1

ONR GUIDE			
PREPARATION FOR AND RESPONSE TO CYBER SECURITY EVENTS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-7.5 Revision 1		
Date Issued:	February 2018	**Review Date:**	March 2020
Approved by:	Matt Sims	Professional Lead	
Record Reference:	TRIM Folder 1.1.3.776. (2017/408051)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

Published 03/18

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 to prepare for and respond to cyber security incidents. 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 and details that the State should establish requirements for protecting the confidentiality of information, the unauthorised disclosure of which could compromise the physical protection of nuclear material and nuclear facilities. The importance of issues relating to CS&IA 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). Paragraphs 3.53 to 3.55 specifically refer to issues relating to confidentiality.

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 7.5 – Preparation for and Response to Cyber Security Incidents 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 Security controls have defined roles such as preventative, detective, corrective and compensatory, and these are layered to mitigate cyber and information risks. One of the functions they perform is to detect and recover from a cyber attack. Accordingly dutyholders should have plans, policies and procedures in place to both reduce the vulnerabilities of their information and associated assets and to ensure that they are able to detect and manage cyber security incidents to recover operational functions.

6.3 Effective arrangements to prepare for and respond to cyber security incidents encompasses all relevant aspects of:

- Incident management strategy
- Incident management policy
- Incident management - identify, defend, detect, respond, recover
- Incident reporting
- Post incident procedures
- Assurance
- Business Continuity and Disaster Recovery (BC&DR)

Regulatory Expectations

6.4 The regulatory expectation is that the dutyholder will ensure that the security plan clearly details their arrangements to prepare for and respond to cyber security incidents in support of maintaining effective CS&IA arrangements.

FSyP 7 - Cyber Security and Information Assurance	Preparation for and Response to Cyber Security Incidents	SyDP 7.5
Dutyholders should implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber-attack), non-malicious leaks and other disruptive challenges.		

7. INCIDENT MANAGEMENT STRATEGY

7.1 Dutyholders should have an Incident Management Strategy (IMS) for the organisation. It is important that the scope is clearly defined and this should align with the scope of the risk management process developed in TAG 7.1 – Effective Cyber and Information Risk Management. The strategy should be informed by:

- a risk assessment (which is a part of the risk management process)
- the categorisation of any SNI, equipment and software in scope
- threat assessment information from organisations such as the National Cyber Security Centre (NCSC)

7.2 The strategy should fit within the framework of cyber security outcomes and postures as described in SyAPs Annexes H to J. It should also consider the wider aspects of BC&DR since the aims of those topics are aligned to incident management. Consequently, the scope of the strategy should include any relevant service providers and suppliers.

7.3 A governance structure should be in place to oversee the IMS, ensuring it is endorsed and signed off by the Board. This structure should be an integral part of wider risk management in the operations area.

7.4 The strategy should also provide for a monitoring and review process to ensure that it is meeting the objectives. This process should include the outputs from planned risk and vulnerability assessments.

Inspectors should consider:

- Does the organisation have an Incident Management Strategy (IMS)?
- Is the scope of the IMS clearly defined and does it align with the scope of the risk management process developed in TAG 7.1 – Effective Cyber and Information Risk Management?
- Is the organisation's IMS informed by:
  - A risk assessment (which is a part of the risk management process)?
  - The categorisation of any SNI, equipment and software in scope?
  - Threat assessment information from organisations such as the National Cyber Security Centre (NCSC)?
- Does the organisation's IMS fit within the framework of cyber security outcomes and postures as described in SyAPs Annexes H to J?

- Does the organisation's IMS consider the wider aspects of Business Continuity and Disaster Recovery (BC&DR)?
- Does the scope of the IMS include any relevant service providers and suppliers?
- Is the organisation's IMS endorsed and signed off by the Board?

8. INCIDENT MANAGEMENT POLICY

8.1 Dutyholders should have an Incident Management Policy (IMP) or similar that is derived from the IMS and which specifies how incidents are identified and managed. There is a considerable amount of advice on incident management processes available from a range of organisations (See references 11 – 15 for further guidance) so inspectors should assure themselves that whatever policy is developed it is tailored to the organisation and is adequate for the purpose. A possible approach is shown in the diagram below.

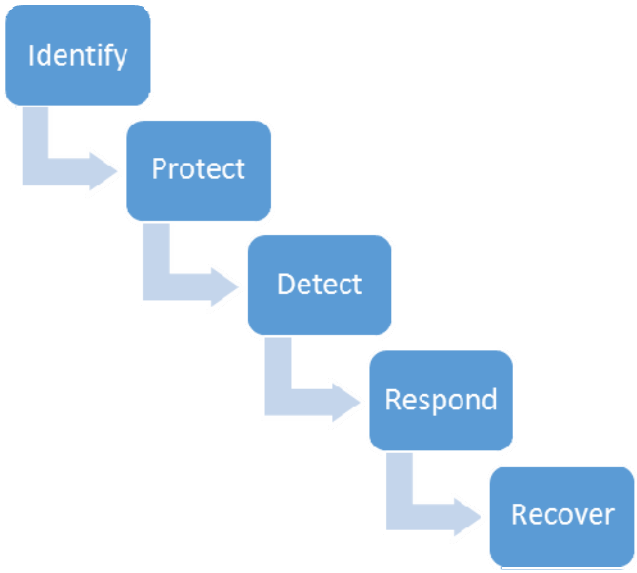

Figure 1: High level view of the Incident Management process

8.2 Inspectors should be assured that the policy is managed and implemented by Suitably Qualified and Experienced (SQEP) staff in the organisation to ensure that it is implemented and appropriate for the business.

8.3 Education and awareness is vital to policy implementation and arrangements should be in place to ensure that all personnel are aware of the policy and their role within it.

8.4 Regular reviews of risk and vulnerability assessments should be carried out as part of the ongoing risk management process to assess if the risks of incidents occurring have increased or not. Since risks change over time, arrangements should be in place to provide assurance that the policy can scale up to adjust the CS&IA measures in place quickly as a consequence of changes in risks or changes to the Government Response Level.

8.5 The IMP should consider the five functions listed in the sections below. This is not intended to be a prescriptive or definitive list and should be refined by the dutyholder as appropriate for their organisation. Inspectors should assure themselves that the relevant topics are covered adequately by the dutyholder. SyAPs Annexes H and J provide indicative incident management capabilities that a cyber protection system may have, mapped across the five functions and graded according to the categorisation of the information and associated assets being protected.

Inspectors should consider:

- Does the organisation have an Incident Management Policy (IMP) or similar that is derived from the IMS and which specifies how incidents are identified and managed?
- Is the IMP tailored to the organisation and adequate for the purpose?
- Is the IMP managed and implemented by Suitably Qualified and Experienced (SQEP) staff in the organisation to ensure that it is implemented and appropriate for the business?
- Do personnel in the organisation understand their responsibilities for incident management?
- Is the IMP regularly reviewed as part of the ongoing risk management process?

9. INCIDENT MANAGEMENT - IDENTIFY

9.1 Dutyholders should identify the business objectives for the resilience of business functions, particularly where the function is a necessary component in the protection of any assets under regulation. This should be aligned with the framework provided in SyAPs Annexes F to J.

9.2 The scope of the incident management process should be clearly defined and should identify all information and associated assets that the dutyholder is responsible for. The scope should be aligned to that covered by the risk assessment described in TAG 7.1 – Effective Cyber and Information Risk Management and should include information and associated assets managed by partners and supply chain companies.

9.3 Dutyholders should have in place a BC&DR plan which identifies the availability requirements for information and associated assets. Any service level agreements should be defined with service providers and suppliers.

9.4 Dutyholders should have definitions and criteria for what constitutes an incident in their organisation. A grading scheme should be in place so that incidents can be categorised.

9.5 Dutyholders should ensure that all personnel in the organisation have clear guidance on how to report incidents and to whom. This guidance should be reinforced through regular awareness training as part of the security culture. Furthermore, provision should be made for ‘no blame’ and anonymous reporting so that personnel can report concerns that could lead to a security incident without fear of recrimination.

9.6 Dutyholders should have a governance structure for incident managing. It should be clear who is responsible for receiving and collating incident reports and what the governance structure is as an incident is identified and managed. Senior managers,

including a Board member, should be part of this structure. It should be clear that CS&IA is part of broader risk management and not purely a matter for technical security personnel.

9.7 Dutyholders should consider that security incidents are likely to be dynamic and have a significant scope so the management process should be flexible and be able to operate in a timely manner. They should assure themselves that there are effective information flows and empowered managers at different levels in the organisation to assist decision-making.

9.8 There should be a clear escalation path for security incidents so that it is understood who is responsible for managing the incident at any one time. If the process includes callout lists and nominated personnel, then inspectors should assure themselves that the process includes provision for them to be appropriately maintained.

9.9 There should be a mechanism for invoking additional resources such as tools, personnel, expertise and decision-making capability as required. Responsibilities should be clearly defined in advance, and there should be adequate arrangements to ensure that personnel are SQEP for the role and that resources are available when required.

9.10 Advice on managing security incidents is available from external organisations such as the Centre for the Protection of National Infrastructure, and CERT UK. Specialist commercial companies certified by NCSC in the Cyber Incident Response Scheme are also available to provide expert support.

9.11 Personnel in key roles should have clearly defined responsibilities and should be empowered appropriately so that they can make operational decisions. They should also be SQEP for their role with initial training and updates as appropriate to reflect changes in the organisation and the dynamic nature of the cyber threat.

9.12 Incident management will involve many parts of the organisation and consideration should be given to including representatives from HR, legal, corporate communications and finance in addition to relevant technical teams both in the affected organisation and its supply chain.

9.13 The incident management structure should have relationships with similar teams in other organisations. There are clear benefits in sharing some information in terms of threat warnings, good practice and lessons learned. A number of organisations offer guidance on incident management and this should be utilised.

9.14 The incident management process should have measures to manage the information that will be generated. It is likely that a lot of data will be generated as part of the analysis and investigation functions and dutyholders should have a plan for managing data so that it is available when required in the format required. However, these arrangements should give due consideration to CS&IA issues such as access control requirements and securing data adequately, at rest and in transit, to ensure any SNI is appropriately protected.

9.15 Dutyholders should consider how security incidents in service provider organisations are to be managed. For example are subcontractors required to have their own incident management process or should they be incorporated into a centralised mechanism?

Inspectors should consider:

- Does the IMP identify the business objectives for the resilience of business functions, particularly where the function is a necessary component in the protection of any assets under regulation?
- Is the scope of the IMP clearly defined and does it identify all information and associated assets that the dutyholder is responsible for?
- Does the scope of the IMP include any relevant service providers and suppliers?
- Does the dutyholder have definitions and criteria for what constitutes an incident in their organisation? Is there a grading scheme in place so that incidents can be categorised?
- Does the dutyholder ensure that all personnel in the organisation have clear guidance on how to report incidents and to whom? Is this reinforced through regular awareness training as part of the security culture?
- Does the organisation make provision for 'no blame' and anonymous reporting so that personnel can report concerns that could lead to a security incident without fear of recrimination?
- Is it clear who is responsible for receiving and collating incident reports within the organisation and what the governance structure is as an incident is identified and managed?
- Is there a clear escalation path for security incidents so that it is understood who is responsible for managing the incident at any one time?
- Are callout lists appropriately updated?
- Does the organisation's incident management team include representatives from HR, legal, corporate communications and finance in addition to relevant technical teams both in the affected organisation and its supply chain?
- Does the incident management process have measures to manage the information that will be generated, to ensure its confidentiality, integrity and availability?

10. INCIDENT MANAGEMENT - PROTECT

10.1 Dutyholders should ensure that all information and associated assets have been identified and are appropriately protected. SyAPs Annexes H to J detail the security outcome that a CPS should achieve and indicative defensive postures.

10.2 Appropriate boundary and internal technical defensive measures should be in place and could include: firewalls, virtual networks (VLANS), network access controls (NAC), de-militarised zones (DMZ), Intrusion Detection or Intrusion Prevention Systems (IDS/IPS), sandboxing, application whitelisting, device port control, malware protection, service proxying (forward and reverse), threat management gateways (TMG), e-mail and web traffic filtering.

10.3 Technical security controls should be applied in a defence in depth structure throughout operational networks. Technical controls should be supported by

procedural, personal and physical measures. Where technical monitoring tools are deployed, a baseline of what 'normal' for the business looks like should be developed. This includes patterns of user behaviour on systems.

10.4 Access to information and associated assets should be controlled through a combination of physical measures (e.g. appropriate doors and locks for secure areas) and technical measures such as multi-factor authentication, NAC and encryption.

10.5 Organisations should have a capability to undertake system monitoring. This may be done though development of a Network Operations Centre (NOC) and/or Security Operations Centre (SOC) or through external monitoring by a suitable service provider.

10.6 Dutyholders should ensure that the organisation's defensive posture is maintained at all times. Therefore, personnel should be aware of, and understand, their role in implementing the organisation's IMP. Furthermore, dutyholders should ensure that appropriate processes and procedures are in place and that these are tailored to roles (for example personnel operating system security monitoring tools such as IDS/IPS, TMG or firewall monitors should be SQEP).

Inspectors should consider:

- Has the organisation ensured that all information and associated assets have been identified and are appropriately protected?
- Does the organisation have in place appropriate boundary and internal technical defensive measures which could include:
  - Firewalls?
  - Virtual networks (VLANS)?
  - Network access controls (NAC).
  - De-militarised zones?
  - Intrusion Detection or Intrusion Prevention Systems?
  - Sandboxing?
  - Application whitelisting?
  - Device port control?
  - Malware protection?
  - Service proxying (forward and reverse)?
  - Threat management gateways?
  - E-mail and web traffic filtering?
- Have technical security controls been applied in a defence in depth structure throughout operational networks? Are technical controls supported by procedural, personal and physical measures?
- Does the organisation ensure that access to information and associated assets are controlled through a combination of physical measures (e.g. appropriate doors and locks for secure areas) and technical measures such as multi-factor authentication, NAC and encryption?
- Does the organisation have a capability to undertake system monitoring? This may be done though development of a Network Operations Centre (NOC) and/or Security Operations Centre (SOC) or through external monitoring by a suitable service provider.
- Do appropriate personnel in the organisation understand their responsibilities for ensuring that the organisation's defensive posture is maintained at all times?

11. INCIDENT MANAGEMENT - DETECT

11.1 Dutyholders should ensure that appropriate tools are available to detect cyber security incidents in a timely manner that supports the CPS relevant security outcomes and response strategy in SyAPs Annex H and I. They should ensure that all risks to information and associated assets are covered. Commercial tools are available to detect both cyber incidents as well as tools that monitor anomalous user behaviour on technical systems.

11.2 Where tools are being used for monitoring they should be configured with the baseline for 'normal' behaviour on the relevant system so that the number of false indications of incidents is kept to a minimum.

11.3 Dutyholders should ensure that incidents are detected and reported as quickly as possible. The output from tools must be configured to be available quickly for analysis by operators and incident managers.

11.4 Dutyholders should clearly define the incident information being logged and its utility. A mechanism should be considered to collate and analyse logs and reports from different monitoring tools to bring them together for operators and managers as quickly as possible. Tools such as a Security Information and Event Manager (SIEM) are commercially available for such functions.

11.5 Dutyholders should ensure that a log is kept of all security incidents. The incident log should be initiated as soon as an incident (as defined by the agreed criteria) is identified.

11.6 The log should include two elements: a record reflecting the timeline of the stages of the incident (to include when it occurred) and what actually happened at each point. This log is vital in any lessons learned review after the incident has been closed. A voice log of telephone calls should be considered since critical decisions may be made verbally.

11.7 The log should also have a summary or register of all security incidents and should use the incident grading scheme. This allows managers to see in a usable format what numbers and types of incidents have occurred in a specified time period and they can take action if required. This register will support longer term analysis of trends of the different types of incidents and support managers in focussing on concerns in priority order.

11.8 Dutyholders should be aware that incident material, such as the log, may be required as evidence in investigations for legal or disciplinary reasons and logs should therefore be access controlled and held securely.

Inspectors should consider:

- Does the organisation ensure that appropriate tools are available to detect cyber security incidents in a timely manner, underpinning the CPS relevant security outcomes and response strategy in SyAPs Annex H and I?

- Does the organisation have a mechanism in place to collate and analyse logs and reports from different monitoring tools to bring them together for operators and managers as quickly as possible?
- Does the organisation ensure that incidents are detected, logged and reported promptly; and that the output from monitoring tools are configured to be available quickly for analysis?
- Is the organisation aware that incident material, such as the log, may be required as evidence in investigations for legal or disciplinary reasons and logs should therefore be access controlled and held securely?

12. INCIDENT MANAGEMENT - RESPOND

12.1 The manner in which an organisation responds to security incidents should be proportionate to the nature of those incidents as they are likely to vary considerably. The incident management function should therefore have the capability to flex up and down as necessary.

12.2 There are many different types of security incident and a mechanism for characterising them should be considered. This mechanism should reflect values such as: asset value, system criticality, operational impact, type, etc. These attributes should be summarised in a value that will support a priority for managing them.

12.3 Identified incidents should be assessed in an initial triage process that establishes the type of incident and assigns it a priority for management based upon agreed criteria. This will allow incidents to be managed in priority order.

12.4 An escalation mechanism should be in place to alert managers of an incident in accordance with the governance structure. This should be supported by a process to bring in additional resources (e.g. personnel with relevant skills) to manage the incident.

12.5 Dutyholders should consider operating a Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) in response to incidents occurring. A CERT or CSIRT team could be a temporary team activated only when a security incident occurs or a permanent implementation that operates alongside or as part of NOC/SOC arrangements.

12.6 A process, as described in a digital forensics plan should be in place to analyse any incident and to gather as much information about it as possible. Consideration should be given to the use of forensic analysis tools whilst bearing in mind the need to preserve evidence. Furthermore, consideration will also need to be given to operating plant and any potential conflict between conserving evidence and maintaining safety (e.g. power down/switch off may make safe in many cases but could lose any forensic evidence). Technical experts and specialist tools should also be available 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 worsening worse and spreading to other areas.

12.7 Dutyholders should ensure that they understand their legal and regulatory responsibilities in the event of an incident and that these are reflected in defined processes and procedures for how incidents are to be responded to and investigated,

and by whom. This should include mechanisms to escalate handling of the incident to relevant managers for decisions that may affect operations and the business.

12.8 The incident management process should include the ability to implement long term containment or mitigation measures. Since an incident generally denotes increased risk to the business, these long term measures should be reflected in the organisation's risk register and managed to a conclusion.

12.9 There should be a process that ensures internal and external reporting of incidents as they occur and develop. External reporting may include regulators, customers, partners and supply chain companies. A prepared Communication Plan should be in place to ensure that the right people are informed for the right reasons at the right time.

12.10 The process should include the ability to invoke disaster recovery and/or business continuity arrangements.

12.11 There should be an incident closure and wrap up process with a final report. The incident log should be closed and retained securely for review.

Inspectors should consider:

- Does the organisation have a mechanism for characterising security incidents, reflecting values such as: asset value, system criticality, operational impact, type, etc.?
- Does the organisation have a process that establishes the type of incident and assigns it a priority for management based upon agreed criteria?
- Is there an escalation mechanism in place to alert managers of an incident in accordance with the governance structure, supported by a process to bring in additional resources to manage the incident?
- Does the organisation operate a Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) in response to incidents occurring?
- Does the organisation's process include the ability to invoke disaster recovery and/or business continuity arrangements?
- Does the organisation have an incident closure and wrap up process with a final report? Is the incident log closed and retained securely for review?

13. INCIDENT MANAGEMENT - RECOVER

13.1 Dutyholders should provide adequate resources to implement and support the incident management policy. Resources should include:

- Sufficient SQEP personnel for the various roles and with an ability to call on additional numbers and skills as necessary
- Adequate equipment and tools for monitoring, detecting, analysing and managing incidents. This will include data storage, mobile devices etc
- Communications equipment both for internal use by the team and resources for links to regulator, external partners, support team and supply chain companies

- Accommodation for NOC / SOC, CSIRT teams with an ability to scale up in response to an incident
- Data management should be catered for to ensure that sufficient storage space is available on systems that are themselves protected and resilient. Logs from monitoring and reporting tools are likely to be quite large and these need to be both stored appropriately and be quickly available as required

13.2 Provision should be made for adequate backup and restore capability for information and associated assets to provide resilience in the event of an incident. These provisions should consider data formats, capacity, security, disaster recovery and accessibility. The restoration capability and provisions should be subject to appropriate levels of exercising.

13.3 Dutyholders should ensure that adequate spares, software licences and updates are provided for IT and other equipment used in incident management.

13.4 Cyber incidents are likely to involve an attacker's use of malicious software and therefore incident response teams will need to analyse code as part of attacks in order to develop mitigations. Accordingly, dutyholders should consider the need for adequate test and development facilities as well as training (not only technical) programmes for incident management teams to maintain skills in response to changing attack technologies and methods and their application to information and associated assets. This is likely to be a complex area and therefore dutyholders should consider whether such capability would benefit from engagement with specialist contractors or organisations such as NCSC. Additionally, the security of incident team equipment, data, accommodation, spares and other materials should be considered and appropriate access controls put in place to protect them.

13.5 Dutyholders should ensure that there is a comprehensive lessons learned and follow-up process after incidents. Such reviews should take place as soon after an incident as possible and should culminate in a report and recommendations for actions that can be addressed by management.

13.6 Incident reports will help identify any deficiencies in process, management, skills, equipment or other areas and dutyholders should have a mechanism in place to track actions to address such deficiencies.

13.7 Such reports may be sensitive and will require protection and controlled distribution but relevant extracts should be made available to all relevant personnel – including supply chain staff as appropriate.

13.8 Dutyholders should have a mechanism in place for testing incident management functions; further guidance on testing is provided at section 15 below.

Inspectors should consider:

- Does the organisation have adequate resources to implement and support the IMP? Resources should include:
  - Sufficient SQEP personnel for the various roles`.
  - Equipment and tools for monitoring, detecting, analysing and managing incidents.

- Communications equipment both for internal use by the team and resources for links to regulator, external partners, support team and supply chain companies.
- Accommodation for support teams with an ability to scale up in response to an incident.
- Secure and resilient data management facilities.

- Does the organisation have suitable provision for adequate backup and restore capability for information and associated assets to provide resilience in the event of an incident? Do these provisions consider data formats, capacity, security, disaster recovery and accessibility? Is the restoration capability and provisions subject to appropriate levels of exercising?
- Does the organisation ensure that there is timely lessons learned and follow up process after incidents?
- Does the organisation have a mechanism in place for testing incident management functions?

14. INCIDENT MANAGEMENT REPORTING

14.1 Dutyholders should have an incident communications plan that describes the types and formats of communications and reports at the various stages of an incident. The plan should specify what communications medium is to be used and the requirements for logging, etc. In particular, dutyholders should be aware of their responsibility under legislation to report incidents to external bodies and these legal obligations should be fully addressed within the communications plan.

14.2 Consideration should be given to the sensitivity of security incidents and their response. For example information that identifies critical system technical vulnerabilities could inform future attackers and access to this should be controlled. Secure communications means may be required for incident managers.

14.3 Communication both within the organisation and externally should be planned and exercised with the appropriate teams which might include business continuity, incident management, communications and public relations. This includes information passed to managers, third-parties, regulators, the Press and international agencies and partners. Attention should be paid to data sensitivity and guidelines defined in advance on what information can be released to whom and when. Good practice proposes pre-agreed communications statements for Press release.

14.4 Arrangements for incident reporting by third-party service providers and suppliers should be defined and these should be part of contract provisions.

Inspectors should consider:

- Does the organisation have an incident communications plan that describes the types and formats of communications and reports at the various stages of an incident? Does the plan specify what communications medium is to be used and the requirements for logging, etc?

- Is the organisation aware of their responsibility under NISR 2003 to report incidents to ONR and are these legal obligations fully addressed within the communications plan?
- Does the organisation consider the sensitivity of security incidents and their response and have secure communications means when required?
- Does the organisation plan and exercise with the appropriate teams which might include business continuity, incident management, communications and public relations?
- Are arrangements for incident reporting by third-party service providers and suppliers defined and are these part of contract provisions?

15. POST-INCIDENT PROCEDURES

15.1 To be fully effective the incident management process should be one of continuous improvement so dutyholders should have arrangements in place for incident review to identify any lessons that can be learned once an incident has been declared over.

15.2 Such a review should look at all security incidents that have occurred, regardless of priority, including those from third parties. The review should be able to identify trends and highlight any specific vulnerabilities in areas such as policy, procedures, information and associated assets.

15.3 The responsibility for reviewing incidents should be carefully considered because if the incident management team conducts its own reviews it may not have sufficient awareness to understand impacts across the business. An adequately empowered manager should conduct any review and ensure that recommendations are formulated and put into action.

15.4 The review should take place as soon as possible after incidents occur so that events are fresh in people's minds. The incident log will play a crucial role in describing the incident timeline.

15.5 All relevant business functions (including suppliers) should be involved in the review process so that they can provide their own perspective of the incident. This is likely to generate recommendations for improvements in various aspects of CS&IA across the organisation. A formal report of the incident should be made, both as a matter of record but also as a vehicle for taking recommendations forwards.

15.6 Dutyholders should consider the legal and disciplinary aspects of security incidents and the importance of the need for forensic evidence and a technical evidence chain.

15.7 Where deficiencies of policy, process, procedure, management, personnel or information and associated assets have been found as a consequence of a security incident, these should be adequately addressed. The incident management process should track these to a successful conclusion or have them included in the risk register.

Inspectors should consider:

- Does the organisation have arrangements in place for incident review to identify any lessons that can be learned once an incident has been declared over?
- Does the post-incident review look at all security incidents that have occurred, regardless of priority, including those from third parties? Is the review able to identify trends and highlight any specific vulnerabilities in areas such as policy, procedures, information and associated assets?
- Does the review take place as soon as possible after incidents occur so that events are fresh in people's minds?
- Does the review involve all relevant business functions (including suppliers) so that they can provide their own perspective of the incident?
- Does the organisation consider the legal and disciplinary aspects of security incidents and the importance of the need for forensic evidence and a technical evidence chain?
- Does the organisation ensure that where deficiencies of policy, process, procedure, management, personnel or information and associated assets have been found as a consequence of a security incident, that they are adequately addressed?

16. ASSURANCE

16.1 It is essential that dutyholders consider how assurance will be provided so that security incidents are detected quickly and managed effectively. A mechanism should be in place to assess the strategy and policy on a regular basis and to assess the implementation of the various steps in the incident management process.

- Dutyholders should have a process to test and exercise the security incident management functions. The testing could include:
  - Document reviews of the strategy and policy.
  - Walkthroughs of the processes.
  - Test call-outs of personnel.
  - Exercise scenarios with Red Teams or external bodies.
  - Technical exercises of the CERT/CSIRT response.
  - Technical scans of IT/OT and supporting systems.
  - Test responses to changes in threat (Government Response Level).
  - Test of forensic readiness to a legal issue.
  - Test reporting times to external authorities.
  - Testing of Business Continuity Plans.
  - Testing of Disaster Recovery Plans.

Inspectors should consider:

- Does the organisation have a mechanism in place to assess the strategy and policy on a regular basis and to assess the implementation of the various steps in the incident management process?
- Does the organisation have a have a process to test and exercise the security incident management functions?

17. BUSINESS CONTINUITY AND DISASTER RECOVERY

17.1 BC&DR are separate topics in their own rights and provide differing but complementary aspects of operational resilience in an organisation. They are aligned closely to security incident management in that they aim to ensure that operations are sustained. They also rely upon a detailed analysis of the business to identify and categorise information and associated assets.

17.2 Dutyholders should have a BC&DR strategy endorsed and supported by the Board. The strategy should be proportionate to the organisation and address all legal and regulatory requirements. The strategy should be implemented by BC&DR plans based upon a risk assessment and using a categorisation system for information and associated assets that fits within the framework detailed in SyAPs Annexes F and G.

17.3 The Deming cycle of Plan, Do, Check, Act can be used to structure how BC&DR plans are implemented and managed. This will assist dutyholders ensure that their BC&DR plans are fit for purpose (e.g. are maintained and are tested adequately).

17.4 BC&DR plans may be invoked in response to incidents and the management of a security incident may be closely linked to the management of BC&DR processes. Dutyholders should therefore have a clear understanding of when and how BC&DR aspects are involved in security incident management and should ensure that incident managers have a comprehensive understanding of BC&DR plans and processes.

17.5 Dutyholders should consider the benefits of an integrated incident and BC&DR management function.

Inspectors should consider:

- Does the organisation have a BC&DR strategy endorsed and supported by the Board?
- Is the strategy proportionate to the organisation and does it address all legal and regulatory requirements?
- Is the strategy implemented by BC&DR plans based upon a risk assessment and using a categorisation system for information and associated assets that fits within the framework detailed in SyAPs Annexes F and G?

18. 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. 2017/124772

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. **NCSC - A Critical Appraisal of Risk Methods and Frameworks** https://www.ncsc.gov.uk/guidance/critical-appraisal-risk-methods-and-frameworks

11. **Good Practice Guide for Incident Management**. ENISA https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

12. **Guide to Incident Response.** CERT. https://www.cert.org/incident-managment/csirt-development/csirt-faq.cfm

13. **Incident Handler's Handbook.** SANS. https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

14. **SANS SCORE APT Incident Handling security Checklist.** SANS. https://www.sans.org/media/score/checklists/APT-IncidnetHandling-Checklist.pdf

15. **Computer Security Incident handling Guide.** NIST. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

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

19. GLOSSARY AND ABBREVIATIONS

BC&DR	Business Continuity and Disaster Recovery
CERT	Computer Emergency Response Team
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
CSIRT	Computer Security Incident Response Team
DMZ	De-militarised Zone
ENISA	European Network and International Security Agency
FSyP	Fundamental Security Principle
HMG	Her Majesty's Government
IAEA	International Atomic Energy Agency
IDS/IPS	Intruder Detection System / Intruder Protection System
IMP	Incident Management Plan
IMS	Incident Management Strategy
NAC	Network Access Controls
NISR	Nuclear Industries Security Regulations
NOC	Network Operations Centre
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
SIEM	Security Information and Event Manager
SNI	Sensitive Nuclear Information
SOC	Security Operations Centre
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide
TMG	Threat Management Gateway
VLAN	Virtual Local Area Network