

AIMSS[©]

(A Heathrow Initiative)

AIRFREIGHT INDUSTRY MINIMUM SECURITY STANDARDS FOR CARGO

In association with Operation Grafton



www.aimss.info

Warning: This document is not intended to negate the need to comply with any UK Legislation, Controls or Directions.

Foreword

The airfreight industry is a key component of the free world. The transportation, storage and handling of cargo are a vital element in the economy of the United Kingdom and as such airfreight carriers have great responsibilities. It is for these reasons that I welcome the introduction of the Airfreight Industry Minimum Security Standards - AIMSS.

It is unfortunate that we live in an age where security has to be a major feature for all businesses. The threat of terrorist attack is real and any improvements in security will frustrate the terrorists' opportunities to attack 'soft' targets. The airfreight industry has a major role to play in reducing the opportunity for organised crime and terrorists profiting from their criminal activities.

Concerns relating to the security of airfreight were raised by the industry itself and working in partnership with the Metropolitan Police Operation Grafton was conceived. Operation Grafton is primarily focused on high value airfreight crimes with a connection to Heathrow. It has three main operational components, intelligence gathering, crime prevention/ reduction and pro-active operations.

This document has been developed as direct result of the cooperation between law enforcement agencies, airlines, road transport industry and the airfreight industry brought together in partnership with Operation Grafton. Members of the crime prevention group, consisting of representatives from AOCC, TAPA, British Airways, Customs and Excise, Metropolitan Police, Surrey Police, Thames Valley Police, BAA, BIFA and the Road Haulage Association, have been key contributors to the workings of this document.

Working in partnership to reduce crime is not an easy task. This document shows what can be achieved with a concerted effort and how diverse agencies and companies can work together towards a common goal. I thank everyone involved in the preparation of AIMSS.

The advice contained in this document will ensure that companies that adopt the minimum standards can be certain that they are assisting the security and law enforcement agencies to prevent and detect serious crime whilst providing a more secure service to their customers.

The inclusion of a self-audit will enable you to review your existing security policies and infrastructure to identify areas of strengths and weaknesses. This audit will also ensure that you identify areas that need to be improved in order to meet the standards before receiving the accreditation survey from the local police crime prevention officer.

This document shows how, with the minimum of financial investment, and good management, cargo security can be improved. The use of best practice will enhance the industry's ability to satisfy customer demands. I wish you well in meeting these minimum standards.

Tarique Ghaffur CBE, QPM
Assistant Commissioner - Specialist Crime Directorate
Metropolitan Police

Acknowledgements

This document would not have been possible without the active contribution and participation of the following agencies and organisations. Thanks is given to TAPA for permission to adapt and use, for AIMSS accreditation purposes, standards developed by the Association.

- Airline Operators Committee (Cargo)
- BAA plc
- British Airways
- British International Freight Association
- HM Customs and Excise
- Metropolitan Police
- Road Haulage Association
- Technology Asset Protection Association

Group Membership

- | | |
|-----------------------|---|
| • Fiona Nivan (Chair) | Metropolitan Police |
| • Mick Tricker | Metropolitan Police |
| • Ian Jenkins | BAA plc |
| • Jason Breakwell | Technology Asset Protection Association |
| • Terry Burton | British Airways |
| • David Corrigan | HM Customs and Excise |
| • Dave Archer | Technology Asset Protection Association |
| • Ian Nightingale | Metropolitan Police |
| • John O'Connell | British International Freight Association |
| • Chrys Rampley | Road Haulage Association |
| • Andrew Roe | Airline Operators Committee (Cargo) |

Contents

Foreword	1
Acknowledgments	2
Introduction	4
<u>Part 1 - Warehouse Security</u>	5
1. Access Control and Staff Identification	5
2. Security of Premises	5
3. Vulnerable Freight	6
4. Collection of Freight	6
5. Training	7
6. Auditing	7
<u>Part 2 - Ground Transport Security</u>	7
9. Driver Requirements	7
10. Vehicle Requirements	8
11. Journey Security	8
<u>Part 3 - Security of Information</u>	9
12. Need to Know Principle	9
13. General Issues	9
14. Pre Alert Messages for Val / Vun	9
15. Collection / Delivery of Cargo to / from Aircraft	9
<u>Part 4 - Vetting of Personnel</u>	10
16. Application Form	10
17. The Interview	11
18. Post Interview	11
<u>Appendices</u>	
Appendix A	13
Staff Employment Application Form	
Appendix B	22
AIMSS Accreditation - Self-Assessment Template	
Appendix C	36
The Secure Transportation of Valuable and Vulnerable Cargo on Airport	
Appendix D	40
Glossary Of Terms	

Introduction

The transportation of high value and vulnerable cargo requires an understanding of the associated risks and the measures that can be taken to reduce those risks. Good security does not necessarily mean vast capital expenditure. Good management procedures and policies can go a long way to reducing your risk.

This document provides a starting point for the security operations of those carriers involved in the transportation of air cargo. The document provides a number of minimum standards intended to reduce the risk of crime and terrorist attack.

The self-assessment template provides a checklist to see which areas you may need to develop or refine. Once completed the self-assessment template can be passed to your local police crime prevention officer. The crime prevention officer will conduct an "Airfreight Industry Minimum Security Standards" cargo survey (AIMSS Survey). If this survey is satisfactory you will receive the AIMSS security seal that can be used on your letterheads etc. AIMSS accreditation will last for a period of two years from the date of validation and the period will be shown on the Certificate of Accreditation. Take advantage of this free service.

The document has been produced in partnership with professional organisations and companies involved in the transportation, regulation and security of air cargo. The minimum standards contained within this document have been derived from existing good practice, specialist knowledge and general crime prevention principles.

These are minimum standards that can be developed and enhanced to meet the specific needs of your customers. The professional haulage organisations and police are able to provide additional information if required.

It is our hope that this document will be used to raise the level of security across the industry and be the catalyst for future developments in the valuable and or vulnerable air cargo industry. AIMSS will itself be reviewed in the light of such developments.

Part 1 - Warehouse Security

1.0 Access Control and Staff Identification

- 1.1 The warehouse must be a restricted area for authorised persons employed by that company. The warehouse should be secured against public access.
- 1.2 All authorised persons must be in possession of a photo identification card that should be clearly displayed at all times.
- 1.3 Any person, other than an authorised person, entering the warehouse, must be signed into a visitors register and given a numbered and dated visitors pass which must be clearly displayed at all times.

The visitor's register must record the name of the visitor, their company, date and time of entering and leaving the warehouse, the purpose of the visit, who they are visiting, details of their vehicle and details of the person recording the information in the register.

- 1.4 An authorised person should accompany the visitor at all times throughout the visit to the warehouse.
- 1.5 Any person found in the warehouse without authority should immediately be challenged and his or her details recorded in writing with their explanation for their presence in the warehouse. If a satisfactory explanation cannot be established, police should be called.

2.0 Security of Premises

- 2.1 The doors giving access to the warehouse should remain closed and secured at all times unless freight is being moved in or out of the warehouse. All loading and unloading areas, entrances and exits to the building should be appropriately illuminated and covered by CCTV.
- 2.2 The warehouse must be fully secured at all times using appropriate security devices commensurate with the risk to the area to be secured. Wherever necessary an audible intruder alarm system should be installed.
- 2.3 Information relating to all consignments must be restricted to persons who are involved in the movement of the actual shipments.¹ All paperwork and data must be protected at all times.
- 2.4 Basic security procedures should be in place and must include protocols for searching staff, visitors and vehicles at the facility. In addition security sweeps of the premises should be conducted on a regular basis.

¹ A fundamental security principle is that the knowledge or possession of sensitive information must be strictly limited to those who clearly have a need to know it in order to do their jobs effectively.

3.0 Vulnerable Freight²

- 3.1 All vulnerable freight should, wherever possible, be located in a locked cage. If this is not possible it should be located in an area from which it is difficult to remove. These areas could include locked containers within the warehouse or high-level shelving. Where practicable, it should be highly visible at all times and covered by CCTV.

A vulnerable freight cargo register should be maintained. This register should contain the following information: date of arrival, air waybill number, number of pieces, commodity, location in the warehouse, signature and printed name of the person locating the freight, date of collection, signature and printed name of the person releasing the freight. Access to the register should be controlled.

- 3.2 Daily bond checks should take place in respect of all shipments. In respect of vulnerable shipments this should take place on the change over of each shift. If the warehouse is not a 24-hour operation then the bond check should take place at the conclusion of the shift and at the commencement of the shift the following day.

4.0 Collection Of Freight

- 4.1 The Standard Conditions for the collection of Freight, agreed by the AOCC (Airline Operators Committee Cargo) and BIFA (British International Freight Association), should be applied where appropriate.³
- 4.2 Random checks should be conducted in respect of companies collecting freight, particularly vulnerable freight. This includes checking with the consignee to confirm that the person collecting freight on their behalf is a genuine agent with the necessary authority to collect the consignment.
- 4.3 A photocopy of the driver's identification and photograph should be taken for all collections, together with the index number of the vehicle collecting the consignment. The index number must be checked against the paperwork by the warehouse staff. These details should be attached to the file in respect of that consignment and retained for a period of not less than 12 months.
- 4.4 The person collecting the freight should be required to provide a thumbprint when collecting any goods. This should be retained by the handling agent in accordance with data protection and any other relevant legislation⁴.

If there is any doubt relating to the collecting agent, the freight should not be released.

² Vulnerable freight includes computers and component parts, mobile telephones, perfumes, cigarettes, wines and spirits etc.

³ The agreed 'Standard Conditions for the Collection of Freight' can be found at www.aimss.info

⁴ For information relating to 'Thumbprint Schemes' contact your local police Crime Prevention Officer, BIFA or the secretary of the AOCC at Heathrow Airport.

5.0 Training

- 5.1 All companies should put into place clear written handling procedures. This document should enable employees to gain a comprehensive understanding of the policy and procedures they are expected to follow. The procedures document should be readily available for staff to consult at any time. Any amendments to the manual must be relayed to staff in writing immediately.
- 5.2 All warehouse staff should be trained in basic security including level 4-security training, robbery response, safety training and bomb threats. A written record should be kept of each employee outlining the training they have completed and any retraining or outstanding training they need to complete.

6.0 Auditing

- 6.1 The company's management should carry out regular audits to ensure that these procedures are being fully complied with. Any non-conformances should be addressed immediately and the appropriate action taken, if necessary, including discipline against staff failing to comply with the requirements.

Part 2 - Ground Transport

7.0 Driver Requirements

- 7.1 All staff involved in the conveyance of valuable and or vulnerable cargo should have met the vetting conditions contained in this document.
- 7.2 All drivers must be qualified to the appropriate level for the vehicle they are to drive. All drivers should be in possession of the new style photo-card driving licence. This should be checked at six monthly intervals.
- 7.3 The company should retain a photocopy of the driver's licence and photo-card as this information can be used to verify details of the driver with the representative of the airline, handling agent or the transport company.
- 7.4 In addition to the drivers company ID card the driver should carry his photo-card driving licence as additional identity.
- 7.5 Drivers are responsible for the daily inspection of the vehicle they are going to use that day. The company should provide a checklist for drivers to ensure that their vehicle is fit for the journey.
- 7.6 Drivers must not give lifts to any unauthorised persons.
- 7.7 Drivers should be fully conversant with the company's security policies and procedures.

8.0 Vehicle Requirements

- 8.1 All vehicles used for the carriage of cargo must be well maintained and of the appropriate type for the cargo conveyed.
- 8.2 The vehicle must be fitted with security devices relevant to the load to be carried. The driver must be aware of the security devices and how to operate them.

9.0 Journey Security

- 9.1 The driver must be present during the loading/ unloading operations to ensure the integrity of the shipment and agree the piece count (where appropriate).
- 9.2 There must be documentary records of shipping details (time, date, driver, shipping/ receiving personnel, shipment details and quantity). Information relating to high value/ vulnerable loads must be strictly limited to those who need to know it in order to do their job.
- 9.3 When in transit with high value/ vulnerable cargo all doors and windows should be secured at all times.
- 9.4 In the event of the vehicle being involved in an accident or incident that immobilises it or requires the driver to remain at the scene, the driver should contact police. Details including name and shoulder number of any attending officer/s should be obtained. Police should be informed of the nature of the load being carried. **Under no circumstances should the doors or windows be opened in an insecure location.**
- 9.5 In the event of the vehicle being required to stop for police the driver is to remain in the vehicle with the doors and windows secured. The driver should contact police control by telephone to confirm credentials of stopping officer/s and inform the control room of the nature of the load being carried. **Under no circumstances should the doors or windows be opened in an insecure location.**
- 9.6 Regular contact should be kept with the driver to identify/ confirm route, stops and ETA.
- 9.7 Wherever possible a relief driver should accompany the primary driver. This will allow one person to remain with the vehicle at all times.
- 9.8 All drivers should be provided with a form of mobile communication.
- 9.9 If a tracking device is fitted to a vehicle it should, wherever possible, be monitored.
- 9.10 All drivers should be directed to park their vehicles in a secure area overnight.
- 9.11 Vehicle keys need to be secured at all times. When the vehicle is away from its base the keys must be kept with the driver at all times.

Part 3 - Security Of Information

10.0 The need to know principle

- 10.1 A fundamental security principle is that the knowledge or possession of sensitive information or material must be strictly limited to those who need to know it in order to do their jobs effectively. No one is entitled to access sensitive information solely on the basis of position or appointment. The greater the sensitivity of the information the more important the principle becomes.

11.0 General Issues

- 11.1 Data protection policies must be in place to cover the retention of information that can identify a living individual (this includes CCTV coverage). All policies must comply with the guidelines provided by the Data Protection Commissioner.
- 11.2 All counter areas where documents are exchanged should be monitored by CCTV.
- 11.3 Collection of VAL/VUN air waybills must be auditable.
- 11.4 SITA/ EMAIL delivery addresses should be regularly reviewed to reduce availability of information.
- 11.5 Passing of mandatory information between host and control authority should be carried out electronically in a secure manner.
- 11.6 The use of company computer systems must be auditable and user sensitive. A password protection system should also be incorporated. All employee passwords must be changed at least quarterly.
- 11.7 All courier collections of documents to be undertaken by registered companies employing approved and listed staff all of whom must be issued with photographic ID's.

12.0 Pre-Alert Messages for VUN/ VAL

- 12.1 Duty Managers or nominated staff should be designated to receive/ or transmit VUN/ VAL messaging. Secure equipment should be used to receive/ send such transmissions.
- 12.2 SITA/ EMAIL codes for receipt or transmission of these messages throughout the company's network should be regularly reviewed.

13.0 Collection/ Delivery of Cargo Documents to/ from Aircraft

- 13.1 Document pouches for VAL/ VUN cargo must be securely conveyed to/ from aircraft carried in a sealed tamper evident pouch. Loose documents from VAL/ VUN should not be transported under any circumstances.
- 13.2 Documents for VAL/ VUN should be handled by staff designated responsible for VAL/ VUN cargo.

Part 4 - Vetting And Recruitment

14.0 Application Form

- 14.1 All application forms should contain all the questions and all the declarations set in Appendix A.
- 14.2 'Guidance for Completion Notes' should be provided with each application form.
- 14.3 Application forms should only be sent to the applicant's home address.
- 14.4 All application forms should be fully completed by the applicant.
- 14.5 All questions should be answered as fully as possible.
- 14.6 Application forms should be legible and where there is ambiguity clarification should be sought.
- 14.7 The application should be marked "STAFF IN CONFIDENCE" and treated accordingly.
- 14.8 Where original documents must be produced at interview, a requirement should be made for inclusion of photocopies of these documents with the application form. This could include driving licence, educational qualifications and proof of home address as appropriate. At this stage there should be no requirement for other photographic ID.
- 14.9 Applicants must be informed of the use of the application form and supporting documents in relation to checks made with previous employers, referees etc and at what stage in the application process these checks will be made.
- 14.10 Consideration should be given to maintaining a database of applicants and relevant information to allow the identification of repeat applicants and referees who support more applications than would be deemed normal.⁵
- 14.11 Where a 'paper sift' takes place documents should either be returned to unsuccessful applicants or destroyed as confidential waste.
- 14.12 All declarations on the application form should be signed and dated and, where appropriate, witnessed.
- 14.13 Application forms should be carefully checked and a record of the staff member who checked each item should be maintained on the application form for audit purposes.
- 14.14 Candidates selected for interview should be contacted in good time to allow them to gather any original documents identified in the application form.
- 14.15 The application forms should be made available to the staff interviewing candidates.

⁵ There may be data protection issues in relation to this item.

15.0 The Interview

- 15.1 Prior to the interview the application form should be read and any areas where clarification is needed should be identified and highlighted.
- 15.2 A generic interview plan should be prepared to ensure that all applicants receive equal treatment. However, specific incidents or areas of concern need to be addressed on an individual basis.
- 15.3 Detailed notes should be taken during the interview especially relating to identified areas of concern. These notes should then be attached to the application form and kept as a matter of record.
- 15.4 All notes of the interview should include: date and time that the interview commenced, persons present, time the interview concluded and the result of the interview (i.e. position offered / candidate not suitable etc.).
- 15.5 The interviewer/s should use open questions rather than closed questions i.e. "Where did you work between March 2000 and September 2002?" ... "Why did you leave?" as opposed to "Did you work at ACME Cargo between March 2000 and September 2002?" ... "You left to join the ACME trading co?". This allows comparison with the answers given on the application form.
- 15.6 The candidate should be encouraged to expand on answers given on the application form.
- 15.7 Applicants should be given the opportunity to clarify periods of unemployment or details of periods of employment with now bankrupt companies or companies in liquidation.
- 15.8 Where an applicant is reluctant to elucidate matters this may be an area for concern and should be reflected in the interview notes.

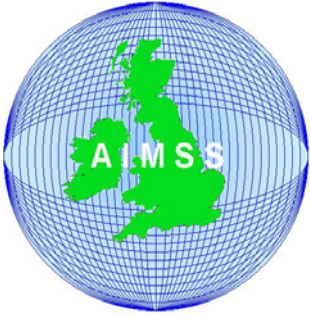
16.0 Post Interview / Job Offer

- 16.1 Details of the candidate's performance during the interview should be available for internal applicants. Feed back sessions should be arranged with unsuccessful internal candidates to allow them to improve their chances next time round.
- 16.2 Unsuccessful candidates should be notified as soon as possible.
- 16.3 Successful candidates should be informed that they have been successful **subject** to referee and security checks as appropriate. In addition the applicant must be informed that referees and other references will be contacted and checked.
- 16.4 Checks should be conducted on all the referees and previous employers. A letter should be sent to the named person at the registered business address given.
- 16.5 Where there is no response to the written request for details, a phone call should be made to establish the authenticity of the company and the references. Checks should be made to ensure that the telephone number relates to the business. If a direct line number to a specific individual is given on the application, consideration should be given to

contacting the business via the main switchboard and asking for the named person.

- 16.6 Consideration should be given to speaking with company HR departments to establish periods of employment. Companies may be reluctant to give details other than the company did or did not employ the person.
- 16.7 All documentation to support the application must be checked. This includes Police Subject Access Report, Criminal Records Bureau Reports, Driving Licence, Passport, National Identity Card, Birth Certificate. All documents checked must be originals or duly certified copies. Photocopies are unacceptable.
- 16.8 The application form should be noted with each action and the result of each enquiry by the person carrying out the action or making the enquiry.

**AIMSS Application for Employment
(Suggested Format)**



(Your Company Name)
Application for Employment



STAFF IN CONFIDENCE

Name:

.....

Position applied for:

.....

Notes for Guidance

Thank you for considering employment with our company. You will appreciate that we take every care when employing new staff. This application form will assist us to progress your application as quickly as possible. All potential employees must complete the form and, where appropriate, CV's should accompany a completed application form.

It is important that you read these notes before completing the application form.

If you are successful, the information that you provide in the application form will be a component part of your conditions of service. Any changes to the information provided on the application form must be notified to the company immediately. If you answer any questions untruthfully or omit any relevant information you may be liable to dismissal and / or criminal proceedings.

Please answer all questions clearly and ensure that your writing is legible.

Where there is insufficient space on the application form please continue on a separate piece of paper.

This form comprises of a number of sections including personal, security and health sections. Some of the information on this form will be used for security clearances where appropriate and may be shared with other security agencies for the purposes of crime reduction measures and counter terrorism matters.

Agreement

I have read the above and understand that my personal details may be shared with security agencies / law enforcement agencies and the police, as the company deems appropriate for the above purposes. I agree that my details may be shared with the agencies identified.

Signed

Date

Print Name

Personal Details

No.			Office use only
1	Surname		
2	Maiden Name		
3	Forenames		
4	Other names used		
5	Have you ever used another name?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
6	If you answered yes to question 5 please provide full details.		
7	Title		
8	Date Of Birth		
9	Address		
10	Postcode		

11	Time at present address		
12	If less than five years at your present address please give full details of all your previous addresses in the past five years		
13	Home Telephone Number		
14	Business Telephone Number		
15	Mobile Telephone Number		
16	Email Address		
17	Nationality		
18	Citizenship		
19	National Insurance Number		
20	Where did you hear about this position?		
21	Do you have friends or relatives working in this company?		

Criminal Convictions / Impending Prosecution Information

22	<p>Have you ever been convicted of a criminal offence? (Including motoring offences, but excluding parking fines).</p> <p><i>Convictions must be declared subject to the Rehabilitation of Offenders Act 1974.</i></p>	Yes <input type="checkbox"/> No <input type="checkbox"/>	
23	If you answered Yes to question 22 please give full details. Continue on a separate sheet of paper if necessary.		
24	Do you have any court proceedings pending or are you awaiting sentencing by a criminal court.	Yes <input type="checkbox"/> No <input type="checkbox"/>	
25	If you answered Yes to question 24 please give full details. Continue on a separate sheet of paper if necessary.		
26	Have you ever received a formal police caution?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
27	If you answered Yes to question 26 please give full details. Continue on a separate sheet of paper if necessary.		

I confirm that the answers above are true and that I have no unspent criminal conviction/s for theft, fraud, conspiracy OR any other offence which could adversely impact on the business of [COMPANY NAME] (except those declared above) and my fitness to carry out my responsibilities within that business. I understand that if I have answered any of the above questions untruthfully or have omitted any relevant information I may be liable to dismissal and/ or criminal proceedings.

Signed

Date

Print Name

Employment History

Please provide details of employment history for the past 5 years. Gaps in employment history must be fully listed and explained. *(Note: Some posts may require details of employment history for extended periods.)*

No contact will be made with previous employers prior to an offer of a position.

Continue on a separate sheet if necessary.

Date	Company/ School Name and Address & Telephone	Position held and brief job description	Office use only

Referees/ References

Please provide the details of two independent referees. These referees must be in a recognised profession (e.g. doctor, solicitor, police officer, company director, teacher, minister). These referees must NOT be members of your family. The referee should have known you for a minimum of two years.

Referee 1

Title

Name

Address (including postcode)

Day Time Telephone

Relationship

Length of time known

Referee 2

Title

Name

Address (including postcode)

Day Time Telephone

Relationship

Length of time known

Documentation

The position that you are applying for requires that security checks be conducted to comply with company policy and, for certain positions, government legislation. Please ensure that you enclose photocopies of the following documents with your application form. **If you are invited for interview you will need to bring the original documents.**

Document	Enclosed	Office Use Only	
Driving Licence	Yes / No		
Passport	Yes / No		
Identity Card	Yes / No		
Work Permit (if applicable)	Yes / No		
Criminal Record Check	Yes / No		
Birth Certificate	Yes / No		
Other (as required)	Yes / No		

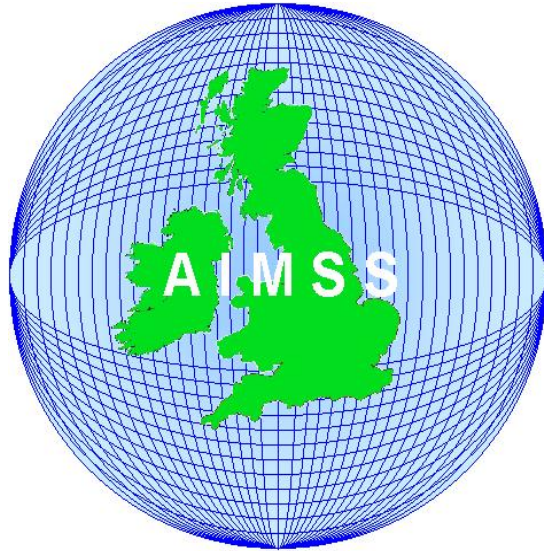
I confirm that the answers given in this application are true and to the best of my knowledge correct. I understand that giving a false declaration will lead to my summary dismissal. I also understand that if I receive a criminal conviction after the date of commencement of employment/ acceptance of this contract I must declare it immediately to the HR department, which will decide how the matter should be treated. Any failure to make any such declaration will constitute a breach of contract and may lead to dismissal or criminal proceedings.

Signed

Date

Print Name

**AIMSS Accreditation
Self-Assessment Template**



AIMSS Accreditation

Notes for Persons Applying for Accreditation

Notes for Persons Applying for Accreditation

Introduction

Welcome to the Airfreight Industry Minimum Security Standards (AIMSS) accreditation guidance. This document is intended to assist those involved in the self-assessment survey of establishments involved in the airfreight industry.

Recent high profile criminal activity in and around cargo handling and transportation has highlighted a need to improve security and to this end, the police and members of the industry have identified AIMSS as the way forward.

AIMSS accreditation will last for a period of two years from the date of validation and the period will be shown on the Certificate of Accreditation. (Where a company fails to meet the AIMSS standards required by its accreditation, the Principal Accreditation Officer may suspend or withdraw the accreditation. The appeals procedure will apply to case of accreditation withdrawal).

Please complete the self-assessment form as fully as possible. This document should be available to the Crime Prevention Officer (CPO) conducting the survey for accreditation.

Please contact your local police station to make an appointment with the CPO for the accreditation survey. Should you have any difficulties please check the AIMSS website (www.aimss.info) for contact numbers.

The Self-Assessment Template

The AIMSS document provides a set of recommendations for industry to improve security measures in relation to their operations. The document is divided into four parts:-

- Warehouse Security
- Transportation of Valuable and Vulnerable Cargo
- Ground Transport Security
- Security of Information

As can be seen from the headings the survey that needs to be conducted will examine processes as well as the physical security measures in place. To assist you a self-assessment template has been created. The template is intended to serve two purposes. Firstly, to provide a guide for the operator to see if he meets the criteria for AIMSS Accreditation and secondly, to provide the crime prevention officer with a starting point for an accreditation survey.

Within the self-assessment document there are two components, mandatory fields and supplementary fields. The mandatory fields are marked with an 'M'. As you would expect the mandatory components are absolutes. Only sites and areas of operation that have all the mandatory fields will be eligible for accreditation. If you do not meet all the mandatory fields it is important that you contact your CPO in order to address the deficiencies in the mandatory fields. Alternatively, additional information is available on the AIMSS web site.

The supplementary fields are areas where the crime prevention officer will offer advice and make a decision based on the surrounding circumstances.

If you have any queries or need further information or advice please see the AIMSS web site at www.aimss.info .

AIMSS ACCREDITATION

Self-Assessment Survey

Name of Company Surveyed:

Address of Premises Surveyed:

Details of Person Responsible for AIMSS Enquires:

Contact Details:

Person Conducting Survey:

Contact Details:

AIMSS ACCREDITATION

Self-Assessment Survey

Fields marked with an **M** are mandatory fields and must be complied with in order to receive AIMSS Accreditation. Fields not marked with an **M** are highly recommended. If in any doubt, please refer to your local police crime prevention adviser for advice.

<u>Sections</u>	<u>Page</u>
Warehouse Security	28
Access Control and Staff Identification	28
Security of Premises	28
Collection Of Freight	30
Training	31
Auditing	31
Ground Transportation	32
Driver Requirements	32
Vehicle Requirements	32
Journey Security	32
Security of information	33
General Issues	33
Pre-Alert Messages	33
Vetting and Recruitment	34
(See also Appendix 'A')	
AIMSS Accreditation	
Suspension/ Withdrawal of Accreditation.	34
Appeals Process	35

Warehouse Security

Access Control and Staff Identification

Ref No.	Accreditation Criteria		Pass	(Notes)
1.1(a)	Access control processes both during and outside normal operating hours to ensure access is granted only for authorised supplier, employees and visitors.	M		Use of staff ID cards and visitor passes will enable unauthorised persons to be identified quickly. Passes should only be issued to persons on production of a valid form of identification.
1.1(b)	Security controlled access points (e.g. numeric keypad locks, guard, receptionist, card access system or intercom with CCTV).	M		Details of visitors entering the facility should be recorded. Only staff and persons who have a valid visitors pass should be allowed access to restricted areas. It is important to bear in mind that if a wall does not reach the ceiling, a door lock system provides little security. CCTV covering the area will allow remote monitoring of an access point and record details of all activity in that area.
1.1(c)	Where a card access system is used, a minimum 30 days record of use should be retained.	M		The company needs to keep a list of authorised users and access to the equipment needs to be restricted to those listed. Staff who are required to access the card access system functions need to be trained to an appropriate level. There must be restricted access to card access system functions and a quarterly review of card access reports. Attention needs to be paid to staff entering on days off or out of working hours etc.
1.3(a)	ID Badge policy for visitors/ contractors in place.	M		All visitors must be issued with an ID badge and wear it at all times whilst in the establishment.
1.3(b)	Employee ID picture badges (showing an expiry date) must be issued, carried and ready for inspection at all times whilst on company premises.	M		Local instructions need to be in place to ensure that badges are carried. Ideally, signs informing staff of the need to carry badges and to challenge any person not known to them should be displayed in the warehouse area.
1.4(a)	Unaccompanied admittance to cargo handling and storage areas should be restricted to authorised staff only.	M		Any visitors to the site need to be escorted and should not be allowed access to vulnerable areas.

Security of Premises

2.1(a)	All external dock/ warehouse doors must be kept shut unless required for operational purposes. Access must be controlled through open doors.	M		A workforce instruction needs to be in place to ensure compliance with this component.
2.1(b)	All external doors should be covered by CCTV.	M		Cameras should be placed in areas where they can not be obstructed by high sided vehicles/ vegetation etc.

3.1(a)	CCTV coverage of break/ build, storage and loading/ unloading areas.	M		There may be an area or areas set aside for these functions. The use of TPZ cameras for this operation is acceptable providing the operation is monitored and recorded.
2.1(c)	External and internal lighting levels must support high quality CCTV images and recording.	M		Lighting is an important addition to CCTV. Flood lighting is not always the most appropriate form of illumination. Consideration needs to be given to ensuring that any lighting does not adversely affect the CCTV system.
2.1(d)	Dock doors illuminated externally at night.	M		See above.
2.1(e)	CCTV system must be able to view sides of the facility.			If the sides of your property contain doors or windows they are vulnerable. Consideration should be given to this component.
11.1(a)	CCTV must be in good working order and fit for the purpose for which it is installed. See CCTV Data Protection Guidance at www.aimss.info .	M		Regular maintenance of CCTV and alarm systems can prevent expensive repairs/ replacement at a later date.
11.1(b)	All CCTV images are recorded in real time, no more than 16 cameras to 1 tape/ disk and if VCR, no more than 12 hours of images on one tape.	M		See CCTV Data Protection Guidance at www.aimss.info .
11.1(c)	Quarterly preventative maintenance plan in place for CCTV systems (can be contracted or in house).	M		Regular maintenance of CCTV and alarm systems can prevent expensive repairs/ replacement at a later date.
2.2(a)	All external doors must be alarmed, and linked to a main alarm system, in premises that do not operate 24 x 7.	M		It is important that the alarm system can be zoned or individually isolated. This allows closed/ locked doors to remain alarmed when other doors are open.
2.2(b)	Restricted access to any installed alarm systems.	M		Only authorised staff should have access to alarm systems and records. Each key holder should have his or her own alarm access code.
2.2(c)	Remote monitoring of any installed alarms to police or security contractor.	M		Alarms including panic alarms should be connected to a central service provider system in addition to any local activation protocols. Additional connection via a G.S.M. system is highly recommended.
2.2(d)	All <i>security system</i> alarms dealt with in real time.	M		
2.2(e)	Motion detection intruder alarms fitted inside warehouse and activated when employees vacate facility.			This facility is particularly important in vault type areas. This must be considered in conjunction with the external door and window alarms.
2.2(f)	Manned security-monitoring post 24 x 7. Secured from attack.			If the premises are a 24-hour operation this facility should be on site.
2.2(g)	Any windows or other openings in warehouse walls must be secured by steel bar/ mesh (or any other appropriate security material or product).	M		Any protection for windows needs to be well maintained and appropriate to the risk in that particular area.

2.2(h)	Ground floor warehouse windows protected by anti-ram posts or other physical barrier.			Where windows are vulnerable to ram raid type attacks this measure is appropriate. However, if windows are situated in areas where this is unlikely i.e. positioned high in the wall or where a vehicle cannot gain access this is not a requirement.
2.2(i)	Dock doors must be of sufficient design to prevent or delay forced entry by use of portable hand tools or ramming by vehicle.			Many dock doors are of the roller door type. Reaching this level of security may be difficult. However, anti-ram posts/ ramps must be considered for the any areas where a vehicle can gain access.
2.2(j)	Reinforced exit doors from warehouse (steel doors and frames or suitable alternative).			As above
2.2(k)	Exterior walls to be designed to resist penetration by removing building fabric, cutting or ramming by vehicle.			Any redesign or new build should meet these criteria. Any strong rooms or secure areas should meet this standard.
2.2(l)	Restricted access vault area for assets on site more than 2 hours. (High-grade security mesh/ wall, alarmed, CCTV).			This is an ideal solution and should be considered, if not already in place. However, measures such as high rack storage under, CCTV, are acceptable.
2.2(m)	Caged area for assets on site more than six hours (chain link cage with roof or similar: padlocked, CCTV, coverage).			As above.
2.4(a)	Procedures for random inspection to control rubbish removal from premises must be in place.	M		Regular removal of rubbish is important. Security or managerial staff should accompany persons engaged in this job on an infrequent basis to reduce the risk of goods being left in the rubbish for later collection.
2.4(b)	Company procedures must incorporate a protocol for searches being carried out on persons and vehicles exiting cargo handling and storage areas.	M		Searches should be conducted on a frequent but irregular basis. Details of anything found should be recorded. Paperwork or photocopies may be as important as actual goods.
2.4(c)	Containers such as coolers, lunch boxes and personal bags should not be allowed in the warehouse. All personal containers must be subject to search when being removed from the premises.			Wherever possible the staff recreation/ locker rooms should be separate from the main warehouse. Employees should pass through a security check area before entering or leaving the premises. Further assistance may be sought from police. Contact local CPO for advice.

Collection Of Freight

4.1(a)	A written procedure must be in place regarding the collection / delivery of cargo. A voluntary thumbprint scheme should be in place for drivers collecting cargo.	M		All drivers delivering or collecting cargo should be checked for appropriate driver identification/ authorization at reception and a record of their vehicle registration kept. At the point of service warehouse staff should confirm driver and vehicle details.
--------	---	---	--	--

Training

5.1(a)	A consignor's Security Policy Statement must be available and communicated to all employees.	M		This document should be readily available and highlighted during training etc.
5.2(a)	Robbery response safety training for all dock, warehouse, Security and reception employees.	M		A document detailing procedures needs to be readily available.
5.1(b)	Procedures in place to routinely test and service security systems.	M		Regular maintenance of security equipment and systems can prevent expensive repairs/ replacement at a later date.
5.1(c)	Security incident reporting system and method of tracking local security incidents.	M		This document may become evidence in any police investigation. Full details should be included in any report. Management should be informed of any emerging trends or significant incidents immediately.
5.1(d)	A database of emergency contact numbers detailing local management and customers should be readily available for supervisors and managers.	M		Wherever possible this should be available on a computer and password protected.

Auditing

6.1(a)	Locally documented procedures for handling cargo must be in place - including auditable damage and irregularity reports and a procedure for communicating security incidents to consignee (or consignee's agent).	M		In addition all staff should be aware of the procedures and a copy should be available for inspection by supervisors and the buyer.
6.1(b)	A minimum of 30 days records must be kept in relation to system alarms.	M		The need to keep records will assist in post event evidence gathering and assist in the development of a more robust system. (e.g. where there have been a number of false alarms more appropriate solutions can be identified. Also faults can be identified and rectified quickly.)
6.1(c)	Auditable process for timely reporting of incidents of lost or missing cargo must be in place. Incidents of missing cargo to be reported by the handler to the consignee (or consignee's agent) as soon as practicable.	M		This document may become evidence in any police investigation. Full details should be included in any report.
6.1(d)	Access to all keys must be controlled and auditable.	M		There should be a booking in and out system for the use of all keys. This provides an audit and accountability trail. All staff should be aware of the company key policy.

Ground Transportation

Driver Requirements

Ref No.	Accreditation Criteria		Pass	(Notes)
7.7(a)	Drivers should be fully conversant with the company's security policies and procedures.	M		The company's security policies must reflect the minimum standards identified in the AIMSS document in relation to ground transport.

Vehicle Requirements

8.1(a)	Solid top, hard sided, locked cargo doors, or reinforced soft-sided trailer should be used for the transportation of vulnerable goods. (See Section 8 of AIMSS document for a definition of vulnerable).	M		It is important that the appropriate vehicle is used for the goods to be transported. If the handler has concerns in relation to the vehicle being used he should contact the shipper to ensure that they are happy with the transport being used.
8.2(a)	All vehicles must be fitted with a functional immobilization device.	M		Drivers should be aware of how all security devices are activated and deactivated. Instructions should be available to all drivers.

Journey Security

8.2(b)	Vehicles and trailers must be sealed using appropriate tamper evident seals.	M		Auditable procedures must be in place for the secure storage, issue and recording of seals. Seal numbers must appear on the appropriate shipping documentation.
9.8(a)	There must be a two-way voice communications system between the driver and his base. An information reporting protocol must also be in place.	M		Drivers should be aware of the immediate actions in the event of an unscheduled event. Training should be provided in relation to breakdown procedures, hijack and hostage situations.
9.6(a)	Only use routes, schedules and planned stops negotiated in advance and approved.	M		Any deviation from the approved routes should be notified immediately.
9.2(a)	There must be documentary records of shipping details (time, date, driver, shipping/ receiving personnel, shipment details and quantity).	M		
9.1(a)	The driver must be present during the loading/ unloading operations to ensure the integrity of the shipment and agree the piece count (where appropriate).	M		The driver is the link between the point of loading and unloading. The cargo is his/ her responsibility throughout the journey to the point of delivery. This continuity reduces the risk of driver blamed theft.
5.1(e)	Company procedures should require that the loading of vehicles and trailers should take place as near as practicable to the departure time of the load.			Unattended vehicles and trailers should not be used for the storage of cargo.

Security of information

General Issues

Ref No.	Accreditation Criteria		Pass	(Notes)
11.2(a)	CCTV should be used to monitor all counter areas where documents are exchanged.	M		
11.3(a)	Collection of VAL/VUN air waybills must be auditable.	M		
10.1(a)	Access to paperwork and information relating to shipments of cargo should be restricted to employees who 'need to know' to allow them to carry out their job effectively.	M		Only those who have an operational need to information should be allowed access. Documents should be stored in a secure environment and completed paperwork should be returned to the secure area as soon as possible. Photocopying of documents should be monitored and a record kept.
11.5(a)	The use of company computer systems must be auditable and user sensitive.	M		A password protection system should be incorporated. All employee passwords must be changed at least quarterly.
11.1(d)	Restricted access to CCTV system functions.	M		The company needs to keep a list of authorised users and access to the equipment needs to be restricted to those listed. Staff who are required to access the CCTV equipment need to be trained to an appropriate level.
11.1(e)	Minimum 30 days retention of all CCTV VCR tapes and held in secure storage area.	M		Each tape should be used sequentially and for a maximum of 12 times only before renewal. Any damaged tapes should be replaced immediately with a new tape and the faulty tape kept for a minimum of 30 days.
11.1(f)	A termination of employment procedure must be in place that ensures the return of ID's, access cards, keys and other sensitive information from employees and contractors.	M		These procedures should form part of the employee or contractor's conditions of service. Any access to IT equipment must be immediately suspended if a member of staff is suspended pending investigation or dismissed. Following dismissal any access rights must be terminated immediately.
11.1(g)	A record should be kept relating to previous employee for a reasonable period of time after the termination of their contract.			Over time there may be the ability to share this information with other companies within the industry. Ensure that any information held complies with the Data Protection Act.

Pre-Alert Messages

12.1(b)	When in receipt of a cargo for which a pre-alert has been received, the receiving site should confirm arrival of the goods and the status of the shipment to the originator as soon as practicable.			
---------	---	--	--	--

12.1(a)	For truck shipments the collection site should pre-alert the destination site with predetermined information in an agreed format including as a minimum: departure time, expected arrival time, truck company, driver name, vehicle registration number and trailer seal numbers.			This information should be passed at the time of departure of the vehicle. Where pre-alerts are not acknowledged the dispatcher should seek to contact the receiving person to ensure that the delivery can be made.
---------	---	--	--	--

Vetting and Recruitment

(Also see appendix 'A')

Ref No.	Accreditation Criteria		Pass	(Notes)
14.1(a)	All employees must provide their employer with an appropriate criminal records check. New employees must also supply a 5-year checkable employment (unemployment) history.	M		This requirement must form part of the job application process. Unfortunately there is substantial evidence that many crimes in this industry are 'inside jobs.' It is important that all employees are appropriately vetted.
14.1(b)	All employment application forms should contain all the questions and all the declarations set in "Application for Employment (Suggested Format)" - Appendix 'A' to the AIMSS document.			

AIMSS ACCREDITATION

Suspension/ Withdrawal of Accreditation.

Where a company fails to meet the AIMSS standards required by its accreditation, the Chief Accreditation Officer may suspend or withdraw the accreditation.

The Chief Accreditation Officer will give written notification to the company of the reasons for its suspension. The company will be informed of the measures required for the reinstatement of AIMSS Accreditation. Failure to rectify the identified fault/s within a specified period will lead to withdrawal of the accreditation.

The appeals procedure will apply to case of accreditation withdrawal. Accreditation will remain suspended during any appeal procedure.

AIMSS ACCREDITATION

Appeals Process

Where a survey has been conducted and there is dispute in relation to the findings or recommendations of the surveying officer the appeals process will be instituted.

In the first instance the appellant must make written representation to the Chief Accreditation Officer detailing the areas in dispute. This should be sent to the following address.

AIMSS Chief Accreditation Officer
Crime Prevention Office
East Ramp
Heathrow Police Station
Heathrow Airport
Middlesex
TW6 2DJ

The Chief Accreditation Officer must receive this written representation no later than 21 days from the receipt of the surveying officers refusal of accreditation report and recommendations.

Information from the appellant must contain the following information:

- Name of the company and premises surveyed.
- Contact details of the company representative for AIMSS related issues.
- The nature of, and the grounds for the appeal.

Upon receipt of an appeal the Chief Accreditation Officer must contact the appellant within 10 working days from receipt to acknowledge receipt of the appeal and detail the action that is to be taken. Details of all correspondence must be recorded.

An investigation into the appeal must be conducted as soon as practicable and in any case started within 15 working days from receipt of the appeal.

The investigation will be conducted in the following manner;

1. The Chief Accreditation Officer will be responsible for the management of the investigation of the dispute.
2. An initial interview will be conducted with the appellant to identify the nature of the dispute.
3. The survey report will be examined and areas of dispute highlighted.
4. The surveying officer will be interviewed in relation to the disputed areas.
5. If considered necessary the Chief Accreditation Officer will conduct or arrange a second survey to be conducted by an independent officer.
6. A report detailing the appeal and Chief Accreditation Officers findings and recommendations will be submitted to the Detective Chief Inspector (DCI) at SO18 Aviation Security Heathrow within 30 working days from the date of receipt of the appeal.
7. The DCI will review the report and make the final decision. There is no appeal against the decision of the DCI.
8. A letter detailing the findings of the Chief Accreditation Officer and the DCI's decision will be sent to the appellant as soon as practicable.

**The Secure Transportation of
Valuable and Vulnerable Cargo on Airport**

Minimum Standards for the Secure Transportation of Valuable and Vulnerable Cargo on Airport.

The standards below should be regarded as the minimum required for the secure transportation of airfreight shipments declared to the carrier as valuable (VAL) or vulnerable (VUN) and may be subject to a security handling charge.

Valuable Cargo⁶

- a. Valuable cargo includes banknotes, diamonds, legal bank documents, gold bullion, platinum, high value jewellery and watches.
- b. An airline or freight handler specialising in the handling of valuable cargo or a recognised security company with airside access must handle all valuable cargo to and from the aircraft.
- c. All valuable cargo must be transported to and from the aircraft in an appropriate secure vehicle. The vehicle must be locked at all times. Subject to traffic conditions, the vehicle must not stop until it reaches the aircraft for exports or the vault or secure area of the warehouse for imports.
- d. If for any reason the vehicle has to stop prior to arriving at the aircraft, vault or secure area under no circumstances should the doors that give access to the valuable cargo be opened.
- e. A sign will be carried indicating that the occupants will not open windows or doors for anyone and, if necessary, follow a police / Customs car to the nearest police station or, if airside, to a predetermined secure facility. The sign will also give a telephone contact number for police / Customs use in the event of any incident involving the vehicle. In the event of the vehicle being involved in an accident or incident that immobilises it or requires the driver to remain at the scene, the driver should contact his control room and ask that police be called to attend the scene. Details including name and shoulder number of the attending officer/s should be obtained from the police control room and passed back to the driver. Police should be informed of the nature of the load being carried. **Under no circumstances should the doors be opened in an insecure location.**
- f. If the valuable cargo is too big to put into the secure vehicle it must be containerised. The container must be locked or sealed and loaded onto appropriate transport. A security escort vehicle must follow immediately behind the transport having a clear and unobtrusive view of the container at all times.
- g. The valuable cargo should only be removed from the security vehicle when it is time for that consignment to be loaded on to the aircraft.
- h. The security guards must maintain a clear view of the valuable cargo until the hold doors are secured and the aircraft departs the stand.

⁶ Valuable cargo is defined under IATA resolution 012.

- i. Imported valuable cargo must be removed from the aircraft immediately. The consignment should be checked and if in order placed straight into the security vehicle and taken immediately to the airline transit shed, handling company or security company.
- j. If any discrepancy is found relating to a valuable cargo consignment when it is removed from the aircraft the police must be informed immediately and the valuable cargo must remain in situ. If there is a security risk to the consignment it must be secured in the security vehicle until the arrival of police.
- k. The occupants of the vehicle carrying the cargo and any escort to that vehicle must have a means of communication in order to be able to have immediate contact with their base and the law enforcement agencies.

Vulnerable Cargo⁷

- l. Vulnerable cargo includes wines, spirits, cigarettes, computer parts, perfume, mobile telephones, firearms and dangerous drugs.
- m. All vulnerable cargo should be secured at all times and either be palletised or locked/ sealed in a container. If the consignment is palletised it should also be shrink wrapped and strapped.
- n. All vulnerable cargo must be transported to and from the aircraft in an appropriate secure vehicle. The vehicle must be secured at all times. Subject to traffic conditions, the vehicle must not stop until it reaches the aircraft for exports or a secure area of the warehouse for imports.
- o. All vulnerable consignments for export should be checked prior to leaving the warehouse to ensure that the consignment is intact. If, having checked the consignment, there is any suggestion that the consignment could have been compromised then it must not leave the warehouse without being fully scrutinized.
- p. Either a representative of the airline, handling agent or the airside transport company should escort all vulnerable cargo from the warehouse to the aircraft.
- q. On arrival at the aircraft the vulnerable consignment should be checked prior to being loaded on to the aircraft to ensure that it is still fully intact. If, having checked the consignment, there is any suggestion that the consignment has been compromised then it must not be loaded onto the aircraft and should be returned to the warehouse.
- r. For imported consignments, immediately the offload of the vulnerable cargo has taken place a representative of the airline, handling agent or the transport company should check the integrity of the consignment to ensure that it is fully intact. If found correct the vulnerable cargo must be taken directly back to the warehouse.

⁷ Vulnerable cargo can be defined as any shipment containing a commodity that may be at risk of being stolen or tampered with.

- s. If there is any doubt as to the integrity of the vulnerable freight a written note should be made of the possible discrepancies and the manager of the airline or handling company should be advised immediately. The vulnerable freight should then be taken directly back to the warehouse.
- t. If the vulnerable cargo is too big to put into the appropriate secure vehicle it must be containerised. The container must be locked or sealed for transportation. A security escort vehicle must follow immediately behind the transport having a clear and unobtrusive view of the container at all times.
- u. For both import and export vulnerable freight, if there is any suggestion that a theft has occurred between the warehouse and the aircraft or the aircraft to the warehouse the police and customs must be advised immediately. The consignment must be stored in a secure area until the police have been given the opportunity to view it.
- v. At no time should the security vehicle or container containing vulnerable cargo be left unattended. The person(s) designated to ensure the security of the vulnerable cargo must have a clear and unobtrusive view of the vehicle, container or cargo when being transferred to and from the aircraft at all times.
- w. Under no circumstances should vulnerable cargo, whether carried as an import or an export, be left at aircraft side or anywhere else on the airport, including a holding area, unless it is supervised at all times.

Appendix D

Glossary Of Terms and Abbreviations

AIMMS	Airfreight Industry Minimum Security Standards
AOCC	Aircraft Operators Committee Cargo
AOD	Airport Of Destination
AWB	Air Waybill
BA	British Airways
BAA	British Airports Authority
BIFA	British International Freight Association
Cargo Area (Designated Airport)	“Any area which appears to the Secretary Of State to be used wholly or mainly for the storage or handling of cargo in an aerodrome and is designated by an order made by him for the purpose of section 27(6) of the Aviation Security Act 1982”
CDR	Cargo Damage Report
CIF	Cost Insurance Freight
CIR	Cargo Irregularity Report
CPO	Crime Prevention Officer
EMEA	Europe Middle East Africa
ERTS	Enhanced Remote Transit shed
ETA	Estimated Time Of Arrival
FAK	Freight All Kinds
FIATA	International Federation Of Freight Forwarders Associations
HAL	Heathrow Airport Limited
IIS	Incident Information Service
LEA	Law Enforcement Agency
MPS	Metropolitan Police Service
MPA	Metropolitan Police Authority
RHA	Road Haulage Association
RTS	Remote Transit Shed
SITA	Société Internationale De Télécommunications Aéronautiques
SSL	Shed Storage Location
TAPA	Technology Asset Protection Association
UTL	Unable To Locate
Val	Valuable
Vun	Vulnerable