Office for Nuclear Regulation

NOT PROTECTIVELY MARKED

ONR GUIDE			
THE CARRIAGE OF DANGEROUS GOODS AND USE OF TRANSPORTABLE PRESSURE EQUIPMENT REGULATIONS 2009 – INSPECTION OF TRANSPORT SECURITY REQUIREMENTS			
Document Type:	Nuclear Safety Technical Inspection Guide		
Unique Document ID and Revision No:	NS-INSP-GD-072 Revision 1		
Date Issued:	July 2019	**Review Date:**	June 2024
Approved by:	Gavin Smith	Transport Competent Authority	
Record Reference:	CM9 Folder 1.1.3.979. (2020/139156)		
Revision commentary:	Rev 0: Updated from ONR-INSP-IN-004 Revision 1 (2019/118673) to convert from a Compliance Inspection Instruction to a Technical Inspection Guide Rev 1: Updated review period		

TABLE OF CONTENTS

Published 05/20

1 INTRODUCTION

1.1 The carriage of dangerous goods by road, rail and inland waterway in Great Britain, including radioactive material, is regulated by the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009 (Statutory Instrument 2009 No. 1348), also referred to as CDG 2009.

1.2 ONR inspects compliance with CDG 2009, and also with the arrangements made under them, to judge the suitability of the arrangements made and the adequacy of their implementation in respect of the civil carriage of Class 7 dangerous goods (radioactive material). To support inspectors undertaking compliance inspections, ONR produces a suite of guides to assist inspectors to make regulatory judgements and decisions in relation to the adequacy of compliance, and the safety of duty holder activities. This inspection guide is one of a suite of documents provided by ONR for this purpose.

1.3 The relevant regulatory requirements concerning the civil carriage of class 7 goods by road and rail in Great Britain are set out in CDG 2009 and subsequent amending Regulations. Regulation 5 requires that no person is to carry dangerous goods, or cause or permit dangerous goods to be carried, where that carriage is prohibited by ADR (European Agreement Concerning the International Carriage of Dangerous Goods by Road) and RID (Regulations Concerning the International Carriage of Dangerous Goods by Rail), including where that carriage does not comply with any applicable requirements of ADR or RID. Inspectors should consult these documents in preparing for and carrying out their compliance inspection.

2 PURPOSE AND SCOPE

2.1 This guidance has been produced to facilitate a sound and consistent approach to compliance inspections of CDG 2009. This guide has been prepared as an aid to inspection activities carried out by ONR inspectors and to provide guidance to inspectors whilst inspecting the security requirements of a duty holder in relation to the transport of Class 7 dangerous goods.

2.2 CDG refers to the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR). CDG 2009 also refers to the Regulations concerning the International Carriage of Dangerous Goods by Rail (RID). Most Class 7 dangerous goods which are not in the scope of the Nuclear Industries Security Regulations (NISR) 2003, Paragraph 2.5 below refers, are transported by road in Great Britain. Consequently, this guide provides detailed guidance on the interpretation of the implementation of the security provisions contained in ADR.

2.3 The guidance is for use by inspectors in ONR. It is envisaged that the inspection of the security requirements of a duty holder will be included as part of an overall inspection encompassing safety and security measures. The guidance does not indicate when or to what frequency inspections of the requirements of CDG 2009 should be carried out, as these matters are covered in individual inspector's inspection plans, which take account of priorities established by the relevant ONR sub division. Security measures taken during the transport[1] of radioactive material to protect it against malicious acts should be based on evaluating the threat to the material and its potential to cause unacceptable consequences.

2.4 Through the Civil Nuclear Security and Safeguards (CNSS) Division, ONR regulates the security of nuclear and other radioactive materials on civil licensed nuclear sites,

[1] For the purposes of the IAEA transport regulations upon which the provisions of ADR and RID are based, 'transport' comprises all operations and conditions associated with, and involved in, the movement of radioactive material; these include the design, manufacture, maintenance and repair of packaging, and the preparation, consigning, loading, carriage including in-transit storage, unloading and receipt at the final destination of loads of radioactive material and packages.

Category I-III quantities of civil Nuclear Materials held off licensed sites or during domestic transport by road, rail and sea, and the international transport of nuclear materials by UK flagged vessels. It also regulates Sensitive Nuclear Information wherever it is held. It does this in accordance with the NISR 2003. Regulations 13-21 of NISR 2003 detail the legal obligations for security while transporting civil Category I-III Nuclear Material. More detailed requirements concerning the transport of civil Category I-III Nuclear Material are contained in specific technical guidance, which is issued by ONR to support duty holders in their implementation of NISR 2003. The transport of Category IV Nuclear Material, radioactive sources and Other Radioactive Material outside civil licensed nuclear sites does not fall under NISR 2003, but where applicable is subject to the requirements for the carriage of Class 7 dangerous goods. The security arrangements for these consignments are regulated by inspectors delivering to the Transport Competent Authority.

2.5 ADR, Chapter 1.10 details the security provisions for the carriage by road of dangerous goods. For the purposes of Chapter 1.10, security means the measures or precautions to be taken to minimise theft or misuse of dangerous goods that may endanger persons, property or the environment.

2.6 In view of the potential vulnerability of radioactive material in transport, the design of an adequate transport security system should incorporate the concept of defence in depth and a graded approach to achieve the objective of preventing the material from becoming susceptible to malicious acts. The transport security system should be designed to take into account:

- The quantity, and the physical and chemical form of the radioactive material.
- The mode(s) of transport.
- The packages being used.
- Measures that are required to deter, detect and delay unauthorised access to the radioactive material while in transport or during storage in transit to defeat any attempted malicious acts.

3 GUIDANCE ON INSPECTION OF ARRANGEMENTS AND THEIR IMPLEMENTATION

3.1 The following sets out ONR's expectations in regard to compliance inspections and to provide guidance to ONR inspectors whilst inspecting the security requirements of a duty holder. The expectations are intended to be used as an aide memoire during inspections, following the security provisions detailed in ADR, Chapter 1.10. Each expectation is followed by detailed guidance intended to provide prompts to assist in identifying potential issues but is not intended to be exhaustive.

3.2 ADR 1.10.1 - General Provisions for the Carriage of Dangerous Goods

3.2.1 ADR 1.10.1.1 - All persons engaged in the carriage of dangerous goods shall consider the security requirements set out in this Chapter commensurate with their responsibilities.

3.2.1.1 To establish who has overall responsibility for security. Depending on the size of the organisation, there could be one or more persons managing security. However, it is ONR's expectation that one person in an organisation should have overall responsibility and accountability for ensuring the security requirements are met.

3.2.1.2 Personnel engaged in the carriage of dangerous goods who have a security function detailed within their job description should ensure that they understand their responsibilities.

3.2.1.3 Reliable and responsible staff are central to making sure that other security measures work effectively. Documentary evidence of the background and experience of anyone recruited and being recruited should be obtained. Employers should warn applicants that giving false information, or failing to disclose material information, might constitute grounds for their not being recruited or subsequent dismissal. Organisations should ensure all new employees who are to be involved with the transport of dangerous goods are suitable for the task and that they hold verifiable licences, certificates where applicable and permission to work in the UK where necessary.

3.2.1.4 When conducting pre-employment checks, candidates should be asked for the following information:

- Full name.
- Address.
- Date of birth. Employers should insist on seeing the applicant's original birth certificate, not a photocopy.
- National insurance or other unique personal identifying number where appropriate.
- Details of any past criminal convictions by requesting a disclosure certificate (where this is allowed by law).
- Full details of references (where applicable).

3.2.1.5 Employers should obtain a continuous (unbroken) record of the applicant's education and employment history. This may not always be easy, but in general they should ask for information covering the preceding 10 years, and as an absolute minimum covering the previous five years.

3.2.1.6 When checking the identity of a candidate, employers should ask to see a passport, an official photo ID and utility bills sent to the applicant's address. Where appropriate, the proof of right to live and work in the UK should have been verified. Information and guidance regarding a job applicant's 'right to work' documents can be accessed via the following link https://www.gov.uk/legal-right-work-uk.

3.2.1.7 The employer should maintain a progress sheet to record all the actions that have been taken concerning pre-employment checks.

3.2.2 ADR 1.10.1.2 - Dangerous goods shall only be offered for carriage to carriers that have been appropriately identified.

3.2.2.1 It is important that carriers are appropriately identified. When offering goods to a road transport contractor, written assurances should be obtained from the contractor concerning compliance with the dangerous goods security requirements. As a minimum, when Class 7 high consequence[2] dangerous goods (HCDG) are being carried, it should be confirmed that the contractor has a transport security plan.

3.2.2.2 The appropriate identification of carriers should also include checking drivers' documents, including their photo ID and, if appropriate, their ADR vocational

[2] See ADR 1.10.3.1.3 and section 3.5 below

qualification. This could be done by the consignor(s) on the carriers' first visit to site, with on-going scheduled or random checks being carried out as part of a supplier audit. Dangerous goods should only be handed over to appropriately identified carriers whose driver can produce suitable identification.

3.2.3 ADR 1.10.1.3 - Areas within temporary storage terminals, temporary storage sites, vehicle depots, berthing areas and marshalling yards used for the temporary storage during carriage of dangerous goods shall be properly secured, well-lit and, where possible and appropriate, not accessible to the general public.

3.2.3.1 For the purposes of ADR, parking or necessary short stops during a journey are not considered temporary storage. Temporary storage does not encompass overnight parking or stops en-route, as 'parking' is not the same as storage. The requirements for parking and supervision are defined in ADR section 8.4.

3.2.3.2 Temporary storage includes stops made necessary by the conditions of carriage as well as changes to the mode of transport. Areas used for the temporary storage of dangerous goods must be secure. This means they should be controlled by a combination of physical barriers, security equipment, procedures and staff vigilance. Guidance on physical security can be found on the Centre for the Protection of National Infrastructure (CPNI) website at: http://www.cpni.gov.uk/advice/physical-security/. The CPNI protects national security by providing protective security advice. Their advice covers physical security, personnel security and cyber security/information assurance.

3.2.3.3 To secure dangerous goods it is reasonable to consider a balance between staff presence and a secure perimeter fence to achieve the right outcome. All relevant areas should be subject to a security risk assessment to establish what measures are required to prevent unauthorised access and action taken accordingly to reduce identified risks. Inspectors should establish if a security risk assessment has been conducted and implemented. A risk assessment template and information on conducting a risk assessment is contained in the Department for Transport (DfT) publication, 'security guidance on the carriage of dangerous goods by road and rail', which is available on the DfT website at https://www.gov.uk/government/publications/security-requirements-for-moving-dangerous-goods-by-road-and-rail. It should be clearly identified in site plans which areas have restricted access. Visitors or contractors should only be issued with temporary passes and escorted where appropriate; pass holders might only be given access to certain areas of the site in line with their duties and issued passes with photographic identification.

3.2.3.4 Restricting access to Class 7 HCDG should be of significant concern and can be delivered in different ways. A critical facility or building containing HCDG should have higher levels of security in place than other areas of the site.

3.2.3.5 Where appropriate, additional fencing or patrols could be considered around the areas where vehicles are kept when loaded with Class 7 HCDG high consequence dangerous goods.

3.2.3.6 Sites shall be well-lit where dangerous goods are kept. Lighting should complement other security equipment such as CCTV and enable any security patrols to be conducted effectively. Regular checks should be carried out by duty holders to ensure that all security equipment and control measures are functioning correctly. General guidance on physical security measures for temporary storage sites, including details on lighting and CCTV is contained at Annex A.

3.2.3.7 Sensitive information, documents and IT should also be protected. It is important to consider the insider threat and transport information should be kept secure to ensure it is not released to anyone who is not authorised to receive the information and/or has no 'need to know'.

3.2.3.8 All reasonable steps should be taken to ensure unauthorised access to dangerous goods is prevented.

3.2.4 ADR 1.10.1.4 - Each member of a vehicle crew shall carry with them means of identification, which includes their photograph, during carriage of dangerous goods.

3.2.4.1 Photographic identification must be carried at all times during carriage. A driver's photo card driving licence or passport would be sufficient to meet this requirement. It is recommended that random spot checks of visiting drivers' and crew members' photo ID passes are carried out. Staff should challenge persons on site who are not familiar and/or not wearing a pass.

3.2.5 ADR 1.10.1.5 - Safety inspections in accordance with 1.8.1 and 7.5.1.1 shall cover appropriate security measures.

3.2.5.1 When inspectors conduct spot checks as detailed in ADR 1.8.1.1, to verify whether the requirements concerning the carriage of dangerous goods have been met, inspections should include security measures. In accordance with section 7.5.1.1 of ADR, drivers and vehicles are required to comply with security provisions and suitable vehicle inspections at sites where loading and/or unloading takes place. Sites receiving or despatching dangerous goods should have suitable measures in place for checking compliance before allowing entry to premises. This could include checking the driver's photographic identification and qualifications, checking names and addresses on transport documentation.

3.3 **ADR 1.10.2 – Security Training**

3.3.1 ADR 1.10.2.1 - The training and the refresher training specified in Chapter 1.3 shall also include elements of security awareness. The security refresher training need not be linked to regulatory changes only.

3.3.1.1 Duty holders are required to provide security awareness training for everyone engaged in the carriage of dangerous goods. A suitable training programme should be drafted and the subsequent training should be provided to all staff involved in dangerous goods transport operations. It should not be limited to drivers or production staff, but include anyone with security roles and responsibilities, as well as anyone with access to transport information. The nature of the training can be tailored to suit the requirements of each organisation and staff members' level of responsibility. Vehicle crews play a key role in journey security as the vulnerabilities increase once the vehicle is on the road. It would be expected to see evidence of more specific training being given to those with specialised security duties or the management of security.

3.3.2 ADR 1.10.2.2 - Security awareness training shall address the nature of security risks, recognising security risks, methods to address and reduce such risks and actions to be taken in the event of a security breach. It shall include awareness of security plans (if appropriate) commensurate with the responsibilities and duties of individuals and their part in implementing security plans.

3.3.2.1 The duty holder's in-house training should cover the above topics. Further security training can be obtained from private training suppliers or other government departments including the CPNI www.cpni.gov.uk and Counter Terrorism Security Advisors (CTSAs) www.gov.uk/government/organisations/national-counter-terrorism-

security-office. Guidance for the design and delivery of security awareness training for the carriage of dangerous goods by road and rail can be found on the DfT website at: https://www.gov.uk/government/publications/security-requirements-for-moving-dangerous-goods-by-road-and-rail.

3.3.2.2 Developing a security culture within an organisation is about encouraging staff to respect common values and standards towards security whether they are inside or outside the workplace. The CPNI has developed a security culture survey tool (SeCuRE 3) to enable organisations to shape the strategic direction of their security policies. SeCuRE 3 can be used by organisations to examine their existing security culture and identify where and why it might need to change. It can be used to assess whether the right mix of mechanisms are in place to deliver the security response desired by the organisation. Information regarding the SeCuRE 3 tool can be found on the CPNI website at: http://www.cpni.gov.uk/advice/personnel-security1/security-culture/.

3.3.2.3 The training should include awareness of the security plans when appropriate, what each person's role is in providing security and the company procedures to be followed for reporting suspicious activity, threats or breaches of security.

3.3.2.4 In the event of a security breach or transport related incidents of Class 7 dangerous goods, in addition to following company procedures and notifying the police if applicable, the duty holder should report the occurrence to ONR in accordance with the requirements detailed in ADR, section 1.8.5. It is to be established that duty holders are aware of the reporting procedures and timescales and that they are aware of the guidance contained on the ONR website including how to contact ONR.

3.3.3 ADR 1.10.2.3 - Such training shall be provided or verified upon employment in a position involving dangerous goods transport and shall be periodically supplemented with refresher training.

3.3.3.1 It is recommended that security awareness training is refreshed at 2 to 3 year intervals, or following a significant event or a major update to the security plan. The training programme should remind operators when refresher training is due. New employees or contractors engaged in the carriage of dangerous goods should be provided with relevant training at the induction stages of their employment at the organisation or site.

3.3.4 ADR 1.10.2.4 - Records of all security training received shall be kept by the employer and made available to the employee or competent authority, upon request. Records shall be kept by the employer for a period of time established by the competent authority.

3.3.4.1 Training records can be kept electronically or in hard copy and should be retained in a secure location for a minimum of four years from the date of the training. ONR must be able to inspect applicable training records on request.

3.4 Class 7 Non-High Consequence Dangerous Goods

3.4.1 Security plans are not required for carriers, consignors and other participants engaged in the transport of Class 7 non-high consequence dangerous goods. However, it is good practice for duty holders involved in the carriage of Class 7 non-high consequence dangerous goods to have a security plan in order to mitigate the security risks.

3.5 Provisions for High Consequence Dangerous Goods (HCDG)

3.5.1 In addition to the above guidance duty holders involved in the carriage of Class 7 HCDG, are subject to additional security requirements detailed below. The following

guidance is for use by inspectors to assist in establishing whether duty holders are in compliance with the further security requirements for the transport of Class 7 HCDG.

3.5.2 ADR 1.10.3.1 - Definition of High Consequence Dangerous Goods

3.5.3 ADR 1.10.3.1.1 - High Consequence Dangerous Goods are those which have the potential for misuse in a terrorist event and which may, as a result, produce serious consequences such as mass casualties, mass destruction or, particularly for Class 7, mass socio-economic disruption.

3.5.3.1 Inspectors must confirm that duty holders involved in the carriage of dangerous goods have a system whereby the consignor is able to identify i that Class 7 HCDG are to be transported. A process is needed to ensure that relevant information is shared between the carrier, consignor and consignee, in advance of the transport of HCDG, to enable duty holders to give specific consideration to determining and applying particular security requirements that may be necessary for an individual consignment.,

3.5.4 ADR 1.10.3.1.3 - For dangerous goods of Class 7, high consequence radioactive material (HCRM) is that with an activity equal to or greater than a transport security threshold of 3000 A_2 per single package (see also ADR 2.2.7.2.2.1) except for the following radionuclides where the transport security threshold is given in table 1.10.3.1.3 (reproduced below).

Table 1.10.3.1.3 – Transport Security Thresholds for Specific Radionuclides

Element	Radionuclide	Transport security threshold (TBq)
Americium	Am-241	0.6
Gold	Au-198	2
Cadmium	Cd-109	200
Californium	Cf-252	0.2
Curium	Cm-244	0.5
Cobalt	Co-57	7
Cobalt	Co-60	0.3
Caesium	Cs-137	1
Iron	Fe-55	8000
Germanium	Ge-68	7
Gadolinium	Gd-153	10
Iridium	Ir-192	0.8
Nickel	Ni-63	600
Palladium	Pd-103	900
Promethium	Pm-147	400
Polonium	Po-210	0.6
Plutonium	Pu-238	0.6
Plutonium	Pu-239	0.6
Radium	Ra-226	0.4
Ruthenium	Ru-106	3
Selenium	Se-75	2

Element	Radionuclide	Transport security threshold (TBq)
Strontium	Sr-90	10
Thallium	Tl-204	200
Thulium	Tm-170	200
Ytterbium	Yb-169	3

3.5.4.1 Inspectors should confirm that duty holders understand that all radionuclides in Table 2.2.7.2.2.1 of ADR can be considered as high consequence radioactive materials if the activity is equal or greater than 3000 A_2 per single package, and is not limited to only those set out in Table 1.10.3.1.3.

3.5.5 ADR 1.10.3.1.4 - For mixtures of radionuclides, determination of whether or not the transport security threshold has been met or exceeded can be calculated by summing the ratios of activity present for each radionuclide divided by the transport security threshold for that radionuclide. If the sum of the fractions is less than 1, then the radioactivity threshold for the mixture has not been met nor exceeded.

3.5.5.1 Inspectors should confirm that, where appropriate, duty holders have undertaken this calculation correctly. This can be achieved by sampling relevant transport documents and the activities declared therein.

3.5.6 ADR 1.10.3.1.5 - When radioactive material possesses subsidiary risks of other classes, the criteria of table 1.10.3.1.2 shall also be taken into account (see also 1.7.5).

3.6 **ADR 1.10.3.2 - Security Plans**

3.6.1 ADR 1.10.3.2.1 - Carriers, consignors and other participants specified in 1.4.2 and 1.4.3 engaged in the carriage of high consequence dangerous goods (see Table 1.10.3.1.2) or high consequence radioactive material (see 1.10.3.1.3) shall adopt, implement and comply with a security plan that addresses at least the elements specified in 1.10.3.2.2.

3.6.1.1 The security plan should be based on the overall operation of the business, not on individual movements, and be tailored to suit the company's operational activities. A transport security plan is not the same as a site security plan, but if the latter exists then one could complement the other or both plans could be merged. The drafting and format of the security plan should take into account the business operation in deciding how to structure the plan. It should be noted that the requirements listed at 1.10.3.2.2 (a) to (h) are the minimum for inclusion.

3.6.1.2 Plans should take into account other plans which may be in place, any risk to the site or carrier, and any unique circumstances or location of premises. Consideration should be given to the detailing the measures for the appropriate protection to the main vulnerable areas, which include the consigning site, consignee site, any temporary in-transit storage sites, any modal or intermodal transfer points and any stops necessary for operational or other reasons. Security plans should be considered 'live' documents and kept under review so that they reflect changes to sites, the nature of the operation and key personnel. Security plans and procedures should be tested by holding regular exercises that adequately test security measures, such as an access control test.

3.6.1.3 The plan should clearly identify those involved in the dangerous goods transport chain and what their security roles and responsibilities are, including dealing with security incidents.

3.6.2 ADR 1.10.3.2.2 - The security plan shall comprise at least the following elements:

(a) Specific allocation of responsibilities for security to competent and qualified persons with appropriate authority to carry out their responsibilities;

(b) Records of dangerous goods or types of dangerous goods concerned;

(c) Review of current operations and assessment of security risks, including any stops necessary to the transport operation, the keeping of dangerous goods in the vehicle, tank or container before, during and after the journey and the intermediate temporary storage of dangerous goods during the course of intermodal transfer or transhipment between units as appropriate;

(d) Clear statement of measures that are to be taken to reduce security risks, commensurate with the responsibilities and duties of the participant, including:

- training;

- security policies (e.g. response to higher threat conditions, new employee/employment verification, etc.);

- operating practices (e.g. choice/use of routes where known, access to dangerous goods in intermediate temporary storage (as defined in (c)), proximity to vulnerable infrastructure etc.);

- equipment and resources that are to be used to reduce security risks;

(e) Effective and up to date procedures for reporting and dealing with security threats, breaches of security or security incidents;

(f) Procedures for the evaluation and testing of security plans and procedures for periodic review and update of the plans;

(g) Measures to ensure the physical security of transport information contained in the security plan; and

(h) Measures to ensure that the distribution of information relating to the transport operation contained in the security plan is limited to those who need to have it. Such measures shall not preclude the provision of information required elsewhere in ADR.

Note: Carriers, consignors and consignees should co-operate with each other and with competent authorities to exchange threat information, apply appropriate security measures and respond to security incidents.

3.6.2.1 ADR 1.10.3.2.2(a). It is ONR's expectation that one person should have full responsibility for security procedures and have sufficient authority to design and implement these. It is to be established who has responsibility for security and the allocation of responsibilities. The person responsible for security should control the security plan and share the information as required within the organisation. Security responsibilities should be documented in the security plan and should form part of job role specification or be included in a person's job description.

3.6.2.2 ADR 1.10.3.2.2(b). A summary of the types of Class 7 dangerous goods regularly carried should be included. The radioisotope(s) being transported, physical and chemical form of the material and the amount being transported should be included. This could be a table which lists the UN Numbers and shipping names identifying which are high consequence dangerous goods. A reference to the Dangerous Goods Safety Advisor Annual Report could be made, which should include a summary of the

dangerous goods moved over the previous 12 months. The consignor and the carrier shall retain a copy of the dangerous goods transport document and additional information and documentation as specified in ADR, for a minimum of three months from the date of carriage in accordance with the requirements of ADR 5.4.4.

3.6.2.3 ADR 1.10.3.2.2(c). An overview of the current operation should be included at the start of the security plan to describe its purpose and scope. This will set out the reasons for the plan, how and why it applies to the business and to the carriage of Class 7 high consequence dangerous goods. In addition to the examples listed in ADR 1.10.3.2.2 (c) security plans should also consider whether drivers should be encouraged to keep their cab doors and windows closed and locked throughout the journey.

3.6.2.4 ADR 1.10.3.2.2(d). The security plan must include the measures detailed at section 1.10.3.2.2(d), which support transport security. The specific instructions and guidance given to drivers and crew plus what specific measures are taken in the event of unplanned or unusual circumstances should be included in this section. The following areas are to be addressed in the security plan to reduce security risks:

- Training. Guidance concerning training is detailed at Section 3.3 of this guidance document.

- Security Policies. A security policy statement should be written and included. Depending on the nature of the operation, and potential vulnerabilities, there should be documented and predetermined arrangements for responding to changes in the National Threat Levels. The security plan should consider changes to business or national threat levels. Duty holders can obtain up to date information and guidance regarding the National Threat Levels via accessing the following link https://www.mi5.gov.uk/home/news/news-by-category/threat-level-updates.html. The security plan is to include the policy for conducting pre-employment checks of potential new employees who will be involved with the transport of dangerous goods as described in 3.2.1.4 – 7 above.

- Operating Practices. The plan should document how Class 7 HCDG are accepted and the process for determining specific security requirements necessary for a particular movement such as how movements are controlled and monitored to ensure security. Additionally, the plan should detail how any problems with the movement are dealt with, for example security during unplanned intermediate stops.

- Equipment and Resources. The security plan statement of measures must also identify and record the equipment and resources deployed in the security arrangements for the transport of Class 7 HCDG. It is possible that the equipment may not be solely for that purpose, e.g. lighting may be provided for operational safety and CCTV in place for preventing vandalism and criminal activity. This section should also identify what resources are available and utilised when there are necessary breaks in a journey.

3.6.2.5 ADR 1.10.3.2.2(e). The security plan should detail the system or procedures in place for reporting a security incident or a security concern. There should be an internal procedure to guide staff on what action to take and who they should report to. Information should be shared or exchanged with other carriers, consignors, competent authorities as well as Police or Security Services, dependent on the nature of the incident. This process should be recorded in the security plan.

3.6.2.6 ADR 1.10.3.2.2(f). The requirement for testing of security plans is to be detailed and the frequency for periodic review and update of the plans. It is good practice to review and update security plans on a regular basis, preferably annually, or in response to an event, to ensure the accuracy of its content and to consider updating the security plan following any security incident or test where lessons have been learned or a change of operations.

3.6.2.7 ADR 1.10.3.2.2(g). The security plan must state how the information in the plan is protected from unauthorised access e.g. held electronically on a password-protected computer in a location with restricted access. If printed, the plan should be kept secure and treated as a sensitive document, only shared with emergency services or the competent authority on request. Everyone with access should be aware the information it contains should only be made available on a need to know basis.

3.6.2.8 ADR 1.10.3.2.2(h). The security plan should describe the measures in place to restrict the distribution of information about the Class 7 dangerous goods transport operations to only those who need the information.

3.6.3 ADR 1.10.3.3 - Devices, equipment or arrangements to prevent the theft of the vehicle carrying high consequence dangerous goods (see Table 1.10.3.1.2) or high consequence radioactive material (see 1.10.3.1.3) and its cargo, shall be applied and measures taken to ensure that these are operational and effective at all times. The application of these protective measures shall not jeopardize emergency response.

3.6.3.1 The application of measures to prevent theft will need to be determined by the carrier and the consignors. Examples of devices and equipment include locks, seals and tracking devices. Duty holders should seek specialist advice from commercial organisations, CTSAs or CPNI when appropriate. There should be a system in place for reporting failures of devices, equipment or arrangements. It is advisable that drivers have a means of communication at all times when carrying Class 7 high consequence dangerous goods.

3.6.3.2 Note: When appropriate and already fitted, the use of transport telemetry or other tracking methods or devices should be used to monitor the movement of high consequence dangerous goods (see Table 1.10.3.1.2) or high consequence radioactive material (see ADR 1.10.3.1.3).

3.6.3.3 Tracking systems are widely available for goods vehicles and trailers. Fitting such equipment represents good practice when carrying Class 7 high consequence dangerous goods. It may also be appropriate to consider tracking the freight or container itself if the goods are particularly sensitive or attractive to thieves.

3.6.3.4 To inspect arrangements for testing and checking that security equipment is operational and fit for purpose on a regular basis. This is to include the checking/testing of tracking systems, mobile phones, alarms, immobilisers, locks, CCTV and any other equipment, the failure of which may be detrimental to the security of radioactive material in transit.

3.6.4 ADR 1.10.4 - In accordance with the provisions of 1.1.3.6, the requirements of 1.10.1, 1.10.2, 1.10.3 and 8.1.2.1 (d) do not apply when the quantities carried in packages on a transport unit do not exceed those referred to in 1.1.3.6.3, except for UN Nos. 2910 and 2911 if the activity level exceeds the A_2 value (see first indent of 1.1.3.6.2). In addition, the requirements of 1.10.1, 1.10.2, 1.10.3 and 8.1.2.1 (d) do not apply when the quantities carried in tanks or in bulk on a transport unit do not exceed those referred to in 1.1.3.6.3. In addition the provisions of this Chapter do not apply to the carriage of UN No. 2912

RADIOACTIVE MATERIAL, LOW SPECIFIC ACTIVITY (LSA-I) and UN No. 2913 RADIOACTIVE MATERIAL, SURFACE CONTAMINATED OBJECTS (SCO-I).

3.6.4.1 The above relates to specified quantities of radioactive materials referenced in ADR, below which the requirements of these security provisions do not apply.

3.6.5 ADR 1.10.5 - For radioactive material, the provisions of this chapter are deemed to be complied with when the provisions of the convention on physical protection of nuclear material and the IAEA circular on "The Physical Protection of Nuclear Material and Nuclear Facilities" are applied.

4 DETERMINATION OF ADEQUACY / MAKING A JUDGEMENT / NON COMPLIANCE

4.1 It is for inspectors to apply their experience and discretion to determine the extent and depth of a particular inspection to include the required security measures, as detailed at Chapter 1.10 of ADR.

4.2 In determining adequacy, the Inspection rating guide, should be used by inspectors, which can be found on the HOW2 process 'Planning and Conducting Interventions'.

4.3 Where inspection indicates that a duty holder's arrangements fall significantly short of CDG 2009 requirements and especially where enforcement action appears to be warranted under the Enforcement Management Model (EMM) and more specifically ONR-ENF-GD-006 - ONR Guide: Enforcement, the inspector should seek advice from the relevant Delivery Lead. When conducting compliance inspections of duty holders, should the following non-compliant subjects be identified, consideration should be given to formal enforcement action being taken:

- Implementation of inadequate physical security measures for Class 7 dangerous goods being held in temporary storage or in transit.
- Security training not being conducted, contrary to ADR, 1.10.2, applicable to the carriage of Class 7 dangerous goods.
- Not having a security plan, contrary to ADR, 1.10.3.2.1, applicable to the carriage of Class 7 high consequence dangerous goods.

4.4 The above list is not exhaustive and consideration should be given to formal enforcement action being taken concerning other non-compliance issues that have been identified, if deemed appropriate.

5 FURTHER READING

5.1 The IAEA Nuclear Security Series guidance identified below are the current versions, it should be noted however that the documents were produced between 2008 and 2011 meaning that a number of the referenced IAEA documents within the guidance have been updated since publication.

5.2 IAEA Nuclear Security Series No 9 Implementing Guide Security in the Transport of Radioactive Material. See link:
http://www-pub.iaea.org/MTCD/publications/pdf/pub1348_web.pdf

5.3 IAEA Nuclear Security Series No 11 Nuclear Security Recommendations on Security of Radioactive Sources. See link:
http://www-pub.iaea.org/MTCD/publications/PDF/Pub1387_web.pdf

5.4 IAEA Nuclear Security Series No 14 Nuclear Security Recommendations on Radioactive Material and Associated Facilities. See link: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1487_web.pdf

5.5 ONR's transport of radioactive materials webpages. See link: http://www.onr.org.uk/transport/index.htm

5.6 INFCIRC/225/Rev.4 (Corrected) The Physical Protection of Nuclear Material and Nuclear Facilities Published by the IAEA. See link: https://www.iaea.org/sites/default/files/infcirc225r4c.pdf

6 DEFINITIONS

ADR	European Agreement Concerning the International Carriage of Dangerous Goods by Road
CDG 2009	The Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009
CCTV	Closed Circuit Television
CNS	Civil Nuclear Security
CPNI	Centre for the Protection of National Infrastructure
CTSA	Counter Terrorism Security Advisor
DGSA	Dangerous Goods Safety Advisor
DfT	Department for Transport
HCDG	High Consequence Dangerous Goods
HCRM	High Consequence Radioactive Material
NISR 2003	Nuclear Industries Security Regulations 2003
ONR	Office for Nuclear Regulation
RID	Regulations Concerning the International Carriage of Dangerous Goods by Rail

ANNEX A – GENERAL GUIDANCE ON PHYSICAL SECURITY MEASURES

Introduction

1. Physical security should be designed to make it as difficult as reasonably practical for an intruder or insider to steal or have unauthorised access to dangerous goods. Good security is a combination of physical measures, sound procedures and the awareness and attitude of managers and employees. Actual measures may vary from location to location, depending on the nature of the business. This Annex highlights effective physical security measures at storage sites including depots and on vehicles used for the transport of Class 7 dangerous goods. The implementation of security measures should be pragmatic and proportionate. Further information and advice regarding physical security systems can be accessed via the CPNI website http://www.cpni.gov.uk/advice/Physical-security/.

Physical Security

2. All good physical security regimes are based on the principle – deter, detect and delay. In order for this principle to work, detection must come before delay.

    - Deter – the overt physical and electronic security measures that might deter a would-be intruder.
    - Detect – alarm systems, with visual (CCTV) verification, to detect the presence of an intruder.
    - Delay – physical security measures that delay the intruder long enough to allow a response force to attend.

Access Control

3. Keep access points to a minimum and make sure the boundary between public and private areas of a building is secure and clearly signed. Good quality access controls should be in use such as magnetic swipe identification cards or 'proximity' cards which are readable from a short distance. When inspecting access control, to establish that there are controls in place to prevent tailgating and the possibility of bypassing barriers.

Searching on Entry and Exit

4. Where appropriate, it should be a condition of entry and/or exit to a site that people may undergo a body search and vehicles are to be searched. Body searches should be witnessed and only trained staff should carry them out. Where there are areas of particular sensitivity and/or risk, random searching on entry and exit could be undertaken. Further information and advice regarding searching can be accessed via the CPNI website http://www.cpni.gov.uk/advice/Physical-security/Screening/. Additionally, information about training security guards to conduct any searching requirements and details on training providers, can be found via the Security Industry Authority (SIA) website http://www.sia.homeoffice.gov.uk/Pages/training.aspx.

Doors

5. Generally, doors should:

    - Be strong in construction;
    - Have commensurate good quality locking hardware;
    - Delay forced entry;

- Prevent undetected entry;
- Allow safe egress.

6. Security doorsets form part of an integrated site security system. It is paramount their performance is considered in conjunction with other aspects of site security such as CCTV, lighting, detection systems, guarding and security procedures.

7. More information can be accessed by following the link below.

8. . https://www.cpni.gov.uk/doors

9. Any external security doorsets that are infrequently used should be internally secured (having ensured compliance with relevant fire safety regulations).

Windows

10. There are many types of windows, each operating in a unique way. Irrespective of this, a number of key features affect the security resistance afforded by windows. These should be taken into account when determining a window's likely resistance to forced entry; undetected or otherwise. These features are as follows:

- Mode of opening;
- Materials used to manufacture the window and how they are assembled;
- Locking mechanism;
- Hinges;
- Glazing method and type of glazing used; and
- Installation method.

11. If there is not already one in place, a good quality alarm system should be fitted to external windows. Further information regarding the security of domestic windows, can be found accessed via the CPNI website https://www.cpni.gov.uk/windows-and-window-protection-systems

Perimeter Security

12. Fences and walls will protect a site by:

- Deterring and delaying intruders;
- Marking a boundary;
- Protecting guards and staff from surprise attack;
- Enabling the use of guard dogs;
- Acting as a barrier to vehicles;
- Enabling the use of Perimeter Intruder Detection Systems (PIDS);
- Protecting against explosive attack.

13. Walls have the following additional uses:

- To protect against rockets, small arms, blast and fragments;
- To prevent observation of guard and patrol movements; and of other protective measures;
- Creating a 'stand-off' for any explosive device.

14. Fences and walls provide only limited delay against intruders; the least secure types can only delay a skilled intruder for a few seconds. A perimeter barrier intended to impede intruders should, therefore, combine a fence or wall with security lighting and human or electronic surveillance, e.g. a PIDS and CCTV.

15. Toppings are designed to increase the difficulty of climbing a fence or wall by increasing the overall height of the fence and also snagging and/or cutting the intruder. It should not aid an intruder by providing a firm hand or foothold. There are many different types of topping available including, barbed tape coils, barbed wire and spikes.

Gates

16. Gates must be compatible with and at least as strong as the perimeter fence. Hinges should have been engineered to prevent a gate being lifted off. A good security padlock of hardened steel should be used. Make sure the bar on any standard padlock is as short as possible and, ideally, the padlock should have a shroud with hardened steel. This makes it harder to open using cutting equipment and so buys time.

Lighting

17. Lighting can be an important security measure, but may in fact assist an intruder if used incorrectly. Ideally a security lighting system should:

- Deter intrusion, or at least reduce an intruder's freedom of action;
- Assist in the detection of intruders either by direct vision or by CCTV;
- Conceal guards and patrols.

18. The guard plan, CCTV and lighting requirement must be carefully co-ordinated taking account of the following rules:

- Lighting should not illuminate guards or patrols;
- Lighting should support guards and CCTV;
- It should not cause nuisance or hazards;
- It must be cost-effective and compatible with site conditions;
- An even level of illumination is more important than absolute light levels. This prevents dark areas in which intruders can lurk.

19. Perimeter lighting. This provides a well-lit area in the form of a strip around the perimeter. To be effective an intruder must have to pass through this well-lit area. The lighting column should not be useable as an aid to scaling the fence.

20. Area Lighting. This generally refers to the areas around buildings within the protected area. The aim is to produce even illumination without dense shadows.

21. Floodlighting. This is used to cast a strong light on the walls of buildings so that intruders are visible either in silhouette or by the shadows which they cast. Lights should be mounted up high, out of reach of intruders.

22. Gatehouse Lighting. This is used at the perimeter entrance and gatehouse in order to:

    - Reveal approaching vehicles and pedestrians and allow guards to identify them, verify passes, carry out vehicle searches, and

    - Conceal guards within the gatehouse while allowing them to see out.

23. Topping up Lighting. This is used to eliminate dark areas not adequately lit by area lighting or floodlighting. Such areas may be lit locally by small light fittings (eg bulkhead fittings) or from a distance by narrow angle floodlights.

CCTV

24. CCTV should form only part of a whole security system and should not be used on its own. It cannot completely replace security staff, but it may enable fewer to be used, their employment on a wider range of duties, or use of an off-site guard/response force. In its simplest form a CCTV system consists of a television camera joined by a transmission link such as a cable to a monitor sited in the guard room or central control point. More complex systems use several cameras and monitors or a single monitor with a switching system to display camera pictures in sequence. Additional facilities such as recorders, automatic switching in response to an alarm signal may be used. Additional information on CCTV systems can be accessed via the CPNI website http://www.cpni.gov.uk/advice/Physical-security/CCTV/. Systems may also require registration under data protection legislation.

25. Using CCTV can help clarify whether a security alert is real and is often vital in post-incident investigations, but only if the images are good enough to identify what happened and provide admissible evidence in court.

26. External lighting will help the effectiveness of security staff and improve the capabilities of CCTV systems if it is carefully designed and used. Effective CCTV systems may help to deter a terrorist attack or even identify planning activity. Good quality images can provide crucial evidence in court.

27. Security staff who are employed in-house are not required to be Security Industry Authority (SIA) licensed. If contract security staff, are employed they must be licensed by the SIA. This includes operating CCTV equipment and applies regardless of whether CCTV cameras are fixed or have a pan, tilt and zoom capability and where operators:

    - Proactively monitor the activities of members of the public whether they are in public areas or on private property;

    - Use cameras to focus on the activities of particular people either by controlling or directing cameras to an individual's activities;

    - Use cameras to look out for particular individuals;

    - Use recorded CCTV images to identify individuals or to investigate their activities.

28. CCTV Considerations.

    - Are the CCTV cameras regularly maintained?

    - Do the cameras cover the entrances and exits to a building?

- Do the cameras cover critical areas such as where Class 7 radioactive material is stored?

- Are the images stored in accordance with the evidential needs of the police and with data protection legislation? Duty holders can obtain advice from their local CTSA concerning the evidential needs of the police.

- Could an individual be positively identified from the recorded images on the CCTV system?

Class 7 Non-High Consequence Dangerous Goods

29. Parts of the site where dangerous goods are stored are to be secured. A safe may be adequate for the secure storage of small quantities of dangerous goods. For slightly larger quantities it might be sufficient to install a secure cage, constructed of weld-mesh material with a locking door, possibly to British Standards such as BS1722:2006 (fencing) and BS3621:2007 (locks) rather than trying to secure an entire building. Access to secure storage areas should be limited to appropriately recruited and trained staff.

30. If Class 7 non-high consequence dangerous goods are stored in vehicles or secure buildings, then chain link fencing may be used provided the vehicles themselves are adequately secured. There may be occasions when fencing or access control may not be required at all. For example if:

    - Vehicles are fitted with high quality security features, such as high security locks, grilles and anti-theft equipment;

    - Trailers cannot be detached and/or towed away; or

    - Bollards to prevent unauthorised vehicle access/egress are present.

Class 7 High Consequence Dangerous Goods

31. At sites where small quantities of Class 7 high consequence dangerous goods are stored, localised storage may be appropriate, or perhaps ‘double layered’ security arrangements such as a safe within a cage.

32. Perimeter security of Class 7 high consequence dangerous goods sites should comprise good quality weld mesh or palisade fencing, preferably constructed to BS1722:2006 standard. Access should ideally be controlled using photographic identification.

33. Security fencing is best fitted with intruder detection equipment that alerts a security control point. There is no requirement for PIDS in the regulations, but on opening of the site each day, procedures should include a check of the secure storage and associated holding. If Class 7 radioactive material has been stolen, or there are signs of interference or attempted theft, this is to be reported to the Police immediately.

Vehicle Communications – High Consequence Dangerous Goods.

34. Vehicles should be fitted with radios or some other means of two-way communications between the driver and their base. Panic buttons can be fitted that a driver presses if under duress, possibly in a hi-jack situation. This will send an alert to the operator so the Police can be contacted. During transport, the carrier should provide, in the vehicle, a means for personnel to communicate with a designated contact point as specified in the security plan.

Dangerous Load Cards – High Consequence Dangerous Goods.

35. Drivers carrying Class 7 high consequence dangerous goods should carry a dangerous load card. It does not specify the vehicle, the driver, or the type of high consequence dangerous goods being carried. A driver should only produce this card if they are stopped by a Police or Driver and Vehicle Standards Agency (DVSA) officer and are suspicious about the bona fides of the officer. The card tells the Police and DVSA that the driver will not open the vehicle until the officer's identity has been verified. The Police and DVSA have approved this procedure. The carrier will need to decide if any load is of high consequence, based on information provided by the consignor. The dangerous load card can be downloaded from the DfT website via this link: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/338874/dangerous-load-card.pdf.

Temporary Storage

36. The following arrangements are to be in place at areas within temporary storage terminals, temporary storage sites, vehicle depots, berthing areas and marshalling yards used for the temporary storage during carriage of Class 7 dangerous goods:

- Storage areas shall be properly secured. If located in a building, appropriate physical security measures are to be in place. If in a cage, it is to be constructed using suitable materials, and padlocks used to secure such cages should be good quality and fitted with a protected shackle.

- Temporary storage areas are to be well lit and, therefore, adequate lighting is to be in place at areas where dangerous goods are stored temporarily during the course of transport.

- Areas used for the temporary storage of Class 7 dangerous goods during carriage are to be properly secure and where possible not accessible to the general public. When inspecting the security of entry points, the physical security of emergency exits and disabled access is also to be checked.

Storage of Vehicles

37. Overnight storage of vehicles in locked buildings is often only practical for light vans. Heavy commercial vehicles need more space, and are generally kept outside. Vehicles should not be left parked against perimeter fences. Although the fence may protect the rear doors from being opened, the top and sides remain vulnerable. If Class 7 high consequence dangerous goods are pre-loaded for departure they are more vulnerable if left overnight. Wherever practicable, vehicles should not be left loaded overnight or for any significant period of time before departure. If vehicles have to be pre-loaded for operational reasons, they should be left in a secure location, locked, with any alarms or immobilisers set and the keys kept in a safe place.

Secure Vehicles

38. All vehicles should have some form of immobilisation. Has the vehicle been fitted with an alarm and immobiliser? Information on security devices for vehicles can be found on the Thatcham website via the following link:. https://www.thatcham.org/what-we-do/security/

Physical Vehicle Security

39. Are the vehicles fitted with strong high security locks? Many security locks depend on the driver to operate them manually. 'Slam locks' can be fitted to load space access points in commercial vehicle bodies. Are vehicles fitted with a bulkhead dividing the driver/passenger area and the load compartment in panel vans, in order to isolate goods in the load compartment? A bulkhead fitted in a panel van means that access is only through the side or rear loading doors, which can be secured with additional locks.

40. Bulkheads come in a variety of materials, such as solid steel, plywood or steel mesh. Correctly fitted mesh bulkheads can give adequate security, but still allow thieves to see the goods, which may make a break-in more likely. Solid bulkheads are better.

Immobilisers

41. Immobilisers aim to render the vehicle and/or trailer immovable. Immobilisation systems can be used in isolation or integrated into an alarm system. Virtually all insurance approved alarm systems will incorporate, as standard, some form of immobilisation as part of the overall security system.

42. Wheel clamps are an effective form of immobilisation, especially on the smaller wheels of light commercial vehicles. Wheel clamps for large commercial vehicles are heavy and cumbersome. Drivers have to fit them and lock them into place, so the risk that they either will not fit them, or that they will fit them incorrectly (particularly at night), is higher than for other vehicle immobilisation devices.

43. To immobilise an articulated trailer, kingpin or trailer leg locks are the most common and effective way. Kingpin locks are a heavy hardened steel clamp or cover, which fits round or over the kingpin and locks it in position. It makes it impossible for the kingpin on the trailer to be coupled with the fifth wheel coupling on the tractor unit. Fitting kingpin locks can be a difficult and dirty job. Trailer leg locks are an alternative. Both kingpin and trailer leg locks are manually operated devices so the driver has to put them on and lock them into position.

Alarms

44. Immobilisation does not stop a criminal from vandalising a vehicle or unloading it where it stands. Alarm systems do two things:

    - they create a loud sound that provides both a warning and a deterrent; and
    - when fitted in conjunction with a vehicle immobiliser, they ‘buy time’.

45. An alarm system powered off the vehicle’s own battery may be perfectly sufficient for light commercial vehicles in low risk operations, where the battery is locked under the bonnet. Large commercial vehicles with exposed batteries on the chassis require a back-up facility for alarm systems. There is little point in having an alarm system that can be rendered inoperable merely by disconnecting the battery terminals.

46. Key switches turn a system on or off (automatic systems ‘pulse’ to allow the driver to re-enter the cab or to unload).

47. In the case of high risk loads, independent alarm security may be fitted to the tractor unit and the trailer, tank or container. Where a single shared alarm system covers the tractor and the trailer, tank or container when they are coupled, the back-up battery may be on the trailer, tank, or container. It provides independent protection when the trailer, tank, or container is free-standing. However, this may leave the tractor without any alarm protection at all when separated. In this case, it is important to immobilise the tractor.

Tracking systems

48. When appropriate and already fitted, the use of transport telemetry or other tracking methods or devices should be used to monitor the movement of high consequence dangerous goods.

49. Some tracking system manufacturers offer 24 hour monitoring via a movement sensor linked to the tracking unit. The system manufacturer is then able to alert the owner if the

vehicle is illegally moved. This means a faster response to theft. Some on-board tracking systems offer additional features, which can monitor the product levels in tankers for example. These enable the operator to have live visibility of the vehicle's location as well as the quantity of product unloaded. Portable tracking devices are available that can be fitted into a load space, a shipping container for example, which can send an alert if the doors are opened.

Cameras on vehicles

50. Cameras are regularly used on the back of goods vehicles to help the driver manoeuvre the vehicle. These are also a valuable covert measure to monitor the security of the load. More frequently now, forward facing cameras are being fitted.

Key Control

51. Parked vehicles should be locked when not in use and the keys kept in a lockable container. This can either be a key safe where any missing keys can be noted at a glance or, if required, a secure metal cabinet. Duplicate keys should have similar protection. The room in which keys are secured should also be protected from access by unauthorised personnel.

52. In respect of storage areas for Class 7 dangerous goods, effective key control is critical in ensuring that resistance to forced entry provided by a doorset is not undermined by unauthorised people gaining access to the keys. It is very important that there are procedures in place to control the issue of keys and to ensure that the loss or theft of keys is quickly identified and reported. Each key should be stamped with a number or symbol to relate it to a particular lock location or system.