

Civil Aviation Authority (CAA)

Cargo Agents (Known Consignor) Guide - Version 5 (CAP 1810)



Contents	2
Version Control	4
Document Security	5
Introduction and Legal Basis	5
Recommended Practices and Guidance	6
The Purpose of the Scheme	6
United Kingdom Civil Aviation Authority (CAA) contact details	6
The Known Consignor Scheme	7
The Approval Process	8
Applying for Approval	8
The Security Programme	8
Validation Fees	10
Access to Premises, Staff and Documents	10
Suitability – Types of Operation	10
Prohibited Articles	11
Manufacturer	11
Distributor	11
Museums and Art Galleries	11
Temporary Exporter	12
Preparation and Responsibilities	13
On-site validation	13
Site Security	14
Security Culture and Insider Threat Policy Requirements	15
Cyber Security	17
Security Management System (SeMS)	18
Identifiable Air Cargo	19
Production (where applicable)	19
Packing (where applicable)	19
Storage (where applicable)	20
Despatch	20
The Audit Trail	20

Consignment Security Certificate (CSC)	20
Electronic Notification of Despatch	22
Transportation	23
The Known Consignor uses own transport	23
The Known Consignor arranges a non-regulated hauler themselves	23
The Known Consignor uses a Regulated agent	24
The Known Consignor uses a Regulated agent who in turn sub-contracts a haulier	24
Vehicle and Driver Checks	25
United Kingdom Supply Chain Security Database	26
Where Security Controls Have Not Been Applied	27
Staff Recruitment	28
Staff Security Training	31
Feedback and Rectification	34
Post Audit	35

Annex A

Useful websites	36
-----------------	----

Document Outline

Version Control

Title	Cargo Agents (Known Consignor) Guide - Version 5 (CAP 1810)		
Authors	Brian Lockie, Mark Foskett and Emma Heather		
Authority	Jonathan Clay		
File Copy	Stored within SharePoint @ CAA.		
Distribution	1. Director and Deputy Director CAA Aviation Security 2. Heads of CAA Aviation Security Regulation & Compliance 3. CAA Head of Training 4. All CAA Compliance Team Managers 5. CAA Compliance Team support 6. All CAA Aviation Security Compliance Auditors 7. All Cargo Agents - Known Consignors		
Version Control	Version	Date	Status
	2.0	12/05/2020	PO FINAL
	2.1	10/12/2020	CW EU Exit Update
	2.1.1	08/02/2021	CW Minor Revision
	3.0	25/04/2023	MF Review & update
	4.0	27/06/2024	TP Air Cargo Agents changes
	5.0	22/07/2026	BL/MF/EH Review & update
Copyright	© 2026 Copyright CAA		

Document Security

This document has been produced to assist Cargo Agents (Known Consignors) in meeting the requirements of aviation security regulations. It contains sensitive information and must be protected.

There is no security classification attached to this document. Due to the nature of the contents, however, this document should:

- be stored securely when not in use; and
- securely destroyed when no longer required

Introduction and Legal Basis

Known Consignors, listed and approved for purposes relating to aviation security under point 3(1) of the Aviation Security (Air Cargo Agents) Regulations 2024 are directed to comply with the relevant provisions of the Single Consolidated Direction (Aviation) (“the SCD”).

This means that approved Known Consignors, as directed parties, must follow relevant aviation security regulations. Of specific relevance in the SCD to the Known Consignor programme are chapters 6 (cargo and mail; principally point 6.4) and 11 (staff recruitment and training).

Approved Air Cargo Agents are listed as a Regulated Agent, a Known Consignor, or a Regulated Supplier. This guide is aimed at Air Cargo Agents (Known Consignors), and for the remainder of this guide reference will be made to ‘Known Consignor.’

A “Known Consignor” means a consignor who originates cargo for its own account and whose procedures meet security rules and standards sufficient to allow carriage of cargo or mail on any civilian aircraft.

This guidance has been developed for Known Consignors to assist an entity to assess their operation and existing security arrangements against the required criteria for the

listing of Known Consignors as described in The Aviation Security (Air Cargo Agents) Regulations 2024.

Recommended Practices and Guidance

In addition to the regulatory requirements outlined within Chapter 6 (Cargo and Mail) and Chapter 11 (Staff Recruitment and Training), this guide will also incorporate recommended practices and guidance that enhance the United Kingdom supply chain security and support a positive security culture.

The Purpose of the Scheme

The Known Consignor scheme is voluntary. There is no legal requirement for any air cargo to be despatched from the shipper having had security controls applied. Unsecure cargo may still be sent for carriage as Air Cargo; however, it will be subject to additional security measures carried out by a Regulated Agent before it can be allowed to fly. Once approved as a Known Consignor, however, an entity must comply with the requirements outlined within the aviation security regulations as a 'directed party.'

Once approved, Known Consignors are permitted to transport cargo as suitable to be treated as SPX (Secure for passenger, all-cargo and all-mail aircraft) from source. Such cargo may be transported by air without the need for any further screening security measures being applied.

United Kingdom Civil Aviation Authority (CAA) contact details

Known Consignor Scheme

Aviation Security

Civil Aviation Authority

11 Westferry Circus

London

E14 4HE

E-mail: KCSupport@caa.co.uk

Link: [Security compliance | UK Civil Aviation Authority](#)

The Known Consignor Scheme

To be approved and listed, a Known Consignor needs to meet the standards required for the shipping of SPX cargo as outlined in this guidance and then make an application to the CAA for the locations for which Known Consignor status is being sought.

Each location will be subject to an on-site validation audit. This audit is undertaken by a Civil Aviation Authority National Aviation Security Compliance Auditor. The auditor will assess the security programme submitted as part of the application process as well as all the relevant processes being undertaken to determine whether the required standards are met for shipping SPX cargo.

The auditors are aware that different consignors operate in separate ways. The auditor will seek to recognise procedures that are already in place such as anti-theft, stock control or quality assurance processes, together with existing access control measures to the premises and other relevant areas. Additionally, the auditor will check that Known Consignors meet the regulatory recruitment and training criteria as listed below.

CAA National Aviation Security Compliance Auditors undertake both announced and unannounced audit activity. A CAA auditor has a statutory right of access to approved Known Consignor premises at all times.

The decision to approve a new Known Consignor site rests with the Department for Transport based on a CAA recommendation.

Once approved and listed as a Known Consignor site on the United Kingdom Supply Chain Security database, each location will be subject to on-site audits at regular intervals to retain its Known Consignor status.

The site listing or re-listing is dependent on:

- A written application being submitted to the CAA
- An up-to-date security programme that has been appropriately signed and dated by a legal representative or person responsible for security, being submitted to the CAA
- Payment of the annual fees
- A successful on-site validation audit

The Approval Process

Applying for Approval

Existing or prospective Known Consignors should apply online using the following link:
[Known consignor scheme | UK Civil Aviation Authority](#)

A new Known Consignor applicant will be contacted via email by the CAA compliance team manager upon application. The compliance team manager will designate a team member as the principle point of contact for the review of the security programme, initial site audit and validation.

An existing Known Consignor that is re-applying may be audited at any time during the listing period. The date of audit may not always be linked to the validation expiry date. On-site audits may be on an announced or unannounced basis.

The CAA seeks to work with the Known Consignor on an announced basis to mutually agree a date. There may be limited flexibility, however, as CAA auditors have a national responsibility with the need to match travel dates with geographically located demand to ensure efficiency of deployment and value for money. There is an expectation, therefore, that during operational hours there will be a suitably trained staff member on site who will be able to deal with a CAA audit, even at short or no notice.

The Security Programme

The application and re-approval process requires the submission of a security programme for approval by a CAA auditor. The approval will be based on the relevance and completeness of the security programme and the implementation of the security programme without deficiencies.

The CAA supplies new applicants with a security programme template. Whilst the template does not have to be utilized, the key elements incorporated within it need to be present in any programme submitted.

There is a requirement for a Known Consignor to draw up, apply and maintain a security programme. That programme shall describe the methods and procedures which are to be followed by the entity to comply with the national aviation security programme (NASP).

If the appropriate authority (Department for Transport) is no longer satisfied that the Known Consignor complies with the requirements of the Known Consignor regulations, the

appropriate authority may withdraw the status of a Known Consignor.

The following key areas need to be considered when drawing up the security programme:

- The programme shall describe the methods and procedures which are to be followed by the entity to comply with the national aviation security programme.
- There must be sufficient narrative included under various headings within the security programme to accurately reflect the operation and the security processes adopted.
- There must be sufficient breadth and depth of detail to fully and accurately describe exactly how the security processes are applied and followed. The descriptions provided should enable a third party to fully understand how the facility operates.
- The security programme must be maintained to accurately reflect current operating procedures.
- If there are any changes to processes or key personnel, these must be reflected in the security programme and notified to the CAA within 7 days.
- The programme shall include internal quality control provisions describing how compliance with these methods and procedures is to be monitored by the entity itself.
- The security programme must include an appropriate internal policy and related measures enhancing staff awareness relating to the insider threat and promoting security culture.
- Cyber security mitigating measures.
- The security programme should be under constant review and in any case at least annually when seeking re-validation.
- The security programme must be signed and dated by the applicant's legal representative or by the person responsible for security at the site. A wet, digital, or electronic signature is required.

The security program is ever evolving in line with regulatory updates and recognised good practice within the aviation security sector. The CAA will update and distribute the security programme template when required.

It is essential that all the guidance narrative within the CAA supplied security programme template is read thoroughly and understood. If anything included is not relevant to the site, then it needs to be amended or edited out. The content must accurately reflect the operation and procedures at the site. The security programme sign off is a declaration that the content is true and accurately reflects procedures and processes on site.

Validation fees

The annual validation fee to be a Known Consignor is subject to change. The details can be found within the following link:

[ORS5 No. 440: CAA Scheme of Charges: Aviation Security | UK Civil Aviation Authority](#)

Subsequent audits may be required if the first on-site validation audit is unsuccessful. There is currently no cost attached to the re-audit, but this may be subject to review and change under the CAA Scheme of Charges.

Access to premises, staff, and documents

It is important that the auditor can deal with relevant staff during the audit and access required records.

This will include:

- The designated Known Consignor Site Security Representative and/or their deputy
- A representative responsible for Known Consignor staff recruitment and training
- All supporting documents must be available in a presentable manner, including Known Consignor staff recruitment and training records
- Access may be required to all parts of the operation. On site staff must be able to facilitate this. Specialist personal protective equipment may have to be provided

Suitability – Types of Operation

The prepared cargo must be originated by the company on the site to be audited. The Known Consignor must, through the security processes adopted and without any form of screening, be confident that it does not contain any prohibited items.

An entity will have to determine at which point a consignment of cargo/mail becomes identifiable as air cargo/mail and demonstrate that there are relevant security measures in place to protect it from unauthorised interference or tampering. This will include details concerning the production, packing, storage, and despatch of identifiable air cargo.

Prohibited articles

Assembled explosive and incendiary devices that are not carried in accordance with the applicable safety rules shall be considered prohibited articles in cargo and mail.

Manufacturer

A manufacturer produces the product from raw materials or components and so has knowledge of exactly what is being produced. The Known Consignor must determine at what point within the on-site process items are suitable to be considered as SPX. Ideally this should be at the latter end i.e. at the point selection of goods for transport is made.

Distributor

A distributor is an organisation which takes in cargo which cannot be identified as air cargo, and which is therefore unsecure. The organisation originates the cargo by choosing which cargo, from a choice of many identical or comparable items, to send by air. This choice must be made entirely by the distributor without any other organisation or person being able to influence or predict which items are going to be identified. This type of operation is often referred to as a 'pick and pack' process.

Museums and Art Galleries

Works of art travelling as air cargo from the United Kingdom require security procedures to be applied to them. There are several specialists regulated agents who deal with fine art, and who can make works of art secure air cargo by hand search. However, a major consideration for museums and art galleries is to avoid unnecessary handling of their works. Known Consignor status can avoid this. The Known Consignor must at be able to demonstrate how items to be transported as secure air cargo are checked, secured, and protected from unauthorised interference from point of selection through to storage, despatch, and transport.

Temporary Exporter

Some organisations do not despatch individual items of cargo on a one-time basis. Instead, the cargo is exhibited, used in competition, or operated on hire or loan by another organisation and returned to the consignor. Therefore, the cargo will be despatched, go outside the direct control of the consigning organisation and be returned to the consignor.

When the cargo is returned, it will be 'unsecure' as it has been outside the secure supply chain. The Known Consignor, before re-despatching the cargo will have to rebuild, repair or otherwise closely examine and/or test the contents – in an equivalent manner to that undertaken whilst manufacturing the cargo. The flow of cargo must be unpredictable to the manufacturer and others within the industry.

Preparation and Responsibilities

Known Consignors are contacted directly by email by the auditor who will be completing the on-site validation. The email will outline the date and time of the audit and what is required to facilitate it. The security programme for the site, if not already submitted, must be made available in advance of the audit date. It is essential that a reply is made as soon as possible by email to maintain the audit trail of communication.

The email will have attached the latest CAA Known Consignor Guides.

These include:

- Cargo Agent (Known Consignor) Security Programme Template
- CAA CAP 1810: Cargo Agent (Known Consignor) Guide
- CAA CAP 2330: Aviation Security Recruitment Guide

The CAA will endeavour to undertake a 'new site' initial on-site validation audit within 6 weeks of the applicant confirming with the CAA that they have fulfilled the regulatory requirements and are ready to receive an audit. The appointed CAA auditor will liaise with the site security representative (SSR) to arrange a suitable date.

Thereafter annual re-validation audits will be conducted on an announced or unannounced basis. Audit activity conducted by the CAA within the aviation security sector is ordinarily conducted on an unannounced basis.

If an announced notification is received, there is an expectation that the allocated date is fixed. CAA auditors have a national responsibility, with the need to match travel dates with geographically located demand, to ensure efficiency of deployment and value for money. Additionally, resources are limited, and audit demand is high.

On-site validation

The purpose of the on-site validation is to enable the CAA auditor to verify that the contents of the submitted security programme are being implemented and confirming the absence of deficiencies.

The on-site validation will be recorded in a secure CAA electronic report format. The auditor may make entries directly via laptop and/or take written notes at the time.

The audit will ordinarily follow the structure of the CAA Known Consignor security programme template, with assessment being made in the following key areas:

- Site Security
- Identifiable Air Cargo
- Packing
- Storage
- Despatch
- The Audit Trail
- Transportation
- Recruitment and Training

The audit is a thorough process that is aimed at ensuring the correct security controls and processes are being adopted in relation to secure air freight. The auditor will ask comprehensive questions; observe site features and processes; inspect documentation; review CCTV images if necessary. The on-site validation will normally take several hours.

Site Security

A Known Consignor shall designate at least one person at each site who shall be responsible for the application and supervision of the implementation of security controls at that site. This person shall have successfully completed a background check. The nominated person is known as the site security representative (SSR). The SSR and Deputy should hold a relevant position within the organisation such that they effectively manage the security of air cargo and can effect change.

For clarity, the position of SSR is site specific. The appointed SSR should ordinarily work at the site in question and spend most of their working time there. An SSR cannot be appointed as responsible for more than one site.

To ensure resilience and to facilitate management oversight of the Known Consignor operation, the nomination of a suitable deputy or deputies to cover leave dates etc. for the nominated SSR should be catered for. Such individual(s) must be background checked, and security trained to the same level as the nominated SSR. This will also be beneficial in adequately dealing with announced or unannounced CAA audits.

A Known Consignor shall ensure that there is a level of security on the site or at the premises sufficient to protect identifiable air cargo and identifiable airmail from unauthorised interference.

Additionally, during production, packing, storage, despatch and/or transportation, as appropriate, identifiable air cargo and identifiable airmail is protected from unauthorised interference or tampering.

It is essential that access to the area where air cargo/mail is processed or stored is controlled. An entity will be required to demonstrate how a site is protected (e.g. a physical fence or barrier) and that appropriate access control procedures are in place for identifiable air cargo. Where applicable, details will be required of any installed alarm and or CCTV systems, on-site security staff, etc. All doors, windows, and other points of access to air cargo/mail need to be secured or subject to access control.

It is recommended practice for all staff involved in a Known Consignor role to be issued with a company photographic ID bearing their name that is prominently displayed or kept on the person at all times whilst accessing secure air freight.

The issue of company ID must be controlled and accounted for. As this function is integral to the overall site security and relevant to the Known Consignor parts of the building, anyone involved in this process should be background checked, and security trained. There should be a supervisory oversight of this process which is incorporated within internal quality assurance activity.

A Known Consignor must be able to demonstrate how statutory authority personnel (the CAA auditor) are correctly identified before being allowed on site and given access to Known Consignor materials. Any checks that facilitate access to secure air cargo/mail must be undertaken by a Known Consignor trained member of staff.

Annex A provides a list of useful websites with advice on protective security and security of premises.

Security Culture and Insider Threat Policy Requirements

Under the National Aviation Security Programme (NASP), it is a requirement for any entity required to have a security programme to include in that programme an appropriate internal policy, and related measures, aimed at enhancing staff awareness, and promoting security culture, to address the insider threat.

This can be achieved by having separate policies on security culture and insider threat or combining under one policy or including it within the operations manual or similar document. An effective security culture will cater for insider threat.

The policy or policies must include the following:

Insider threat - the processes and practices that:

- help to deny, deter, and detect the insider threat; and
- enables timely and proportionate action to be taken when insider risks are identified.

Security culture – the processes and practices in place to promote / implement /embed a positive security culture.

A description of the approach the entity will take to ensure that all staff receive training to understand their role in mitigating insider risk and supporting a positive security culture.

Developing and sustaining an effective security culture is an essential component of a protective security regime and helps mitigate against a range of threats that could cause physical, reputational, or financial damage to the company. Security culture refers to the set of values, shared by everyone in the company, which determine how people are expected to think about and approach security. Getting security culture right will help develop a security conscious workforce and promote the desired security behaviours from staff.

The benefits of an effective security culture include.

- A workforce that are more likely to be engaged with, and take responsibility for, security issues
- Increased compliance with protective security measures
- Reduced risk of insider incidents
- Awareness of the most relevant security threats

As mentioned, a positive security culture provides the sound foundations of mitigation against a range of threats and vulnerabilities. When considering mitigating measures in relation to the insider threat, the following key areas should be addressed:

An effective security culture:

A nominated member of the company executive accountable for its implementation. This individual should have overall control of security. A risk assessment should assist strategic decisions.

Structured approach – ideally part of a Security Management System (SeMS) (see page 18), a risk driven framework designed to embed security within operations and culture.

On-going education:

Staff to be trained at earliest opportunity in relation to the threat that can be posed.
Encourage staff vigilance and confidence.

Training to be on-going. KC staff receive initial and recurrent training. Therefore, seek to promulgate the message to others appropriate to the functions they perform.

To ensure vigilance is maintained, on-going messaging at all levels. Where possible, position security as an enabler to help achieve business objectives.

A joined-up response:

Know what to do if an insider threat is identified. Prepare for worst case scenario by having a tabletop exercise involving all interested parties, both internal and external e.g. at least security and HR departments. This will enable a comprehensive response agreed in advance.

The policy should reference the need for collaboration on insider threat matters, looking for, and exploiting, all opportunities to share lessons learned and promote awareness and best practice in the local community.

This is a regulatory requirement that forms part of the CAA Known Consignor validation. A Known Consignor must be able to demonstrate how this obligation is being met.

Cyber Security

Cyber-attack is an existing and on-going threat for companies and individuals. Whilst airports and other critical infrastructure areas relevant to aviation security have mandated regulated minimum standards to protect their critical information, communications technology systems and data areas from attacks, it is pertinent to highlight the issue with Known Consignors.

The Civil Aviation Authority is part of the global security community and receives updates regarding threats and in some cases imminent attacks, which affect the aviation sector. Relevant information will be shared. Sensitive information is passed via the secure Egress system, potentially out-of-hours.

It is appreciated that Egress accounts may not be monitored daily. It is good practice, therefore, to provide the CAA, where practicable, with a monitored group email address for the company. The security programme is a suitable location to record this point of contact for information sharing. Relevant information can be disseminated using this method, if necessary, referring to additional information sent via Egress. This will allow preventative action to be taken to protect your company.

The link to the CAA cyber website is: [Cyber Security | UK Civil Aviation Authority](#)

Security Management System (SeMS)

SeMS is an organised, systematic approach to managing security which embeds security management and security culture into the day-to-day activities of an organisation. It provides the necessary organisational structure, accountabilities, policies, and procedures to ensure effective oversight. SeMS is an assurance system for security.

The need to effectively manage security performance remains a constant priority. The regulator maintains an overview but cannot – nor should not – do it all. The Cargo Agent (Known Consignor) sector is best placed to ensure that it consistently delivers an elevated level of security and maintains vigilance. SeMS provides the tools and structure to do this. It is good for security and good for business.

The CAA oversees a SeMS programme. It will provide advice and guidance and dedicated support to Cargo Agents (Known Consignors) on how to pursue SeMS. Most will already have SeMS elements in place but perhaps not working together as an effective whole. SeMS will deliver better security assurance to all.

SeMS is a structured approach to quality assurance of security provisions. It consists of 10 steps.

1. Management Commitment
2. Threat and Risk Management
3. Accountability and Responsibilities
4. Resources
5. Performance Monitoring, Assessment and Reporting
6. Incident response
7. Management of change
8. Continuous Improvement
9. Awareness and Education
10. Communication

For further information on SeMS please visit www.caa.co.uk/SeMS where a free SeMS framework together with additional guidance documents are available to download. Guidance and advice is available from the CAA SeMS team via SeMS@caa.co.uk.

Identifiable Air Cargo

The auditor will confirm at which point the consignment of air cargo/mail becomes identifiable as such, for example at the initial order stage; during production; packing; storage; despatch. An assessment will be made regarding the measures in place to ensure the protection of cargo from the point it becomes identifiable air freight e.g. CCTV overview; physical protection; supervision etc. This relates to cargo/mail that is to be transported as secure air cargo under the Known Consignor approval and accompanied by a schedule 6.1 declaration (Consignment Security Certificate (CSC)).

The auditor will identify who has access to the air cargo from the point it becomes identifiable as such, to ensure the integrity of security is maintained. To access identifiable secure air cargo/mail an individual must either be suitably background checked, and security trained or be escorted by a person who meets these requirements. Consequently, the auditor will ascertain what provisions are in place for employees; contractors; cleaners; visitors etc.

Production (where applicable)

If the product can be identified as air cargo/mail during production, then measures must be taken to protect air cargo/mail from unauthorised interference or tampering at this stage. Access to the production area will need to be controlled and the production process supervised.

Packing (where applicable)

Access to the packing area must be controlled and the packing process supervised. If the product can be identified as air cargo/mail while packing, then measures must be taken to protect air cargo/mail from unauthorised interference or tampering at this stage.

Details of the packing process will be confirmed, and the Known Consignor must be able to demonstrate that all finished goods are checked prior to packing.

The finished outer packing needs to be robust and the method whereby the finished outer packing is made tamper evident demonstrated e.g. using numbered seals, security tape or bespoke stamps.

There must always be adequate security controls in place for materials used to make secure consignments tamper evident e.g. numbered single use plastic, metal or adhesive seals,

tamper evident tape.

Tamper evident materials must be stored securely; access must be controlled and stock as well as issue and use must be accounted for.

All tamper evident seals must be kept under secure conditions. Seals must be subject to effective stock control and issued from a central point by a designated person responsible for controlling and recording the issue of seals. A record of all seals issued must be kept and retained for a period of at least 7 days.

The process and means of packing and making consignments tamper evident as well as the processes to store, control and account for tamper evident materials should be articulated within the security programme.

Storage (where applicable)

Access to the area where identifiable air cargo is stored must be controlled. If the product can be identified as air cargo/mail whilst being stored, then measures will need to be taken to protect air cargo/mail from unauthorised interference or tampering at this stage.

Despatch

Access to the despatch area must be controlled. If the product can be identified as air cargo/mail during the despatch process, then measures must be taken to protect air cargo/mail from unauthorised interference or tampering at this stage.

Finally, the finished and packed air cargo/mail must be checked prior to leaving the site to ensure that no prohibited articles are present, and that the shipment has not been tampered with.

The Audit Trail

Consignment Security Certificate (CSC)

A defined audit trail of the security processes applied to a consignment is an important requirement of a robust process. It provides documentary evidence of the actions taken and processes followed that assist in confirming compliance with regulations, as well as providing a crucial tool and reassurance for internal quality assurance monitoring.

The auditor will ensure that the Known Consignor produces a schedule 6-1 security declaration in the correct format. This is done in the form of a Consignment Security Certificate (CSC). The detail of this form is found within the KC security program template.

The auditor will confirm that the person signing the CSC is aware that they are accepting responsibility for ensuring to the best of their knowledge that no prohibited items are contained within the consignment.

There should be an auditable trail or relationship between the signatory of the CSC and the packer of the shipment. The Known Consignor must identify who should sign the CSC and at what point in the process. Ideally, the packer is the person best placed to make the declaration that the consignment does not contain prohibited articles. If the packer is not the signatory, then there should be a documented/auditable communication between the packer and the person signing the CSC that would provide the necessary reassurances and provide a defined audit trail. The CSC must be signed after the identified air cargo is packed and made secure.

The CSC is a stand-alone security document and carries significant weight in ensuring that the supply chain security is maintained. All CSCs must be stored, prepared, and always moved securely. Blank templates, if stored electronically, should be stored on access controlled (password protected) computers. The template should be in a folder with access restricted to authorised Known Consignor staff only. Ideally, the document itself should also be password protected as an additional layer of security.

Computer screens should auto-lock within a narrow timeframe in the event an operative leaves a workstation. Consider using privacy screen covers on computer monitors to ensure that any sensitive information that relates to or may identify air freight cannot be overseen. Pre-signing CSCs in advance or remotely is not acceptable.

The unique consignment identifier used on the CSC must provide an auditable link with the consignment in question that will identify the make-up of the consignment (weights; dimensions; contents) order details; customer; destination etc. Any unique identifier may be used. This may be an air waybill number supplied by the regulated agent; an internally generated order or consignment number; individual crate/container numbers etc.

It is important that the CSC is completed accurately, signed and the original travels with the consignment. If the CSC is inaccurate, the consignment may be declared unsecure which means it may be delayed whilst it is made secure cargo at a Regulated Agents premises. This may also incur an additional cost for the consignor. Faxed or email copies of CSCs are not acceptable.

To provide an audit trail of the completion of the CSC, a Known Consignor must retain an

exact copy of the original signed document that accompanied the consignment. This can be retained as a hard copy or an electronic scanned copy. Ideally, this should be marked or stamped 'Copy' and must be retained to the same secure standards as the blank template i.e. only approved Known Consignor staff can access. A retention period of at least 14 days is recommended to allow the consignment to reach its destination.

Additionally, recommended practice is to maintain an up-to-date list of staff who are authorised to complete the CSC, together with their sample signatures. This assists if there are any queries raised in relation to the consignment, as well as ensuring – as part of internal quality assurance processes – that staff complete security declarations in a consistent and compliant manner. Again, this needs to be retained securely.

When completing a schedule 6-1 Consignment Security Certificate the following must be adhered to:

- The company UAI and address matches the information in the UK Supply Chain Security Database.
- The unique consignment identifier matches other documentation and the cargo Consignment.
- The wording and format of the declaration matches that contained in Schedule 6-1.
- The CSC contains the signature, name, and position in the company of the person signing the CSC.
- The date format is: dd/mmm/yy i.e. 02/Jul/25.
- The time format is: tttt i.e. 1108.
- The person signing must record their name in BLOCK capitals.
- The authorised signatory must be background checked and have completed the relevant training modules from the current Air Cargo (Known Consignor) Security Training syllabus.

Electronic Notification of Despatch

It is recommended practice to retain – as part of the consignment documentation – any communications made with the receiving Regulated Agent to whom the consignment is destined for - or the transporting haulier - regarding arrangements made for collection and the details of the consignment provided.

Improvements to United Kingdom supply chain security require Cargo Agents (Regulated Agents) to send an electronic notification of despatch (pre-alert) to the receiving Regulated Agent of the consignment. The notification should include, as a minimum, the unique identifier of the consignment and the scheduled date of the consignment's arrival.

This is an improvement to supply chain security and is recommended practice to be adopted into the Known Consignor process as well. An electronic notification to the receiving

Regulated Agent incorporating the aforementioned details should be sent. Confirmation of receipt should be requested.

Transportation

The prepared consignment needs to be adequately protected during transportation to the Regulated Agent to maintain the integrity of the supply chain security. To ensure that unauthorised interference or tampering has not been facilitated, the Known Consignor must demonstrate how the integrity of the consignment has been maintained.

There are four defined options for the transportation of secure air cargo.

1. The Known Consignor uses their own transport.
2. The Known Consignor uses a contracted haulier with whom they have a haulier agreement.
3. The Known Consignor uses a Regulated Agent.
4. The Known Consignor uses a Regulated Agent who in turn sub-contract a haulier with whom they have haulier agreement.

The Known Consignor uses their own transport

The Known Consignor must ensure that drivers have been trained to the required level and that the vehicles used are appropriate and can be secured. The means and methods of securing will need to be demonstrated.

The Known Consignor arranges a non-regulated haulier themselves

If a contracted haulier is used, the Known Consignor must ensure that there is a signed haulier declaration in place in the correct format.

A template Haulier Declaration is attached at Annex B. The Known Consignor should retain the original declaration. The haulier should also provide their drivers with a copy of this declaration which they should be able to produce if asked when delivering SPX cargo to a Regulated Agent.

To enter into an agreement, the Known Consignor must perform due diligence with regards to confirming with the haulier that they are capable of meeting the requirements of the haulier declaration i.e. a site visit of the haulier's premises; checking vehicle standards; checking driver recruitment and training records to ensure they meet the required standards.

When signing the declaration, the haulier is agreeing to ensure compliance with the National Aviation Security Programme, the haulier shall co-operate fully with all related compliance monitoring activity, as required, and provide access to documentation, facilities and premises as requested.

This process should be undertaken on an annual basis and a new declaration in the required format confirmed and signed.

The Known Consignor uses a Regulated Agent

There is no requirement to provide evidence about driver training where a CAA approved Regulated Agent has made the transport arrangements for collecting air cargo/mail from the Known Consignor.

To protect the secure air cargo from unauthorised interference or tampering, prior to handing the secure cargo over to the Regulated Agent, the status of the Regulated Agent must be verified. A validation check of the Regulated Agent must be undertaken on the United Kingdom Supply Chain Security Database on the day of despatch prior to collection. This should include the Regulated Agent to whom the secure cargo is going, and any Regulated Agent involved in the collection of the secure cargo.

The Known Consignor uses a Regulated Agent who sub-contracts a haulier

If a Regulated Agent sub-contracts a haulier who is not a listed Regulated Agent, then there needs to be a haulier agreement between the listed Regulated Agent and the haulier. The Regulated Agent must keep a copy of the original signed haulier declaration.

The Known Consignor is entitled to verify that the haulier declaration is in place. This can be achieved by requesting a copy from the Regulated Agent or checking a copy of the haulier declaration which should be carried by the driver.

Vehicle and Driver Checks

If a Known Consignor is using their own transport or a contracted haulier, they must ensure that the load compartments are securable, normally with the use of seals or by locking. Curtain sided vehicles must be secured with TIR cords. The load areas of flatbed vehicles must be kept under observation when air cargo is being transported. A flatbed vehicle should only be used where it is impossible to secure a load within the load compartment of a vehicle.

The condition of the vehicle on arrival at the Known Consignor site must be checked to ensure that if other secure cargo is being transported, that the load areas were appropriately secured or protected.

Numbered seals must be handled in the same manner as any other tamper evident materials (as described at Packing – page 19) i.e. kept securely; access restricted; stock and issue of seals accounted for.

To protect secure cargo from unauthorised interference or tampering, measures need to be in place to verify the identity of the driver/passengers of the vehicles collecting the air cargo/mail.

Two forms of photographic ID must be checked. Official photographic ID will confirm the identity of the driver. In addition, company issued photographic ID should be checked to confirm that they are an employee of the relevant company. Company issued ID will often also include the security training status of the driver.

Official photographic ID issued or recognised by the national authorities:

- Identity Card,
- Passport
- Driving licence
- Other official document, which includes their photograph.

It is recommended that to provide an audit trail of the security provisions applied to the transporting of secure cargo that a record is made of the registration number of the transporting vehicle; condition on arrival at site; driver's details; the two forms of identification checked; the seal number/ means used to secure the vehicle.

United Kingdom Supply Chain Security Database

Information about approved Known Consignor sites will be entered into the United Kingdom Supply Chain Security Database which is accessible by Regulated Agents, Known Consignors, and air carriers.

A Cargo Agent (Known Consignor or Regulated Agent) cannot be considered 'listed' until its details are published in the United Kingdom Supply Chain Security Database. The Department for Transport (DfT), as the Appropriate Authority for the United Kingdom, is required to update the database with the necessary details of approved Cargo Agents (Known Consignors and Regulated Agents). The CAA manages this database.

The database is updated daily. Consequently, the validity of any Cargo Agent (Known Consignor or Regulated Agent) must be checked on the day of collection. Each check conducted on the database is recorded. To access the database an authorised individual will be provided with personal log-in details. Log in details must only be used by the person authorised and must not be shared with any other person.

Although usage of the database is automatically logged, consideration should still be given as to what processes will be adopted at the site to ensure the database is checked on the date of despatch as required, e.g. this could include a screenshot of the validation check retained with the consignment documentation. It is imperative that the security operative responsible for handing over the secure cargo to the collecting cargo agent is aware of the result of the database check.

The United Kingdom database can be used to identify and confirm listed Regulated Agents to facilitate the transportation of SPX cargo. All Known Consignors will need a user account to access the database. Details will be provided by the CAA Known Consignor support team (KCsupport@caa.co.uk)

The Database is located at: [Home | Supply Chain Security](#)

Where Security Controls Have Not Been Applied

When, for whatever reason, any of the aforementioned security controls have not been applied to a consignment, or where the consignment has not been originated by the Known Consignor for its own account, the Known Consignor shall clearly identify this to the Regulated Agent so that the consignment can be adequately screened – if appropriate to do so.

When such cargo is transported to the Regulated Agent, the Known Consignor shall ensure that:

- these consignments are separated from consignments which it has originated.
- the origin is clearly indicated on the consignment or on accompanying documentation.
- no CSC is issued.

All such consignments must be screened before they are loaded onto an aircraft.

Alternatively, the consignment can be transported other than by air.

OFFICIAL

Staff Recruitment

The Known Consignor must ensure that all staff implementing security controls are recruited and trained in accordance with the regulatory requirements. This also applies to all staff with access to identifiable air cargo/mail to which the required security controls have been applied. Recruitment checks must be completed successfully before the person is trained or deployed, and there is a requirement that all recruitment and training records must be retained for the duration of the employee's contract.

When considering becoming a Known Consignor, the role of each staff member will need to be considered to confirm what – if any links – they have to the proposed Known Consignor process.

Broadly, there are two groups of personnel to consider:

- All staff implementing security controls must be background checked – including referencing – in accordance with the requirements of regulation before receiving the training appropriate to their role.
- All other staff with access to identifiable air cargo or identifiable air mail to which the required security controls have been applied must also be background checked and subject to security awareness training in accordance with regulatory requirements.

If this is not completed properly the security status of any consignment will be invalid so it is essential that a knowledge of roles and staff members is fully understood so that an accurate assessment can be made as to whether they need to be background checked and trained.

Regardless of whether any of the requirements above are delivered by in-house staff, a recruitment agency, or contractors, the responsibility for compliance with the regulation's rests with the Known Consignor.

A CAA auditor is authorised to examine recruitment records, and they must be produced when required. This applies to all staff involved in the Known Consignor process at the site – whether permanent, temporary or agency. Consequently, it is advantageous that these records are readily accessible in the event of an audit. Consideration must be given as to how these records would be made available without delay if they are normally held off site and / or by a third party such as a recruitment agency.

The audit will normally include an interview with the person responsible for the recruitment of staff together with an examination of a selection of staff recruitment and security training records.

OFFICIAL

To assist in the auditing of recruitment files, a list of Known Consignor staff should be maintained and made available to the auditor.

The list should include details such as:

- Name
- Start date with company.
- Start date in Known Consignor role.
- Criminal Record Certificate issue/expiry date
- Training delivery/expiry date

As a basic guide, the following documents should form part of the recruitment records held for a Known Consignor staff member. They must be made available in a presentable form that can be in hard copy or electronic format.

- Application form – signed and dated by the candidate.
- Relevant regulatory declarations – must form part of the job application process but could be separate from the application form.
- National Insurance number of candidate.
- Proof of identity.
- 5 Year employment/educational history, including evidence to cover gaps over 28 days.
- Written confirmation (e.g. references) from employers and educational establishments or HMRC data verifying the person's 5 years employment / education history.
- A Criminal Record Certificate (CRC) from all countries of residence of more than 6 months in the preceding 5 years
- Proof of interview to initially assess aptitude & abilities – normally interview notes.
- The name of the person who took the decision on the suitability of the person being recruited.

Repeat background checks guidance:

A background check is valid for 3 years.

When reviewing and renewing the standard background check for Known Consignor staff, a record of how this process has been undertaken must be recorded and held on the employee's file.

In practice this will only usually involve repeating the check of criminal records as the identity and work history will most likely be with the current employer. However, ongoing compliance with the other aspects of the check will also need to be demonstrable.

As recommended practice a file note or proforma to confirm that the person's identity has

OFFICIAL

not changed (or where it has that this has been validated e.g. in-date passport; through sight of a marriage certificate or deed poll for change of name, etc.) and to confirm that the person has remained in continuous employment for the period with no unexplained gaps of more than 28 days should be completed.

All recruitment and training records must be retained for the duration of the employee's employment.

The CAA document "CAP 2330: Aviation Recruitment Guide" describes the recruitment procedure in detail. These measures are required to be met by Known Consignors to comply with the regulatory requirements set out within Chapter 11 (Recruitment and Training) of the UK NASP.

Further details can be found at:

[Security | UK Civil Aviation Authority](#)

AvSecVetting@caa.co.uk

Staff Security Training

A Known Consignor must ensure that all relevant staff (permanent, temporary or agency staff, contractors, and drivers) have received the appropriate training in air cargo security. Relevant staff are those who perform a security function; have access to identifiable air cargo or have information about it. The minimum level of training is determined by the employee's job role/function. Initial and recurrent training must be delivered by a DfT Certificated Instructor in accordance with Chapter 11 of the UK NASP.

All staff with unescorted access to identifiable air cargo will need training in accordance with the approved Cargo and Mail (Known Consignor) training syllabus. Drivers must also be trained if they are to transport secure air cargo.

Individual training records must be kept on file for the duration of the employee's contract. This includes all historic training records.

A revised Cargo and Mail (Known Consignor) syllabus was published in 2022 to replace the 2014 syllabus. There is an expectation that all Known Consignor training is delivered in accordance with the revised 2022 syllabus.

There are 11 modules within the 2022 syllabus. Staff roles must be assessed to ascertain which modules need to be delivered. This should be conducted in consultation with the training provider using the Function Matrix so that appropriate modules are delivered and staff are neither under nor over trained.

Even if staff do not have unescorted access to secure air cargo, certain functions are considered as security functions and therefore relevant staff must be suitably background checked, and security trained e.g. staff who may prepare and/or sign off CSCs; management of access control systems or staff that validate the United Kingdom Supply Chain Security database.

Known Consignor staff should normally be trained only under the Cargo and Mail (Known Consignor) syllabus. However, in exceptional circumstances Known Consignors may be allowed to use training delivered from the Cargo and Mail (Regulated Agent) syllabus.

Where an individual has already successfully completed training under the Cargo and Mail (Regulated Agent) syllabus, this training may in some cases be accepted as equivalent to Cargo and Mail (Known Consignor) training. In these circumstances, the certificated instructor must be satisfied that the trainee has retained sufficient knowledge and competence from previous training before delivering the Cargo Agent (Known Consignor) specific content and

OFFICIAL

this must be noted on the training record.

If the trainee has insufficient knowledge or competence, appropriate additional training must be provided and, in some cases, full initial training in line with this syllabus may be the preferred option. For further details, contact the CAA for advice and approval before accepting or delivering Regulated Agent training for Known Consignor staff.

All these courses can be found in the CAA Aviation Security Training website at:

[Training and Human Factors | UK Civil Aviation Authority](#)

Courses must be delivered by a CAA accredited training provider using a CAA accredited Cargo and Mail (Known Consignor) trainer.

A list of training providers and trainers is available at:

[CAP1975: CAA-Registered Training Providers | UK Civil Aviation Authority](#)

List of all CAA-Registered Training Providers registered under the CAA Quality Assurance Framework, the registration number, and the Department for Transport (DfT) aviation security syllabuses they are registered to deliver.

[CAP1976: UK Aviation Security Instructors | UK Civil Aviation Authority](#)

List of DfT certificated UK aviation security instructors delivering training under the National Aviation Security Programme (NASP).

Some training providers offer public courses to which you can send employees. Alternatively, many trainers will deliver courses at your site. There is no fixed fee for training, so consignors may wish to contact several providers to compare quotes.

Further Information:

Further information about training for Known Consignors can be obtained from:

Avsec.training@caa.co.uk or
KCsupport@caa.co.uk

OFFICIAL

As a guide:

Cargo and Mail (Known Consignor) 2022 syllabus.

ACTIVITY	MODULES
Access to secure cargo	1-3
Airside pass requirement	1-3; 4
Escorting (airside)	1-3; 5
Drivers	1-3; 7
Implementing Security Controls	1-3; 6; 8; 9
Completing the CSC	1-3; 10
Responsible person/ SSR at site	1-3; (4;5 only if airside pass holder) 6-11

Feedback and Rectification

Feedback:

At the conclusion of the audit, the auditor will deliver concise and accurate verbal feedback to the SSR as to the findings. The auditor will provide an assessment of each heading area audited.

In line with the rest of the aviation sector, the potential assessment outcomes are:

- Fully Compliant
- Compliant Improvement Desirable
- Not Compliant
- Seriously Deficient
- Seriously Deficient with a Deficiency Notice

The verbal feedback delivered at the conclusion of the audit will be followed up with written electronic feedback which will be forwarded to the SSR via secure email (Egress). This will normally be done as soon as practicable after the audit. A copy will be retained by the CAA.

Rectification:

If any aspect(s) are assessed as being not compliant (not compliant through to seriously deficient with a deficiency notice), the auditor will precisely outline what the issues are and offer guidance as to how they can be rectified. A time frame to address the problem(s) or to submit a written plan as to how the issues will be addressed will be agreed. Normally this is within 10 working days.

It is important that the identified issues are treated seriously and efforts to rectify them are expedited. Validation or re-validation is dependent on a secure process without deficiencies. If regulatory requirements are not consistently met, then a site is subject to de-listing.

The responsibility to address identified shortcomings rests with the Known Consignor. Within the agreed timeframe, the Known Consignor must inform the auditor of how they have or intend to rectify the identified issue(s).

The auditor will decide if the rectification plan will suffice or if more mitigating actions are required. It is possible in appropriate circumstances to confirm rectification issues by email. Some cases may, however, necessitate a further on-site audit.

OFFICIAL

Post Audit

Following the site validation visit, the auditor will compile an electronic written report, which is securely retained on a CAA central recording system called CYGNUM. This system is used by CAA Aviation Security to demonstrate to the Appropriate Authority (DfT) that the United Kingdom is maintaining its mandated aviation security compliance activity.

Once completed - and any rectification points agreed with the Known Consignor - the auditor will inform the CAA Known Consignor support team that the site validation has taken place and the outcome.

A Known Consignor's site validation status is confirmed by the entity being included or remaining on the United Kingdom Supply Chain Security database.

Annex A

Useful Websites

[Disclosure and Barring Service - GOV.UK](#)

Disclosure and Barring Service

[AccessNI criminal record checks | nidirect](#)

AccessNI – Criminal Record Checks

[Disclosure levels - mygov.scot](#)

Disclosure Scotland, Basic CRB (Criminal Record Background)

[Home | MI5 - The Security Service](#)

MI5 Security advice, including documents on personnel security.

[National Protective Security Authority | NPSA](#)

Security advice, including physical, personnel and electronic security measures.
