ONR GUIDE			
PROTECTION OF NUCLEAR TECHNOLOGY AND OPERATIONS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-7.3 Revision 0		
Date Issued:	March 2017	**Review Date:**	March 2020
Approved by:	David Pascoe	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19077. (2017/110600)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 03/17

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1).

1.2 The term 'security plan' is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's arrangements for the protection of nuclear technology and operations. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The term 'dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil nuclear licensed sites and other nuclear premises subject to security regulation, a 'developer' carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

3.2 NISR defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers CS&IA to be an important component of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 Fundamental Principle L of the CPPNM refers to confidentiality. The importance of issues relating to cyber security and information assurance is also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 3: Legislative and Regulatory Framework – 3.3 The legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime:

    g) Provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets.

    h) Ensure that prime responsibility for the security of nuclear material, other radioactive material, associated facilities, associated activities, sensitive information and sensitive information assets rests with the authorised persons.

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12 A nuclear security regime ensures that each competent authority and authorised person and other organisations with nuclear security responsibilities contribute to the sustainability of the regime by:

    h) Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times.

4.3 A more detailed description of the elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 2).

4.4 The IAEA also publishes Implementing Guide NSS No. 23-G 'Security of Nuclear Information' (Reference 8) and Technical Guidance NSS No. 17 'Computer Security at Nuclear Facilities' (Reference 9).

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder's security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder's submission demonstrating they have effective processes in place to achieve Security Delivery Principle 7.3 – Protection of Nuclear Technology and Operations, in support of FSyP 7 – CS&IA. The TAG is consistent with other CNS TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 5) describes the Cabinet Secretary's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs. This ensures that dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, SNI and the employment of appropriate personnel security controls both on and off nuclear premises.

5.3 The Classification Policy (Reference 6) indicates those categories of SNI, which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

6.1 SNI is information relating to activities carried out on or in relation to civil nuclear premises which needs to be protected in the interests of national security. Information and associated assets comprise data in various formats (such as digital, hard copy and knowledge) as well as information technology and operational technology (equipment or software). It is a dutyholder's responsibility to determine which information and associated assets are considered relevant. However, hard copy SNI, computer based systems that store, process, transmit, control, secure or access SNI should always be included; and technology stored or utilised on the premises in connection with activities involving nuclear or other radioactive material relating to either nuclear safety or nuclear security, should always be considered. Appendix 1 of TAG 7.2 provides a description of SNI and a flow chart to assist in its identification.

6.2 Information and associated assets should be resistant to increasingly complex cyber threats and should also be resilient, in terms of being able to recover operational status quickly in the event that these threats are able to impact a system.

6.3 The protection of nuclear technology and operations encompasses all relevant aspects of:

- System categorisation and critical dependencies
- Achieving the Cyber Protection System (CPS) outcome and response strategy
- Achieving the cyber security posture
- Security control principles
- Resilience and assurance of controls
- Cyber security awareness, training and skills.

Regulatory Expectations

6.4 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies arrangements for the protection of nuclear technology and operations.

FSyP 7 - Cyber Security and Information Assurance	Protection of Nuclear Technology and Operations	SyDP 7.3
Dutyholders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities.		

7. SYSTEM CATEGORISATION AND CRITICAL DEPENDENCIES

System Categorisation

7.1 Dutyholders should be aware of the different types of technology that deliver functions as part of the nuclear security and safety related equipment and software operating at sites. The safety aspects of these systems are defined in the Safety Case which identifies a safety functional category and safety classification for each system. However, it is also important not just to consider the potential consequences of what

the systems are designed to do, but also what they are capable of doing if compromised. Designers often think in terms of what the system is programmed or intended to do, but adversaries tend to think in terms of what the system can be made to do. Therefore, dutyholders also need to understand the security aspects of these systems in terms of how they deliver operational functions and the role they play in protecting the public from the risks associated with a radiological event caused by malicious events, including cyber-attack.

7.2 Dutyholders should be able to differentiate between the types of technology using a categorisation methodology for cyber security. This should identify that there are different technologies in use from standard Information Technology (IT) systems, both in the way in which they operate and because the consequence of their failure, compromise or sabotage can be more severe. An important component of the categorisation methodology is consistency; it should be an auditable and repeatable process that can incorporate changes over time. SyAPs Annexes F and G provide a framework with which, dutyholders' categorisation methodologies and processes should align.

7.3 This approach should identify a system's operational security value and can be used to inform risk management decisions. There are a number of widely available risk assessment methodologies that can be used as the basis for the dutyholder risk assessment and these include:

- ISO27005:2011
- IEC (ISA) 62443-3-2 Security risk assessment and system design
- US National Institute of Standards and Technology SP 800-30
- Octave Allegro
- Information Systems Audit and Control Association: Control Objectives for IT 5
- Information Security Forum – Information Risk Analysis methodology; and
- Open Group FAIR Risk Analysis Standard

7.4 The scope of the categorisation methodology should include all technology for which the dutyholder is responsible, including that operated by partners, service providers and suppliers. The types of systems in scope of the categorisation methodology should include but are not limited to:

- Computer Based Systems Important to Safety, namely, computer based safety protection systems and computer based safety related systems
- Basic Process Control & Instrumentation Systems
- Systems used in connection with activities involving Nuclear Material and Other Radiological Material
- Computer Based Security Systems
- Nuclear Material Accountancy and Control Systems
- Systems relating to aspects of Vital Areas
- Essential communications and reporting systems
- Systems holding code repositories
- Mobile systems providing critical support functions

- Systems holding details of security risks or vulnerabilities
- Systems holding SNI
- Other digital and information systems as relevant

7.5 Section 4.5 of SyAPs describes a security functional categorisation and classification scheme for protective security systems. The intention is that the importance of the security functions needing to be delivered is clearly understood and systems are classified in accordance with the functions they deliver. In that regard, dutyholders should also take account of any safety function categorisation and classification scheme.

7.6 The benefit of applying a functional categorisation and classification scheme is that dutyholders should be guided to ensure that cyber security is integral to the way the systems are designed (for example, through incorporation of non-computerised elements within the architecture or the use of data diodes to ensure non-interference between systems of different classification), implemented and operated. Security by design is particularly significant since it sets the relevance and importance of security into the system at the outset and becomes part of the operational culture. It is highly likely that that the methodology for digital assets categorisation will have a strong correlation with security functional categorisation.

System Dependencies

7.7 The categorisation and methodology for technology should also highlight where interdependencies between systems exist. Dutyholders should be aware of the need to understand such interdependencies, not only because of potential complications in supporting and upgrading systems, but also because of cyber security risks reflected from one system to another.

7.8 To support this, dutyholders should understand the process interactions and information flows from, to and between technology and those flows should be a part of the categorisation and classification methodology.

7.9 The methodology should identify dependencies on other assets that support the technology. These other assets may comprise mobile devices or other forms of information system, whose failure or compromise would impact operations.

Inspectors should consider:

- Is there a clear understanding of what technology is in scope?
- Is an effective categorisation methodology in place that is appropriate to the organisation?
    - Is it aligned with the framework provided in SyAPs Annexes F and G?
    - Is it auditable and provides consistent results?
    - Does this cover partners, service providers and suppliers?
- Have system dependencies been identified adequately?

8. ACHIEVING THE CYBER PROTECTION SYSTEM OUTCOME AND RESPONSE STRATEGY

8.1 Following categorisation, the security outcome and response strategy that the CPS for each asset in scope should achieve is determined by the CPS Outcome and Indicative Security Posture Table at SyAPs Annex H. The required effects of both the CPS outcome and response strategy are then defined in the table at SyAPs Annex I.

8.2 When used together, these two tables define and describe what the CPS must be designed to achieve but do not provide prescriptive statements on how to do so. Therefore, whilst dutyholders are expected to demonstrate in their security plan that the CPS delivers a specified outcome and response, they have considerable flexibility in the design, allowing the adoption of innovative solutions that are aligned to business processes and operations. Additionally, dutyholders should bear in mind that applying additional cyber controls in order to achieve an outcome may not be the most pragmatic solution (particularly where Outcomes 1 or 2 are required). Instead, it may be possible to reduce the category of asset, for example, by modifying a process, configuration or the application of additional, segregated and/or diverse systems.

8.3 A more detailed description of the four CPS outcomes is provided below.

CPS Outcome 1

8.4 CPS Outcome 1 is the most demanding outcome for protecting technology. It requires the CPS to be able to prevent hostile penetration of the technology by the relevant threat actor through the implementation of sufficient cyber protection controls. To be effective against higher-skilled threat actors, a CPS designed to deliver Outcome 1 will typically be securely architected, hardened for deployment and robustly defended by advanced Intrusion Protection Systems (IPS) and Intrusion Detection Systems (IDS). It will also require all maintenance and management activities to be undertaken in a secure manner (e.g. patching kept up to date), with any changes to system configuration being proven not to be ill-conceived, or executed before deployment and subject to testing from a security perspective.

8.5 In order to secure confidence in the ability of a CPS to achieve Outcome 1, it is important that the security integrity of the system is subject to routine and frequent assurance, including utilising demonstrable techniques such as simulated attack (penetration) testing using the level of cyber skills and capabilities associated with the relevant threat actor.

8.6 Dutyholders should also consider that it may be possible for the higher skilled threat actors to develop attack methodologies/techniques that are capable of defeating even advanced protection measures. Therefore the CPS may require support from a Cyber Emergency Response Team (CERT) to respond to, and recover from, a cyber-attack. The team should include technical experts and specialist tools to support incident analysis and help to inform and implement appropriate short term containment measures to reduce the immediate impact of an incident or to prevent it getting worse and spreading to other areas.

8.7 A CPS required to meet Outcome 1 should demonstrate a complete suite of controls designed to minimise risks posed by the insider threat. These controls may include technical measures such as secure configuration and continuous system monitoring, and, procedural elements such as two-person principles and a comprehensive searching regime designed to minimise the risk of introduction of prohibited items (e.g. portable media within sensitive areas) or unauthorised removal of SNI.

CPS Outcome 2

8.8 CPS Outcome 2 is also highly demanding. It should offer significant protection and an assured real time detection capability of cyber-attack against the technology. This differs from the expectation in Outcome 1 in that the threat actor may be able to penetrate the asset before the response actions have successfully defeated the attack.

8.9 A CPS designed to deliver Outcome 2 should be protected by IDS of technical quality matched to the skill level of the relevant threat actor and supported by an appropriate IPS. As for Outcome 1, to be effective against the higher skilled threat actors, it is highly likely that the CPS will require support from a Cyber Emergency Response Team (CERT) to respond to, and recover from, a cyber-attack.

8.10 A CPS required to meet Outcome 2 should demonstrate a rigorous suite of controls designed to counter risks posed by insider activity.

CPS Outcome 3

8.11 For Outcome 3, the focus of the CPS is on providing assurance that a cyber-attack on technology will be detected in real time. A security system designed to deliver Outcome 3 is typified by IDS of technical quality matched to the skill level of the relevant threat actor. However a CPS meeting Outcome 3 should also be supplemented by cyber protection measures such as IPS and provision of appropriate capability to effect response and recovery, (for example through a specialist business unit or contractor with the appropriate skills available 'on call').

8.12 A CPS required to meet Outcome 3 should demonstrate a suite of controls designed to reduce the risks posed by insider activity.

CPS Outcome 4

8.13 CPS Outcome 4 requires the system to be able to facilitate effective post event investigation and forensic analysis. A security system designed to deliver Outcome 4 is likely to be characterised by technological and procedural measures based on the principles of confidentiality, integrity and availability that ensure accurate data (e.g. Security Incident and Event Management) logging, allowing forensic analysis by specialists capable of establishing cyber as a likely root cause. This should be supported by notification to the relevant authorities to enable counter compromise action to be implemented and selection of suitable additional controls minimise the risk of reoccurrence.

8.14 A CPS required to meet Outcome 4 should demonstrate appropriate controls designed to manage the risks posed by insider activity.

Inspectors should consider:

- Has the dutyholder selected the correct CPS outcome(s) for the technology concerned?
- Are claims and arguments made in respect of achieving the CPS outcomes supported by sound evidence?(e.g. through conduct of a structured and systematic approach to advanced threat penetration testing such as the CBEST approach used in the financial sector or expert judgement from organisations such as the National Cyber Security Centre (NCSC))

- Has there been appropriate interface between the dutyholder with all organisations providing elements of the CPS?

9. ACHIEVING THE CYBER SECURITY POSTURE

9.1 The CPS Outcome and Indicative Security Posture Table at SyAPs Annex H details three postures of 'Routine', 'Robust' and 'Fortified'. These postures represent increasingly comprehensive suites of CPS controls designed to reduce the risk that a cyber-attack on technology will be successful. The postures are applied using a graded approach according to the categorisation of the technology concerned.

9.2 The table at SyAPs Annex J provides a description of how the postures relate to the CPS functions of Identify, Protect, Detect, Respond and Recover, that dutyholders may incorporate within their CPS design in order to achieve defence in depth. Annexes H and J are intended to be used in conjunction and there is likely to be a correlation between the security posture of the CPS function and the security classification (refer to Key Security Principle 5.2 of SyAPs) of the controls that achieve it.

9.3 The security postures are not prescriptive and are intended to give a broad indication of the levels of defence in depth, rigour and risk mitigation that are expected to protect nuclear and other radioactive material and facilities against cyber-attack. Accordingly, a dutyholder may be able to justify a lower posture (for example, by adoption of a novel solution, or due to the nature of the technology being protected) provided the outcome is achieved. One approach may be to increase the security postures of other functions. However in these cases, it is likely that inspectors need to scrutinise an extensive body of evidence to support their assessment decision, particularly where the gap is large (e.g. 'Routine' is adopted where 'Fortified' is indicated).

10. SECURITY CONTROL PRINCIPLES

10.1 Once technology and any associated process interactions and information flows have been identified and characterised, appropriate control measures can be designed and implemented to achieve the relevant CPS outcome. Dutyholders should implement security controls based upon an appropriate risk assessment methodology as this will focus security resources on areas of greatest risk and provide a traceable and repeatable process for effective risk management. Care needs to be taken when introducing measures to mitigate cyber security risks to technology to ensure that they do not compromise or otherwise conflict with operational performance. This may require pragmatic judgements to be made in the application of risk management criteria, particularly for existing systems and equipment. Specific guidance on the application of cyber security control measures to computer based systems important to safety is available in TAG NS-TAST-GD-046 (Reference 10).

10.2 There are a number of risk treatment methodologies which dutyholders may consider appropriate. Most of them are based around risk treatment involving, Treat, Transfer, Tolerate, Terminate and Take the Opportunity mechanisms. Whichever methodology is chosen there should be traceability of which risks are to be mitigated, in what priority order and how; it should also align with the framework described in Annexes F to J of SyAPs.

10.3 A defence in depth and diversity by design approaches should be adopted where appropriate and dutyholders should implement cyber security controls that are current and relevant. In that regard, dutyholders should be particularly aware of the risks posed to technology from portable media devices. As described in the above section, the controls should detect threats, protect against identified risks, deter malicious intent

and provide measures to improve system resilience and recovery so that disruptions to operations are appropriately mitigated.

10.4 Operational systems may include older technologies where security may not have been designed in from the outset. In such cases dutyholders should demonstrate awareness of this and compensate for it with other security measures (which may include additional physical security or procedural controls). Whenever any such system is replaced or upgraded then dutyholders should use the opportunity to ensure security is an intrinsic part of the change.

10.5 Risks change over time and the mechanism for assessing and implementing controls should be able to respond effectively to new requirements. As with other aspects of change management, changes to security controls should be made on compatible test and development systems first.

10.6 Libraries of cyber security controls are widely available and these include: ISO standards (ISO27001, 27032 etc, IEC 62443, CoBIT, NIST Framework, SANS / CPNI Top 20, NCSC 10 Steps to Cyber Security.

10.7 Dutyholders should consider the following cyber security control measures (taken from the CIS 20 Critical Controls (Reference 11)):

- Inventory of authorised and unauthorised devices
- Inventory of authorised and unauthorised software
- Security configurations for hardware and software on mobile devices, laptops, workstations and servers
- Continuous vulnerability assessment and remediation
- Controlled use of administrative privileges
- Maintenance, monitoring, and analysis of audit logs
- Email and web browser protections
- Malware defences
- Limitation and control of network ports, protocols and services
- Data recovery capability
- Secure configurations for network devices such as firewalls, routers and switches
- Boundary defence
- Data protection
- Controlled access based on the need to know
- Wireless access control
- Account monitoring and control
- Security skills, assessment and appropriate training to fill gaps
- Application software security
- Incident response and management
- Penetration tests and red team exercises

10.8 Dutyholders should recognise that standard IT security controls such as patching, may not be able to be implemented on Operational Technology (OT) systems completely or in the way that they would be for IT systems. Where a specific control cannot be fully implemented it should be balanced by a defence in depth approach that compensates the weakness of one control with other mechanisms. Where there are control deficiencies for whatever reason, this should be reflected using the dutyholder's risk management function.

10.9 When security controls can be implemented, the specific characteristics of OT systems should be taken into account to ensure that they do not have an adverse effect on operations. For example when a software patch is available, a suitable change management process should be applied to ensure that it does not adversely affect operations, specifically the performance characteristics of security, safety and/or safety-related systems.

10.10 Dutyholders should ensure that the change management process takes account of essential updates required to technical security controls to reflect technology changes or a revised set of controls to reflect business changes and changes to threats. A security manager, or other role with security responsibilities, should be a member of any change management group to give subject matter advice as required.

Inspectors should consider:

- Is the selection of technical cyber security controls based upon a risk assessment and aligned with the SyAPs?
- Are controls used within a defence in depth approach?
- Does the dutyholder have an adequate mechanism for testing control implementations?
- Are control implementations actively managed by a monitoring process that reflects changes in risk?
- Can the control assessment and implementation process scale up as required?

11. RESILIENCE AND ASSURANCE OF CONTROLS

Cyber Security Resilience

11.1 Dutyholders should consider that information and associated assets will be subject to cyber-attack of some description at some point. Therefore, dutyholders should design and implement technology that is resilient to cyber-attacks, responding effectively. The requirements for system resilience should be based upon risk assessment and be closely aligned to plans for Business Continuity and Disaster Recovery.

11.2 Resilience in system architecture and functions and the ability to both respond and recover from a cyber security incident are crucial. An example of the means by which cyber resilience can be improved can be to incorporate non-computerised platforms and elements across one or more layers within the architectural design of systems. Accordingly due consideration should be given to these aspects when planning security measures.

11.3 Cyber resilience relies upon effective system and security monitoring and a swift response to a cyber security incident (see TAG 7.5 – Preparation for and Response to Cyber Security Incidents).

Assurance of Security Controls

11.4 Dutyholders should have an adequate mechanism in place for providing assurance of security control effectiveness. The process should include ongoing monitoring as part of the operational management function. The process should provide feedback from assurance into the risk management process since this underpins risk management decisions.

11.5 The dutyholder assurance mechanism should identify the system components and functions that require some form of assurance so that appropriate planning of activities can take place. The mechanism should provide for different types of assurance for different system elements and different stages of system operation. It should also provide for a structured approach that will cover all system aspects (e.g. component, sub-system, system and management).

- Using components that have been assured
- Testing of system technical configurations
- IT Health Checks
- Vulnerability scans and penetration tests
- Red team cyber security exercises

11.6 Technical assurance should be planned to continue at specified points throughout the lifetime of the digital and information assets in scope.

11.7 The dutyholder mechanism should include assurance of the effectiveness of operational procedures, people and places. This can be carried out as team exercises (either run within the organisation or by independent outside experts). Such exercises should be closely aligned to incident management and disaster recovery assurance.

11.8 Assessments of the effectiveness of assurance can be made by risk managers. The Accreditor function is often used to provide independent assessments.

11.9 Assessments of the effectiveness of assurance of IT/OT systems should be justified in independently verified documentation, which identifies, risk assesses, and details the risk controls necessary to manage and/or mitigate cyber security risks to each computer based system, to a level acceptable to the organisation. Each justification may apply to multiple systems of the same category or class that are utilised for the same or similar purposes.

Inspectors should consider:

- Has the categorisation methodology been used to help define the level of assurance required?
- If component assurance is required, has the use of evaluated products been considered?
- If technical testing is planned is it being conducted by suitably qualified and experienced personnel?
- Is assurance (all types) planned for the lifetime of the information asset?
- Is each IT/OT system supported by independently verified documentation that identifies the risks to that system and confirms that those risks have been mitigated to an acceptable level?

12. CYBER SECURITY AWARENESS, TRAINING AND SKILLS

12.1 People play a vital and critical role within cyber security. Dutyholders should therefore have a comprehensive and well communicated mechanism for ensuring that all personnel receive training that covers awareness of the organisation's cyber security threats and their role in mitigating them. Training should ideally be role specific for technical, non-technical and security personnel.

12.2 Awareness training should commence at induction for all personnel at all levels in the organisations. This should include partners, service providers and suppliers. Such training should include an overall awareness of cyber security threats and the ways in which attacks can be delivered (e.g. use of social engineering techniques to gain intelligence). It should also provide an overview of how the organisation is managing risks.

12.3 The training should be updated and reinforced at regular periods, as appropriate to keep pace with changing technology and threats.

12.4 There are many approaches for delivering effective training and a structured multi-media approach should be considered in order to provide a useable security knowledge base supported by different delivery mechanisms such as e-learning, Computer-Based Training packages, routine internal briefings, mailshots, newsletters and on-line tests such as phishing e-mails. Further guidance on competence management is available in security delivery principles 3.1 – 3.4 and associated TAGs.

12.5 Operational technical or security roles, such as system administrators, control room operators or auditors should have relevant security skills and qualifications in their job description. Staff should receive security training directly relevant to their responsibilities.

12.6 Staff should be encouraged to gain assessment of security skills including through formal qualifications. There are many schemes available to support recognised qualifications such as the NCSC Certified Professional (CCP) scheme.

Inspectors should consider:

- Have the security aspects of roles in the organisation been defined?
- Have roles that require security qualification and/or experience been defined?
- Is security awareness training updated and reinforced regularly?
    - Is there a mechanism for evaluating training effectiveness?

13. REFERENCES

1. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403

2. **IAEA Nuclear Security Series No. 13.** Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (**INFCIRC/225/Revision 5**). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.

3. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

4. **Convention on the Physical Protection of Nuclear Material (CPPNM)** https://ola.iaea.org/ola/treaties/documents/FullText.pdf

5. **HMG Security Policy Framework**. Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

6. **NISR 2003 Classification Policy** – Trim Ref. 2012/243357.

7. **Security Assessment Principles** – Trim Ref. 2017/121036

8. **IAEA Nuclear Security Series No. 23-G**. Security of Nuclear Information http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf

9. **IAEA Nuclear Security Series No. 17**. Computer Security at Nuclear Facilities http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

10. ONR ND-TAST-GD-046. Computer Based Safety Systems http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-046.pdf

11. **Critical Security Controls V6.0.** The Centre for Internet Security. https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

14. GLOSSARY AND ABBREVIATIONS

CBSIS	Computer Based Systems Important to Safety
CERT	Cyber Emergency Response Team
CNS	Civil Nuclear Security
CPS	Cyber Protection System
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
IDS	Intrusion Detection System
IPS	Intrusion Protection System
IT	Information Technology
NCSC	National Cyber Security Centre
NISR	Nuclear Industries Security Regulations
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
OT	Operational Technology
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyAPs	Security Assessment Principles
TAG	Technical Assessment Guide