secretary may vary known consignor security program*

There are two grounds for the Secretary to vary the known consignor's security program. The first is when the Secretary is no longer satisfied that the security program adequately

addresses the requirements in subregulation 4.41Z(2), and the second where the Secretary is satisfied on reasonable grounds that varying the security program is in the interest of safeguarding against unlawful interference with aviation. For example, the second may be exercised where the current security program no longer addresses the current security environment and needs to be updated, or where varying the program will enhance security outcomes or reduce administrative burden for industry. By reducing administrative burden, industry can better allocate resources to prevent unlawful interference with aviation.

Under subregulation 4.41ZB(3), the known consignor has the option to request an amendment to the varied program or ask for a revocation of its approval. As a requirement of this request, under subregulation 4.41ZB(6), the known consignor must provide the Secretary with written details of its proposed amendment and written reasons why the proposed amendment is being requested. For example, if the known consignor receives a varied program and notes that it does not accurately reflect its operations, it may ask the Secretary for an amendment to that varied security program to better reflect its operations.

#### *4.41ZC Consideration of request to amend known consignor security program as varied by the Secretary*

This regulation provides for the Secretary to consider a known consignor's request to amend a varied security program. The Secretary must take into account the following matters: whether the known consignor security program, as proposed to be varied, addresses the requirements set out in subregulation 4.41Z(2); existing circumstances as they relate to safeguarding against unlawful interference with aviation; the current use of the known consignor security program by a business of the kind carried on by the known consignor (for example, if the known consignor is in a particular type of industry such as meat processing, the program should be tailored towards this industry); the efficient administration of the known consignor scheme; and any other matter the Secretary considers relevant. In relation to other relevant matters, these may include safeguarding against unlawful interference with aviation, accuracy of information in the proposed amendment to the varied security program or whether the proposed amendment allows effective compliance and audit processes to be conducted.

#### *4.41ZD Secretary may direct known consignors to vary security programs*

This regulation is distinguished from regulation 4.41ZB by the Secretary directing the known consignor to vary the program, as opposed to providing a varied program under regulation 4.41ZB. For example, this may be an email from the Secretary to the known consignor directing the known consignor to change parts of the security program. Under this regulation, the known consignor needs to provide the Secretary with the varied security program in accordance with the direction. If the known consignor does not vary the program in accordance with the notice of direction, then that is a ground for revocation of the known consignor's approval.

#### *4.41ZE Known consignor may request Secretary to vary known consignor security program*

Under this regulation, the known consignor may request the Secretary to vary the known consignor security program.

#### *4.41ZF Consideration of request to vary known consignor security program*

This regulation provides for the Secretary to consider a request made by the known consignor to vary its security program. The Secretary must take into account the following matters in making this decision: whether the known consignor security program, as proposed to be varied, addresses the requirements set out in subregulation 4.41Z(2); existing circumstances as they relate to safeguarding against unlawful interference with aviation; the current use of the known consignor security program by a business of the kind carried on by the known consignor (for example, if the known consignor is in a particular type of industry such as meat processing, the security program should be tailored towards this industry); the efficient administration of the known consignor scheme; and any other matter the Secretary considers relevant. In relation to other relevant matters, these may include safeguarding against unlawful interference with aviation, accuracy of information in the proposed varied program or whether the variation allows effective compliance and audit processes to be conducted.

This decision by the Secretary is also subject to further oversight and review under regulation 8.03A.

#### *4.41ZG Offence—failure to comply with known consignor security program*

This offence penalises known consignors that do not comply with the security program that is in force for the known consignor. Non-compliance examples include known consignors not clearing cargo as outlined under the measures and procedures for clearing cargo or leaving facility security in a state of disrepair or ineffectiveness. The imposition of the strict liability offence here is consistent with the principles in *A Guide to Framing Commonwealth Offences*.

This is a specific offence which has strict criteria. Requiring proof of fault in this instance would undermine deterrence. It would be particularly difficult to prove fault in these circumstances as extensive documentation regarding an intent to breach the security program would be required to establish the fault elements of the known consignor. Known consignors are also placed on notice to guard against the possibility of any contravention under their security program. If fault was required for this offence, significant resources would be needed for enforcement and this would significantly impact on the resources available to ensure the security of the air cargo supply chain.

Furthermore, security programs are documents that are technical in nature, referring to specific industry practices (such as a meatworks or a pharmaceutical operation) and change regularly. It is appropriate to sub-delegate the offence to the program as the Secretary needs to ensure industry can comply with the programs that accurately reflect their operations. For example, it would be impractical to prescribe in the amending Regulation individual offences that apply to different export industries in Australia. That is, a fish exporter is unlikely to

have the same security measures as a radio exporter. Lastly, businesses have the option (through the amendment provisions in the amending Regulation) to agree or disagree with the content of the programs to which they are bound to comply with.

#### *4.41ZH Offence—disclosing known consignor security program information without consent*

This offense penalises a person if the person discloses information about the content of a known consignor security program and the person does not have the consent of the known consignor to disclose such information. The penalty unit of 50 units is consistent with previous regulation 4.46, which is a similar offence for disclosing information not in accordance with a security program.

#### **Item [14] – Regulation 4.42 to 4.44**

This item repeals the previous regulation for the definition of a RACA and replaces it with a new definition. Under regulation 4.42, a person is a RACA if the person carries on a business that includes the handling or making arrangements for transport of cargo and the examination of cargo, in accordance with a notice given to the person made under regulation 4.41J or regulation 4.41JA. This is a change from the previous RACA framework where a person as a RACA was not required to demonstrate that they have examined cargo in accordance with a notice issued under the Principle Regulations.

This item also repeals the previous application framework for RACAs and replaces it with a new RACA application framework.

#### *4.43 Applying for designation as a RACA*

This new regulation provides a framework for designating RACAs. Under subregulation 4.43(1), if a person already carries out a business that includes handling or making arrangements for the transport of cargo, and the examination of cargo in accordance with a regulation 4.41J or regulation 4.41JA notice, then it may also apply to become a RACA. An applicant may also apply to the Secretary to be designated as a RACA if it intends to carry out a business that includes the handling or making arrangements for transport of cargo, and the examination of cargo in accordance with a regulation 4.41J or regulation 4.41JA notice. This enables businesses that have invested resources into examining cargo, but which have not yet started to examine cargo, to apply. Subregulation 4.43(2) requires that the application be made on the application form designated by the Secretary and include the information required by the form.

After the form is lodged, the Secretary may request the applicant to provide further information in relation to the application or access for inspection one or more of the applicant's sites to gather further information. Subregulation 4.43(3) enables the Department to inspect the applicant's site in order to validate information on the application form or gather any other information that is necessary in relation to the application. Requests made under subregulation 4.43(3) must be in writing and specify the period of which the further information or access is to be provided.

Subregulation 4.43(5) provides that an inspection may be conducted by an APS employee, a person who is engaged as a consultant or contractor to perform services for the Department or a law enforcement officer. The category of persons able to conduct an inspection is set to be broad to capture a variety of different government inspectors. This is appropriate under the circumstances due to:

- the need to meet the potential demand of RACA applications to ensure that Australia's exports to the United States are not disrupted;
- the non-intrusive nature of the inspections will limit the power of APS employees. That is, the persons conducting the inspections will not have any powers to enter premises or take information without agreement from the business;
- limiting the classification of APS employees would not be appropriate as the inspection may be conducted by staff from different classifications;
- limiting the category of APS employees may prevent APS employees from certain agencies from conducting an inspection, where that agency has expertise in inspecting a particular industry; and
- the dispersed nature of the freight forwarding industry in Australia will potentially require inspectors to be sourced from regional offices where the broad pool of Commonwealth employees is required to efficiently conduct inspections.

Furthermore, contractors or consultants engaged by the Department may also be able to conduct an inspection on behalf of the Secretary. This will provide the Department with flexible options to meet the demand for inspections and reduce the risk of delay in designating RACAs.

While the inspection is upon request by the Secretary, under subregulation 4.43(6), if an applicant does not provide access, the Secretary may refuse to consider the application any further. This refusal also applies to circumstances where the applicant does not provide further information as requested by the Secretary.

The decision on application is governed by Regulation 4.43A. In making a decision, the Secretary may take into account anything submitted in the application and any further information obtained as a result of a request for further information or information obtained during an inspection. As cargo is examined by a RACA to receive clearance for uplift onto aircraft, the standard of security expected is high. Subregulation 4.43A(2) also provides for the Secretary to consider any other information relevant to make a decision on the application. For example, this framework allows the Secretary to consider the holistic security situation for an application. The Secretary may refuse to approve an application even if the application was filled out correctly. It may be that the inspection resulted in new information that highlighted new risks that were not evident in the application form.

Under subregulation 4.43A(3), the Secretary's decision on the application must be made in writing. This decision must be made within 90 days of the application being made. However, the 90 day rule is subject to "stopping the clock", which is covered under subregulation 4.43A(6).



If the Secretary does not make a decision under subregulation 4.43A(1) within 90 days of the application being made, the Secretary is taken to have refused to designate the applicant as a RACA at the end of that period. Subregulation 4.41N(4) must also take into account the stop clock mechanism in the next paragraphs.

The stop clock under subregulation 4.43A(6) operates in two circumstances: where the Secretary has requested further information under paragraph 4.43(3)(a), or requested access for inspection under paragraph 4.43(3)(b). Once the Secretary has made a request in these circumstances, the stop clock is activated for each request that is made. The stop clock halts the 90 days decision period until further information under paragraph 4.43(3)(a) is given or an inspection under paragraph 4.43(3)(b) is conducted. The end period may also be given a date within the written notice under paragraph 4.43(3)(a) or 4.43(3)(b). The stop clock mechanism provides time, where necessary, for the Secretary to review further information or to conduct inspections.

For example, the stop clock mechanism is worked through below for a freight forwarder. At the beginning, the freight forwarder applies to become a RACA. The Secretary may ask the RACA applicant about additional security measures relating to personnel security at the freight forwarder facility. Once this request is provided to the RACA in writing, the 90 day decision period is immediately halted on the day on which the written notice is given. It may take the freight forwarder exporter two weeks to provide this information, and the two weeks do not count towards the 90 day decision making period. When the applicant provides the requested information, the 90 day decision period begins to countdown again. At the 45 day mark, the stop clock may be triggered again by the Secretary requesting an inspection to the applicant's site. Due to examination equipment not arriving for a few months, an inspection may not be possible until a few months after the request for inspection. This means that the stop clock can last for several months before the Department can conduct an inspection of the site. Once the inspection is completed, the 45 day countdown starts again, and if there are no further requests for inspections or information, the Secretary will have 45 days to make a decision whether to approve or refuse the designation of the applicant.

#### *4.43B Duration of designation*

This regulation changes the previous designation duration for RACAs. Previously, a RACA's designation would not lapse, while its TSP had a five year expiry date. Under the new framework, a RACA's designation is of a finite duration while the RACA security program continues in force until the RACA designation is revoked.

The duration of designation is governed under regulation 4.43B. Subregulation 4.43B(1) provides that the RACA's designation commences on the day specified in the notice of designation under subregulation 4.43A(3). The day specified in the notice must also take into account whether the applicant is examining cargo or not. A RACA's designation does not begin until it is carrying on a business that originates cargo. Under subregulation 4.43B(3), the designation continues until the end of the period specified in the notice or when the designation is revoked under regulation 4.44. The period specified in the notice must be at

least 12 months, but not more than 5 years, after the day on which the designation commences. Flexibility is required to allow the Secretary to take into account a variety of aviation security relevant factors in setting out the designation period. For example, if a business is deemed as higher risk, it may be subject to a shorter designation duration, which provides the Secretary with a degree of increased oversight of that business.

#### *4.43C Action by Secretary in relation to designation*

Regulation 4.43C provides for the Secretary to issue a written notice if there is a change to a RACA's operations resulting in the RACA no longer carrying on a business in accordance with the requirements of its RACA security program. The notice may propose one or more of the following actions:

- that the RACA agree to restrict its activities to those that are in accordance with the RACA security program provided to it by the Secretary. For example, this may be used to restrict a RACA from conducting any actions or operations that conflict with the measures and procedures in the known consignor security program;
- that the RACA agree to the Secretary imposing a condition on the RACA's designation relating to activities that are not in accordance with the RACA's security program. This notice may be proposed where it is more practicable to have conditions imposed on a RACA, rather than to place restrictions on the RACA;
- that the RACA agree to comply with a different RACA security program. The situations that may warrant this include a RACA agreeing to comply with a RACA security program for a particular industry, which may be a model program, such as a security program for certain types of freight forwarders. This option provides additional administrative flexibility by allowing the Secretary to issue a written notice to have a RACA comply with a different RACA security program, without having to vary the program for the RACA or direct to vary the program; and/or
- that the RACA's designation as a RACA be revoked. The RACA must accept the action before it is taken to have requested a revocation under subregulation 4.44. That is, this proposal does not revoke the RACA's status without agreement.

#### *4.43D Application for designation to be renewed*

This regulation sets out the process for a RACA to apply for renewal of its designation as a RACA. The application cannot be made until it is within the last 12 months of a RACA's designation period. Like the designation process, the renewal of designation application must be in the form approved by the Secretary and include the information required by the form. The Secretary may request in writing additional information in relation to the application or request access for inspection of one or more of the RACA's sites to gather further information in relation to the renewal of the designation application.

#### *4.43E Decision for renewal of designation application*

Under regulation 4.43E, the process for the renewal of a RACA designation is the same process for the designation of the RACA.

#### *4.43F Designation continues until decision on renewal application*

Regulation 4.43F deals with the designation duration of a RACA during its renewal application process.

A RACA's designation is taken to continue during the renewal application process until a decision has been made by the Secretary to renew or refuse to renew the application.

#### *4.43G Duration of re-designation*

Similar to the designation duration, the RACA's renewed designation commences on the day specified in the notice of renewed designation under subregulation 4.43E(3) and continues in force until the end date specified in that notice or until the re-designation is revoked under regulation 4.44. Similarly, the duration of the re-designation period is between 12 months to 5 years.

#### *4.44 Revocation of RACA designation*

If the RACA has requested a revocation in writing under regulation 4.44, the Secretary must revoke the designation of the RACA.

##### *4.44A Revocation of RACA designation to safeguard against unlawful interference with aviation*

The Secretary may revoke a RACA's designation if the Secretary is satisfied that doing so will be in the interest of safeguarding against unlawful interference with aviation. To ensure that Australia and Australian interests are protected, this revocation power is exercised based on intelligence and/or an assessment of risk. For example, the Secretary may revoke a RACA's designation if intelligence or an inspection visit noted potential threats to aviation security which will pose a threat to the integrity of the secure air cargo supply chain. This revocation must also be accompanied by reasons for the revocation.

##### *4.44B Revocation of RACA designation on other grounds*

Regulation 4.44B will set out the other grounds on which the Secretary may revoke the designation of a RACA. These grounds include a variety of situations where the RACA may have gone out of business, may have provided false or misleading information, may have not complied with a RACA security program or has not accepted an action in a notice under regulation 4.43C. Before the Secretary decides to revoke a RACA's designation, the RACA is provided with a written notice of the proposed revocation and its reasons. This provides the opportunity for the RACA to make a submission as to why the designation should not be revoked. The RACA must make the submission within the response period, which is a minimum of 14 days commencing on the day the notice is given. The Secretary must consider the submission and notify the RACA in writing of the decision and the reasons for decision. If the Secretary does not provide a notice within the 28 days after the response period for the decision, then the Secretary is taken to have decided to revoke the RACA's designation.

The RACA may appeal to the Administrative Appeals Tribunal for a review of the decision by the Secretary on this matter.

#### *4.44C automatic revocation if RACA accredited as AACA*

This regulation provides for automatic revocation of a person as a RACA if the person is accredited as an AACA.

#### **Item [15] – Regulations 4.45A and 4.46**

These regulations are repealed. There is no longer a requirement for a RACA to notify the Secretary of changes to information contained in its application. However, this does not preclude any requirements the RACA security program may have around information notification under the measures and procedures for quality assurance and incident response.

Regulation 4.46 is repealed as the disclosure of information offences are now attached to known consignors under regulation 4.41ZH, RACAs under regulation 4.46H and AACAs under regulation 4.51H. However, the offence mechanism for aviation industry participants other than a RACA, AACA or known consignor disclosing information not in accordance with a security program continues to apply under regulation 4.51J.

#### **Item [16] – After Subdivision 4.1A.2**

##### *Subdivision 4.1A.2A—RACA security programs*

#### *4.46 Secretary must provide RACA with security program*

The RACA security program must set out the following requirements under subregulation 4.46(2). The requirements are consistent with international arrangements and are organised into pillars below. These are:

1. measures and procedures to ensure security of the RACA's facilities. This may be tailored for individual businesses that have different ways of keeping their facility secure. For example, the security program may be based on relevant facility security measures in place at the business, such as access controls, fencing or locks;
2. measures and procedures to ensure security of the RACA's personnel. This is aimed to prevent instances of a trusted insider using their access rights to place an unauthorised explosive in cargo. For example, the security program may contain details of background checks as well as how the business aims to mitigate the trusted insider threat, such as having multiple people working together to reduce the instances of a lone individual gaining access to cargo;
3. training requirements and procedures for the RACA's personnel. Under this pillar, the security program must set out the training requirements and procedures for the RACA's personnel. For example, training requirements may specify a particular training course that the RACA's personnel must take, such as security awareness or set out procedures on how personnel may be trained to handle cargo;

4. measures and procedures for clearing cargo. As a RACA, the security program provides a means in which cargo can be handled and cleared in accordance with the regulations. For example, the clearing cargo component in a RACA's security program details the processes of how cargo is to be handled and kept secure after examination;
5. measures and procedures to ensure the chain of custody for cargo. Chain of custody covers the security of cargo as it leaves a RACA's premises. Usually, cargo is transported out of a RACA facility by a ground transporter. The measures and procedures here may relate to how the RACA checks the identity of a ground transporter to ensure the chain of custody is intact;
6. measures and procedures to be used for handling high risk cargo. For example, this may include how high risk cargo is identified and what the necessary steps are required to deal with high risk cargo to enable its clearance; and
7. measures and procedures for oversight of the measures, procedures and requirements for paragraphs (a) to (f), including quality assurance and incident response. Once accredited, RACAs are required to implement quality assurance activities to ensure that all security measures and procedures implemented remain effective and relevant during their accreditation period. Examples of quality assurance activities include internal and external audits and reviews.

Subregulation 4.46(3) and subregulation 4.46(4) provide that the Secretary may provide a person who has renewed the RACA designation with a RACA security program. However, if there is already a security program in force for the RACA, then the original security program remains in force. This is to remove the need to re-issue security programs upon the renewal of designation, which reduces administrative burden for industry.

#### *4.46A When a RACA security program is in force*

A RACA's security program is in force when it comes into force as specified in the program. Subregulation 4.46A(3) provides that the security program for the RACA remains in force for so long as the RACA is designated as a RACA.

#### *4.46B Secretary may vary RACA security program*

There are two grounds for the Secretary to vary the RACA's security program. The first is when the Secretary is no longer satisfied that the program adequately addresses the requirements in subregulation 4.46(2), and the second is when the Secretary is satisfied on reasonable grounds that varying the program is in the interest of safeguarding against unlawful interference with aviation. For example, the second may also be exercised where the current security program no longer addresses the current security environment and needs to be updated, or where updating it will enhance security outcomes or reduce administrative burden for industry. By reducing administrative burden, industry can better allocate resources to prevent unlawful interference with aviation.

Under subregulation 4.46B(3), the RACA has an opportunity to request an amendment to the varied program or ask for a revocation of its designation. As a requirement of this request under subregulation 4.46B(6), the RACA must provide the Secretary with written details of its proposed amendment and written reasons why the proposed amendment is being requested. For example, if the RACA receives a varied program and notes that it does not accurately reflect its operations, it may ask the Secretary for an amendment to that varied program to better reflect its operations.

#### *4.46C Consideration of request to amend RACA security program as varied by the Secretary*

This regulation provides for the Secretary to consider a RACA's request to amend a varied security program. The Secretary must take into account the following matters in making this decision to accept the amendment to the variation: whether the RACA security program, as proposed to be varied, addresses the requirements set out in subregulation 4.46(2); existing circumstances as they relate to safeguarding against unlawful interference with aviation; the current use of the RACA security program by a business of the kind carried on by the RACA; the efficient administration of the RACA scheme; and any other matter the Secretary considers relevant. In relation to other relevant matters, these may include safeguarding against unlawful interference with aviation, accuracy of information in the proposed amendment to the varied program or whether the proposed amendment allows effective compliance and audit processes to be conducted.

#### *4.46D Secretary may direct RACAs to vary security programs*

This regulation is distinguished from regulation 4.46C by the Secretary directing the RACA to vary the program as opposed to providing a varied program under 4.46C. For example, this may be an email from the Secretary to the RACA to direct the RACA to change parts of the program. Under this regulation, the RACA needs to provide the Secretary with the varied program in accordance with the direction. If the RACA does not vary the program in accordance with the notice of direction, then that is a ground for revocation of the RACA's designation.

#### *4.46E RACA may request Secretary to vary RACA security program*

Under this regulation, the RACA may request the Secretary to vary the RACA security program. This provides an opportunity for a RACA to request a variation of its program.

#### *4.46F Consideration of request to vary RACA security program*

This regulation provides for the Secretary to consider a request made by a RACA to vary its security program. The Secretary must take into account the following matters in making this decision: whether the RACA security program, as proposed to be varied, addresses the requirements set out in subregulation 4.46(2); existing circumstances as they relate to safeguarding against unlawful interference with aviation; the current use of the RACA security program by a business of the kind carried on by the RACA (for example, if the RACA is in a particular type of business such as the off-airport examination of cargo, the program should be tailored towards this industry); the efficient administration of the RACA

scheme; and any other matter the Secretary considers relevant. In relation to other relevant matters, these may include safeguarding against unlawful interference with aviation, accuracy of information in the proposed varied program or whether the variation allows effective compliance and audit processes to be conducted.

This decision by the Secretary is also subject to further oversight and review under regulation 8.04.

#### *4.46G Offence—failure to comply with RACA security program*

This offence penalises RACAs that do not comply with the security program that is in force for the RACA. Non-compliance examples include RACAs not clearing cargo as outlined under the measures and procedures for clearing cargo or leaving facility security in a state of disrepair or ineffectiveness. The imposition of the strict liability offence here is consistent with the principles in *A Guide to Framing Commonwealth Offences*.

This is a specific offence which has strict criteria. Requiring proof of fault in this instance would undermine deterrence. It would be particularly difficult to prove fault in these circumstances as extensive documentation regarding intent to breach the security program will be required to establish the fault elements of the RACA. RACAs are also placed on notice to guard against the possibility of any contravention. If fault was required for this offence, significant resources would be needed for enforcement and this would significantly impact on the resources available to ensure the security of the air cargo supply chain.

Furthermore, security programs are documents that are technical in nature, referring to specific industry practices and change regularly. It is appropriate to sub-delegate the offence to the program as the Secretary needs to ensure industry can comply with the programs that accurately reflect their operations. For example, it would be impractical to prescribe in the amending Regulation individual offences that apply to different RACAs in Australia. That is, a cargo terminal operator may have different security measures in place than an off-airport freight forwarder. Lastly, businesses have the option (through the amendment provisions in the amendment Regulation) to agree or disagree with the content of the programs to which they are bound.

#### *4.46H Offence—disclosing RACA security program information without consent*

This offense penalises a person if the person discloses information about the content of a RACA security program and the person does not have the consent of the RACA to disclose such information. The penalty unit of 50 units is consistent with previous regulation 4.46, which is a similar offence for disclosing information not in accordance with a security program.

### **Item [17] – Regulations 4.48 to 4.51D**

This item repeals the current regulations on applying for accreditation as an AACA and replaces it with a new application framework for AACA accreditation.

#### *4.48 Applying for accreditation as an AACA*

This new regulation provides a framework for the process of accrediting AACAs. If a person already carries out a business that includes the handling or making arrangements for transport of cargo, then it may also apply to become an AACA. An applicant may also apply to the Secretary to be accredited as an AACA if it intends to carry out a business that includes handling or making arrangements for the transport of cargo. This enables businesses that have invested resources into handling or making arrangements for the transport of cargo, but which have not yet started to conduct these activities, to apply. Subregulation 4.48(2) requires that the application be made on the application form accredited by the Secretary and include the information required by the form.

After the form is lodged, the Secretary may request the applicant to provide further information in relation to the application or access for inspection one or more of the applicant's sites to gather further information. Subregulation 4.48(3) enables the Department to inspect the applicant's site in order to validate information on the application form or gather any other information that is necessary in relation to the application. Requests made under Subregulation 4.48(3) must be in writing and specify the period of which the further information or access is to be provided.

Subregulation 4.48(4) provide that an inspection may be conducted by an APS employee, a person who is engaged as a consultant or contractor to perform services for the Department or a law enforcement officer. The category of persons able to conduct an inspection is set to be broad to capture a variety of different government inspectors. This is appropriate under the circumstances due to:

- the need to meet the potential demand of AACA applications to ensure that Australia's exports to the United States are not disrupted;
- the non-intrusive nature of the inspections limits the power of APS employees. That is, the persons conducting the inspections do not have any powers to enter premises or take information without agreement from the business;
- limiting the classification of APS employees will not be appropriate as the inspection may be conducted by staff from different classifications;
- limiting the category of APS employees may prevent APS employees from certain agencies from conducting an inspection, where that agency has expertise in inspecting a particular industry; and
- the dispersed nature of the freight forwarding and transport industry in Australia potentially requires inspectors to be sourced from regional offices where the broad pool of Commonwealth employees is required to efficiently conduct inspections.

Furthermore, contractors or consultants engaged by the Department may also be able to conduct an inspection on behalf of the Secretary. This will provide the Department with flexible options to meet the demand for inspections and reduce the risk of delay in accrediting AACAs.



While the inspection is upon request by the Secretary, under subregulation 4.48(6), if an applicant does not provide access, the Secretary may refuse to consider the application any further. This refusal also applies to circumstances where the applicant does not provide further information as requested by the Secretary.

#### *4.49 Decision on application*

The decision on application is governed by regulation 4.49. In making a decision, the Secretary may take into account anything submitted in the application and any further information obtained as a result of a request for further information or information obtained during an inspection. As cargo is handled by an AACA to maintain its cleared status for uplift onto aircraft, the standard of security expected is high. Subregulation 4.49(2) also provides for the Secretary to consider any other information relevant to make a decision on the application. For example, this framework allows the Secretary to consider the holistic security situation for an application. The Secretary may refuse to approve an application even if the application was filled out correctly, it may be that the inspection resulted in new information that highlighted new risks that were not evident in the application form.

Under subregulation 4.49(3), the Secretary's decision on the application must be made in writing. This decision must be made within 90 days of the application being made. However, the 90 day rule is subject to "stopping the clock", which is covered under subregulation 4.49(6).

If the Secretary does not make a decision under subregulation 4.49(1) within 90 days of the application being made, the Secretary is taken to have refused to accredit the applicant as an AACA at the end of that period. Subregulation 4.49(3) must also take into account the stop clock mechanism in the next paragraphs.

The stop clock under subregulation 4.49(6) operates in two circumstances: where the Secretary has requested further information under paragraph 4.48(3)(a), or requested access for inspection under paragraph 4.48(3)(b). Once the Secretary has made a request in these circumstances, the stop clock is activated for each request that is made. The stop clock halts the 90 days decision period until further information under paragraph 4.48(3)(a) is given or an inspection under paragraph 4.48(3)(b) is conducted. The end period may also be given a date within the written notice under paragraph 4.48(3)(a) or 4.48(3)(b). The stop clock mechanism provides time, where necessary, for the Secretary to review further information or conduct inspections.

For example, the stop clock mechanism is worked through below for a person applying to be an AACA. At the beginning, the person applies to become an AACA. The Secretary may ask the AACA applicant about additional security measures relating to personnel security. Once this request is provided in writing, the 90 day decision period is immediately halted on the day on which the written notice is given. It may take the person two weeks to provide this information, and the two weeks do not count towards the 90 day decision making period. As the applicant provides the requested information, the 90 day decision period begins to countdown again. At the 45 day mark, the stop clock may be triggered again by the Secretary

requesting an inspection to the applicant's site. Once the inspection is completed, the 45 day countdown starts again, and if there are no further requests for inspections or information, the Secretary will have 45 days to make a decision whether to approve or refuse the accreditation of the applicant.

#### *4.50 Duration of accreditation*

The duration of accreditation is governed under regulation 4.50. Subregulation 4.50(1) provides that the AACA's accreditation commences on the day specified in the notice of accreditation under subregulation 4.49(3). The day specified in the notice must also take into account whether the applicant is handling cargo or not. An AACA's accreditation does not begin until it is carrying on a business that handles or makes arrangements for the transport, of cargo. Under subregulation 4.50(3), the accreditation continues until the end of the period specified in the notice or when the accreditation is revoked under regulation 4.51D. The period specified in the notice must be at least 12 months, but not more than 5 years, after the day on which the accreditation commences. Flexibility is required to allow the Secretary to take into account a variety of aviation security relevant factors in setting out the accreditation period. For example, if a business is deemed as higher risk, it may be subject to a shorter accreditation duration, which provides the Secretary with a degree of increased oversight of that business.

#### *4.51 Action by Secretary in relation to accreditation*

Regulation 4.51 provides for the Secretary to issue a written notice if there is a change to an AACA's operations resulting in the AACA no longer carrying on a business in accordance with the requirements of its AACA security program. The notice may propose one or more of the following actions:

- that the AACA agree to restrict its activities to those that are in accordance with the AACA security program provided to it by the Secretary. For example, this may be used to restrict an AACA from conducting any actions or operations that conflict with the measures and procedures in the known consignor security program;
- that the AACA agree to the Secretary imposing a condition on the AACA's designation relating to activities that are not in accordance with the AACA's security program. This notice may be proposed where it is more practicable to have conditions imposed on a AACA, rather than to place restrictions on the AACA;
- that the AACA agree to comply with a different AACA security program. The situations that may warrant this include an AACA agreeing to comply with an AACA security program for a particular industry, which may be a model program, such as a security program for certain types of transport companies. This option provides additional administrative flexibility by allowing the Secretary to issue a written notice to have an AACA comply with a different AACA security program, without having to vary the program for the AACA or direct to vary the program; and/or

- that the AACA's accreditation as an AACA be revoked. The AACA needs to accept the action before it is taken to have requested a revocation under regulation 4.51D. That is, this does not revoke the AACA's accreditation without agreement.

#### *4.51A Application for accreditation to be renewed*

This regulation sets out the process for an AACA to apply for renewal of its accreditation as an AACA. The application cannot be made until it is within the last 12 months of an AACA's accreditation period. Like the accreditation process, the renewal of accreditation application must be in the form approved by the Secretary and include the information required by the form. The Secretary may request in writing additional information in relation to the application or request access for inspection of one or more of the AACA's sites to gather further information in relation to the renewal of the accreditation application.

#### *4.51B Decision for renewal of accreditation application*

Under regulation 4.51B, the renewal process for an AACA accreditation is the same as the AACA accreditation process.

#### *4.51C Accreditation continues until decision on renewal application*

Regulation 4.51C deals with the accreditation duration of an AACA during its renewal application process.

An AACA's accreditation is taken to continue during the renewal application process until a decision has been made by the Secretary to renew or refuse to renew the application.

#### *4.51CA Duration of re-accreditation*

Similar to the accreditation duration, the AACA's renewed accreditation commences on the day specified in the notice of renewed accreditation under subregulation 4.51B(3) and continues in force until the end date specified in that notice or until the re-accreditation is revoked under regulation 4.51D. Similarly, the duration of the re-accreditation period is between 12 months to 5 years.

#### *4.51D Revocation of AACA accreditation*

If an AACA has requested a revocation in writing under subregulation 4.51D(1), the Secretary must revoke the accreditation of that AACA.

#### *4.51DA Revocation of AACA accreditation to safeguard against unlawful interference with aviation*

The Secretary may revoke an AACA's accreditation if the Secretary is satisfied that doing so will be in the interest of safeguarding against unlawful interference with aviation. To ensure that Australia and Australian interests are protected, this revocation power is exercised based on intelligence and/or an assessment of risk. For example, the Secretary may revoke an AACA's accreditation if intelligence or an inspection visit noted potential threats to aviation

security which will pose a threat to the integrity of the secure air cargo supply chain. This revocation must also be accompanied by reasons for the revocation.

#### *4.51DB Revocation of AACA accreditation on other grounds*

Regulation 4.51DB sets out the other grounds on which the Secretary may revoke the accreditation of an AACA. These grounds include a variety of situations where the AACA may have gone out of business, may have provided false or misleading information, may have not complied with an AACA security program or has not accepted an action in a notice under regulation 4.51. Before the Secretary decides to revoke an AACA's accreditation, the AACA is provided with a written notice of the proposed revocation and its reasons. This provides the opportunity for the AACA to make a submission as to why the accreditation should not be revoked. The AACA must make the submission within the response period, which is a minimum of 14 days commencing on the day the notice is given. The Secretary must consider the submission and notify the AACA in writing of the decision and the reasons for decision. If the Secretary does not provide a notice within 28 days after the response period for the decision, then the Secretary is taken to have decided to revoke the AACA's accreditation.

The AACA may appeal to the Administrative Appeals Tribunal for a review of the decision by the Secretary on this matter.

#### *4.51DC Automatic revocation if AACA designated as a RACA*

This regulation provides that the accreditation of an AACA is automatically revoked if the AACA is subsequently designated as a RACA.

#### **Item [18] – Subdivision 4.1A.4**

This subdivision is repealed and replaced with a new subdivision for the AACA security program regulatory framework. The replacement of subdivision 4.1A.4 will create a uniform security framework across supply chain participants including known consignors, RACAs and AACAs.

#### *Subdivision 4.1A.4—AACA security programs*

##### *4.51F Secretary must provide AACA with security program*

The AACA security program may set out the following requirements under subregulation 4.51F(2). As AACAs cover a more diverse freight forwarding industry than RACAs, not all of the pillars below will be applicable for all AACAs. This regulation is designed to incorporate proportionate regulation and provide flexibility for industry. For example, an AACA that is solely a transport company may not have relevant facility security measures in place, and therefore the requirements below need to be flexible and be determined by the Secretary. The AACA security requirements may contain:

1. measures and procedures to ensure security of the AACA's facilities. This pillar requires the security program to set out requirements for facility security, and this

- may be tailored for individual businesses that have different ways of keeping their facility secure. For example, the security program may be based on relevant facility security measures in place at the business, such as access controls, fencing or locks;
2. measures and procedures to ensure security of the AACA's personnel. This is aimed to prevent the instances of a trusted insider using their access rights to place an unauthorised explosive in cargo. For example, the security program may contain details of background checks as well as how the business aims to mitigate the trusted insider threat, such as having multiple people working together to reduce the instances of a lone individual gaining access to cargo;
  3. training requirements and procedures for the AACA's personnel. Under this pillar, the security program must set out the training requirements and procedures for the AACA's personnel. For example, training requirements may specify a particular training course that the AACA's personnel must take, such as security awareness or set out procedures on how personnel may be trained to handle cargo;
  4. measures and procedures for handling cleared cargo. As an AACA, the security program provides a means in which cargo can be kept clear. AACAs do not clear cargo, which is a function of RACAs and known consignors. Therefore, this pillar will deal with measures and procedures in handling cleared cargo. For example, the measures may involve checking cargo for tampering or keeping the cargo in a lockable container as it is transported;
  5. measures and procedures to ensure the chain of custody for cargo. The measures and procedures here may be related to keeping cargo clear and ways to identify cargo that has been tampered with. The measures and procedures here may also relate to how the AACA checks the identity of a ground transporter to ensure the chain of custody is intact;
  6. measures and procedures to be used for handling high risk cargo. For example, this may include how high risk cargo is identified and what the necessary steps are required to deal with high risk cargo to enable its clearance; and/or
  7. measures and procedures for oversight of the measures, procedures and requirements for paragraphs 4.41F(2)(a) to (f), including quality assurance and incident response. Once accredited, AACAs are required to implement quality assurance activities to ensure that all security measures and procedures implemented remain effective and relevant during their accreditation period. Examples of quality assurance activities include internal and external audits and reviews.

Subregulation 4.51F(3) and subregulation 4.51F(4) provides that the Secretary may provide a person who is reaccredited as an AACA under regulation 4.51B with an AACA security program. However, if there is already a security program in force for the AACA, then the original security program remains in force. This removes the need to reissue security programs upon the renewal of accreditation, which reduces administrative burden for industry.

#### *4.51FA When an AACA security program is in force*

An AACA's security program is in force when it comes into force as specified in the program. Subregulation 4.51FA(3) provides that the security program for the AACA remains in force for so long as the AACA is accredited as an AACA.

#### *4.51FB Secretary may vary AACA security program*

As the AACA security program contains discretionary pillars (as opposed to the RACA and known consignor programs which must contain all required pillars), the circumstances for the Secretary to vary the AACA's security program no longer include the Secretary being no longer satisfied that the program adequately addresses the requirements in subregulation 4.51F. Instead, the Secretary may vary the AACA security program if the Secretary is satisfied on reasonable grounds that varying the program is in the interest of safeguarding against unlawful interference with aviation. This may be exercised in the event where the current security program no longer addresses the current security environment and needs to be updated. For example, the Secretary may vary the program to improve the content of the program which will enhance security measures and reduce administrative burden. By reducing administrative burden, industry can better allocate resources to prevent unlawful interference with aviation.

Under subregulation 4.51FB(2), the AACA has an opportunity to request an amendment to the varied program or ask for a revocation of its accreditation. As a requirement of this request under subregulation 4.51FB(5), the AACA must provide the Secretary with written details of its proposed amendment and written reasons why the proposed amendment is being requested. For example, if the AACA receives a varied program and notes that it does not accurately reflect its operations, it may ask the Secretary for an amendment to that varied program to better reflect its operations.

#### *4.51FC Consideration of request to amend AACA security program as varied by the Secretary*

This regulation provides for the Secretary to consider an AACA's request to amend a varied security program. The Secretary must take into account the following matters in making this decision to accept the amendment to the variation: the existing circumstances as they relate to safeguarding against unlawful interference with aviation; the current use of the AACA security program by a business of the kind carried on by the AACA; the efficient administration of the AACA scheme; and any other matter the Secretary considers relevant.

#### *4.51FD Secretary may direct AACAs to vary security programs*

This regulation is distinguished from regulation 4.51FB by the Secretary directing the AACA to vary the program as opposed to providing a varied program under 4.51FB. For example, this may be an email from the Secretary to the AACA to direct the AACA to change parts of the program, or to take out a section and replace it with a new section. Under this regulation, the AACA needs to provide the Secretary with the varied program in accordance with the

direction. If the AACA does not vary the program in accordance with the notice of direction, then that is a ground for revocation of the AACA's accreditation.

#### *4.51FE AACA may request Secretary to vary AACA security program*

Under this regulation, the AACA may request the Secretary to vary the AACA security program. This provides an opportunity for AACAs to request a variation of their program.

#### *4.51FF Consideration of request to vary AACA security program*

This regulation provides for the Secretary to consider a request made by the AACA to vary its security program. The Secretary must take into account the following matters in making this decision: the existing circumstances as they relate to safeguarding against unlawful interference with aviation; the current use of the AACA security program by a business of the kind carried on by the AACA (for example, if the AACA is in a particular type of industry such as courier services, the program should be tailored towards this industry); and the efficient administration of the AACA scheme. In relation to other relevant matters, these may include safeguarding against unlawful interference with aviation, accuracy of information in the proposed varied program or whether the variation allows effective compliance and audit processes to be conducted.

This decision by the Secretary is also subject to further oversight and review under regulation 8.05.

### **Item [19] – Subregulations 4.51G(2) and (3)**

These subregulations are repealed. Subregulation 4.51G(3) is repealed as the defence of reasonable excuse is not consistent with the strict liability offences for known consignors and RACAs. As AACAs play a critical role in ensuring cleared cargo remains cleared in the supply chain, it is appropriate to align the strict liability offence that applies to known consignors and RACAs for AACAs. Non-compliance examples include an AACA not adhering to chain of custody measures as outlined under its program. The imposition of the strict liability offence here is consistent with the principles in *A Guide to Framing Commonwealth Offences*. This is a specific offence which has strict criteria. Requiring proof of fault in this instance will undermine deterrence. It will be particularly difficult to prove fault in these circumstances as extensive documentation regarding an intent to breach the security program is required to establish the fault elements of the AACA. AACAs are also placed on notice to guard against the possibility of any contravention under their security programs. Furthermore, if fault is required for this offence, significant resources will be needed for enforcement and this will significantly impact on the resources available to ensure the security of the air cargo supply chain.

### **Item [20] – Regulation 4.51H**

This regulation is repealed, along with the applicable offence. There is no longer a requirement for AACAs to notify the Secretary of information changes under the regulations.

However, this does not preclude the AACA security program from prescribing these requirements under the measures and procedures for quality assurance and incident response.

In place of the repealed regulation is a new offence for persons that disclose information about an AACA security program, where that person does not have the consent of the AACA to do so. This offence aligns with the offences for disclosing information for known consignors and RACAs.

#### **Item [21] – At the end of Division 4.1A**

##### *Subdivision 4.1A.6—Other matters*

##### *4.51J Offence—disclosure of information*

This offence takes the offences in previous regulation 4.46 and consolidates them for application for aviation industry participants other than RACA, AACA and known consignors. This offence applies in relation to the disclosure of airline or flight details about how particular cargo will be carried, and that the disclosure is not in accordance with a security program. The penalty units carried over from previous regulation 4.46 remains unchanged. Furthermore, it is appropriate to sub-delegate this offence to the security program, as the contents of the security program are technical in nature and are subject to change. For example, it would be impractical to prescribe in the amending Regulation the different disclosure requirements for each individual business. Lastly, aviation industry participants (other than RACA, AACA and known consignors) must submit their TSP for approval under section 18 of the Act, which provides them with control over how they comply with disclosure requirements their TSPs.

#### **Item [22] – After regulation 8.03**

This regulation provides for review of decisions in relation to known consignors.

#### **Item [23] – At the end of regulation 8.04**

This change establishes the same review of decisions for RACAs in relation to a Secretary's decision to refuse to accept amendments to a RACA security program.

### **Part 2—Application and transitional provisions**

#### **Items [24 to 27] – Application and transitional provisions**

These items provide transitional provisions in relation to recently amended regulations including the *Customs and Other Legislation Amendment (Australian Border Force) Regulation 2015*, the *Aviation Transport Security Amendment (2015 Measure No.1) Regulation 2015* and the *Transport Security Legislation Amendment (Job Ready Status) Regulation 2015*.



## **Item [28] – in the appropriate position in Part 10**

### *10.04 Definitions*

This regulation provides for a reference to definitions used in Part 2 – Application and transitional provisions.

### *10.05 Continuation of existing designation for RACAs who have a notice given under regulation 4.41J*

The operation of this regulation provides for an existing RACA that examines cargo under a notice given under current regulation 4.41J to continue its designation as a RACA. This means that a RACA that currently has been issued with a notice under regulation 4.41J will be transitioned to a RACA after November 1, 2016.

Under subregulation 10.05(3), the duration of the RACA designation is set by this transitional subregulation. If the TSP for the RACA will have remained in force until on or after 1 July 2017, then the designation for the RACA continues until the end of that TSP expiry date (unless the RACA's designation is revoked earlier). For example, if a RACA's TSP was to expire on 2 July 2017, then the designation of the RACA will continue until 2 July 2017. To remain designated as a RACA after 2 July 2017, the RACA must go through the designation renewal process.

Under subregulation 10.05(4), if the TSP for the RACA expires sometime between 1 November 2016 and 30 June 2017, then the designation of the RACA has effect until the day specified by a written notice by the Secretary (unless it is revoked earlier). Under this circumstance, the Secretary is required to give notice to the RACA by 15 November 2016 and specify a new date until which the designation has effect. For example, if a RACA's TSP was to expire on 29 December 2016, the Secretary must write to the RACA and provide a new date which the designation has effect. The Secretary may choose to extend the previous designation for another 12 months until 29 December 2017. After 29 December 2017, the RACA will need to go through the renewal process for designation to remain as a RACA.

### *10.06 Security programs for RACAs whose designation has been continued under regulation 10.06*

This regulation provides for transitioning the TSP of a RACA whose designation is continued under regulation 10.06. If a TSP was in effect on or after 1 November 2016, that previous TSP becomes the RACA security program provided by the Secretary under regulation 4.46. Furthermore, the measures and procedures to be used for handling and treating suspect cargo under subregulation 2.41(5) of the old regulations become measures and procedures for handling and treating high risk cargo under the amending Regulation. The intent of the changes is to allow the previous TSPs to continue operating as RACA security programs, and for those references in the previous TSP to suspect cargo to be treated as references to high risk cargo.

As the transition may create some obsolete or inconsistent references in a RACA security program, subregulation 10.06(3) provides for the Secretary to direct the RACA to vary its RACA security program. Despite the existing framework of direction to vary under subregulation 4.46D(4), the variation in this instance comes into force when the notice of variation is given to the RACA. This allows the variation to come into force the moment the Secretary issues the direction to vary, which provides regulatory certainty that the variation is in place immediately upon the Secretary issuing the notice for direction to vary (regardless of whether the RACA has sent back the varied program). This mechanism is required during the transitional phase to enable the Secretary, if required, to efficiently transition RACAs onto a new security program in a short amount of time. This is required to ensure that industry has sufficient time to prepare for new air cargo arrangements for cargo destined to the United States by 1 July 2017.

Under subregulation 10.06(6), if the RACA does not vary the program in accordance with the direction to vary under subregulation 10.06(3), the Secretary may immediately revoke the RACA's designation as a RACA.

To avoid doubt, the TSP that is transitioned to become a RACA security program remains in force for so long as the RACA is designated as a RACA. This is a change from the previous framework for TSPs, where the previous TSPs had an expiry date of five years.

#### *10.07 Transition of existing designations for RACAs who do not have a notice given under regulation 4.41J*

The operation of this regulation provides for existing RACAs that do not examine cargo under a notice given under current regulation 4.41J to transition to AACAs. This means that RACAs that have not been issued with a notice under regulation 4.41J will be transitioned to an AACA after 1 November 2016. The intention of this transitional provision is to give effect to the RACA to AACA transition policy. Under the new air cargo security framework, an industry participant can only be a RACA if it examines cargo under a notice under 4.41J or 4.41JA. This provides for a clear mechanism to recognise when cargo has been examined and cleared.

Under subregulation 10.07(3), the duration is set for the accreditation for the newly transitioned AACA. If the TSP for the RACA (previous to the transition) will have remained in force until on or after 1 July 2017, then the accreditation for the newly transitioned AACA continues until the end of that expiry date in the TSP (unless the AACA accreditation is revoked earlier). For example, if a RACA's TSP was to expire on 2 July 2017, then the new AACA will continue its accreditation until 2 July 2017. To remain accredited as an AACA after 2 July 2017, the AACA must go through the accreditation renewal process.

Under subregulation 10.07(4), if the TSP for the RACA expires sometime between 1 November 2016 and 30 June 2017, then the accreditation of the newly transitioned AACA has effect until the day specified by a written notice by the Secretary (unless the AACA accreditation is revoked). Under this circumstance, the Secretary is required to give notice to the AACA by 15 November 2016 and specify a new date until which the accreditation has

effect. For example, if a RACA's TSP was to expire on 29 December 2016, the Secretary must write to the newly transitioned AACA and provide a new date until which the accreditation has effect. The Secretary may choose to extend the previous designation (to an accreditation) for another 12 months until 29 December 2017. After 29 December 2017, the AACA will need to go through the renewal process for accreditation to remain as an AACA.

*10.08 Security programs for RACAs whose designation has been transitioned to accreditation as an AACA under regulation 10.07*

This regulation provides for transitioning the TSP of a RACA whose designation is transitioned to an accreditation as an AACA under regulation 10.07. If a TSP was in effect on or after 1 November 2016, that previous TSP becomes the AACA security program provided by the Secretary under regulation 4.51F. Furthermore, the measures and procedures to be used for handling and treating suspect cargo under 2.41(5) of the regulations become measures and procedures for handling and treating high risk cargo under the amending Regulations. The intent of the changes to suspect cargo is to allow the previous TSPs to continue operating as AACA security programs, and for those references in the previous TSPs to suspect cargo to be treated as references to high risk cargo.

As the transition may create some obsolete or inconsistent references in an AACA security program, subregulation 10.08(3) provides for the Secretary to also direct the newly transitioned AACA to vary the AACA security program (which is the previous TSP taken to be an AACA security program). Despite the existing framework of direction to vary under subregulation 4.51FD(3), the variation in this instance comes into force when the notice of variation is given to the AACA. This allows the variation to come into force the moment the Secretary issues the direction to vary, which provides for regulatory certainty that the variation is in place immediately upon the Secretary issuing the notice for direction to vary (regardless of whether the AACA has sent back the varied program). This mechanism is required during the transitional phase to enable the Secretary, if required, to efficiently transition RACAs to AACAs and provide them with a new AACA security program in a short amount of time. This is required to ensure that industry has sufficient time to prepare for new air cargo arrangements for cargo destined to the United States by 1 July 2017.

Under subregulation 10.08(6), if the AACA does not vary the program in accordance with the direction to vary under subregulation 10.08(3), the Secretary may immediately revoke the AACA's accreditation as an AACA. For example, if the AACA does not respond within the set time period provided under subregulation 10.08(4), this will mean that the AACA did not vary the security program in accordance with the direction given under subregulation 10.08(3) and the Secretary may immediately revoke the AACA's accreditation.

To avoid doubt, the TSP that is transitioned to become an AACA security program remains in force for so long as the AACA is accredited as an AACA.

#### *10.09 Revocation of existing designation for RACAs who do not have a TSP in force immediately before 1 November 2016*

This regulation clarifies that if a person was designated a RACA before 1 November 2016 and the TSP for the RACA was not in force, then the previous designation of the RACA is taken to have been revoked under regulation 4.44. This means that any RACA that has an expired TSP before 1 November 2016 has their designation revoked on 1 November 2016.

#### *10.10 Continuation of existing accreditation for AACAs*

This regulation provides for continuing the accreditation of AACAs that were AACAs before the RACA to AACA transition under regulation 10.07. If a person was an AACA before 1 November 2016 under the old regulations, their accreditation as an AACA will continue as if they were accredited as an AACA under regulation 4.49.

Under the old regulations, an AACA accreditation did not need to be renewed. Subregulation 10.10(3) provides that the Secretary will need to set out the duration period of the accreditation by written notice by 30 June 2017. For example, an AACA under the previous regulations will continue to be accredited as an AACA after 1 November 2016, and the Secretary may issue a written notice to that AACA on 30 May 2017 to set out that the accreditation of that AACA lasts until, for example, 30 May 2018.

#### *10.11 Security programs for AACAs whose accreditation has been continued under regulation 10.10*

Under this regulation, the Secretary must provide a new AACA security program under regulation 4.51F for AACAs that have continued their accreditation. This ensures that AACAs will receive an updated security program that takes into account the new regulatory arrangements. The Secretary must provide this new program by 15 November 2016.

#### *10.12 Application of offence of loading cargo without security declaration*

This regulation governs the offence of loading cargo onto a prescribed aircraft without a security declaration. Regulation 4.41G applies to cargo that is loaded onto a prescribed aircraft on or after 1 November 2016, whether or not a security declaration was made before that day.

#### *10.13 Notices issued under regulation 4.41J*

This regulation transitions notices that have been issued under the old regulation 4.41J into either a 4.41J notice or a 4.41JA notice of the amending Regulation. This enables notices that have been issued before 1 November 2016 to still be valid under the amending Regulation. Depending on the nature of the notice issued, it may be dealt with either as a notice under 4.41J or as a notice under 4.41JA. For example, if the notice issued under the old regulation 4.41J had enhanced examination requirements, it may be dealt with as a 4.41JA notice after 1 November 2016. However, these transitional notices will only have effect until 30 June 2017.

### *10.14 High risk cargo*

This regulation gives effect to applying high risk cargo references to TSPs prepared or varied for operators of a prescribed air service on or after 1 November 2016.

## **Schedule 2—Amendments commencing 1 July 2017**

### **Part 1—Amendments**

#### **Item [1] – Regulation 1.03**

This regulation inserts two new definitions. These are category 1 and category 2 destinations. In order to meet United States TSA requirements, category 1 destination is prescribed under the amending Regulation as a destination within the United States of America. Category 2 destination means a destination other than a category 1 destination. Currently, the only country in category 1 is the United States of America.

#### **Item [2] – Paragraph 4.41CA(2)(a)**

This regulation makes changes to Schedule 1 by requiring that cargo receiving clearance via examination from a RACA is different for category 1 and category 2 destinations. For a category 1 destination cargo to receive clearance, the cargo must be examined by a RACA in accordance with a 4.41JA notice. For category 2 destinations cargo to receive clearance, the cargo may be examined by either a 4.41J or a 4.41JA notice to receive clearance.

#### **Item [3] – Subparagraph 4.41D(c)(viii)**

This regulation makes changes to Schedule 1 by requiring that security declarations contain information about the examination method applied to cargo for category 1 and category 2 destinations. For example, if cargo is travelling to the United States, the security declaration will need to contain information about the examination method applied to the cargo by the RACA, including whether it was examined under a 4.41JA notice.

#### **Item [4] – Regulation 4.41D (note 1)**

This amendment makes a change to the note under regulation 4.41D to cross reference to the changes made under Item [3].

#### **Item [5] – Paragraph 4.41F(3)(c)**

This regulation amends the offence provision by setting out the new offence provision commencing on 1 July 2017 for issuing security declarations. This amendment makes it an offence for a RACA to issue a security declaration if it has not examined the cargo to be unloaded at a:

- category 1 destination—under a notice issued under regulation 4.41JA; or
- category 2 destination—under a notice issued under regulation 4.41JA or 4.41J.

**Item [6] – Regulation 4.41J (heading)**

This regulation substitutes the heading for 4.41J notice to be clear that the notice is used for category 2 destinations.

**Item [7] – Subregulation 4.41J(2)**

This item removes the Schedule 1 examination requirement reference and sets out that the requirements that the 4.41J notice is used for cargo that is to be unloaded at a category 2 destination.

**Item [8] – Subregulation 4.41J(2)(note)**

This item repeals the note.

**Item [9] – Regulation 4.41JA (heading)**

This item repeals the heading and substitute it with a new heading that links the notice to examination of cargo for a category 1 destination.

**Item [10] – Subregulation 4.41JA(2)**

This item removes the Schedule 1 reference for the examination notice under regulation 4.41JA to be clear that the notice is used for examining cargo that is to be unloaded at a category 1 destination.

**Item [11] – Subregulation 4.41JA(2) (note)**

This item removes the Schedule 1 note and replaces it with a new note. The new note makes it clear that while a 4.41JA notice may be used to meet examination requirements for a category 1 destination, the notice may also be used to meet examination requirements for category 2 destinations.

**Part 2—Application and transitional provisions**

**Item [12] – At the end of Division 4 of Part 10**

*10.15 Offence of loading cargo without security declaration—from 1 July 2017*

This amendment provides for new requirements for regulation 4.41G under Schedule 1. From 1 July 2017, if cargo is to receive clearance via examination and is to be unloaded at a category 1 destination, the cargo must have a security declaration that states the cargo has been examined in accordance with a regulation 4.41JA notice. This amendment requires a regulated business loading cargo on a prescribed aircraft for a category 1 destination to check whether the security declaration states that it has been examined under a regulation 4.41JA notice. Cargo that does not require examination to receive clearance is not affected by this amendment. For example, cargo that receives clearance via a known consignor must have a security declaration, but that declaration does not need to meet the requirement to state that it

has been examined under a 4.41JA notice (this is because cargo does not need to be examined to receive clearance if it originates from a known consignor).

For category 2 destinations, cargo that receives clearance via examination must have a security declaration that states the cargo has been examined in accordance with either a regulation 4.41J notice or a regulation 4.41JA notice. This means that cargo that is inbound to category 2 destinations has a wider range of options for its examination before it can be loaded. For category 2 destinations, cargo originating from a known consignor or is otherwise covered in a notice made under subparagraph 44B(2)(b)(i) of the Act will not need to be examined to receive clearance.

#### *10.16 Notices issued under regulation 4.41J—from 1 July 2017*

This amendment transitions any legacy 4.41J notices issued before 1 July 2017 to 4.41J notices under Schedule 2. For example, if a RACA was issued a 4.41J notice on 27 February 2017, that notice will still have effect on and after 1 July 2017 as if the notice has been issued under the schedule 2 amendments.

#### *10.17 Notices issued under regulation 4.41JA—from 1 July 2017*

This amendment transitions any legacy 4.41JA notices issued before 1 July 2017 to 4.41JA notices under Schedule 2. For example, if a RACA was issued a 4.41JA notice on 27 February 2017, that notice will still have effect on and after 1 July 2017 as if the notice has been issued under the schedule 2 amendments.