2

ONR GUIDE			
PREPARATION FOR AND RESPONSE TO CYBER SECURITY EVENTS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNSS-TAST-GD-7.5 Revision 3		
Date Issued:	March 2021	**Review Date:**	March 2024
Approved by:	Paul Shanes	Professional Lead for CS&IA	
Record Reference:	(2021/27620)		
Revision commentary:	Revisions to align to new and updated national and international standards		

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 1). 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 2).

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 judgement 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 3) and the IAEA Nuclear Security Fundamentals (Reference 4). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 Fundamental Principle K expects states to establish requirements for contingency plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, to be prepared and appropriately exercised by all dutyholders.

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 5). Paragraphs 3.53 to 3.55 specifically refer to issues relating to confidentiality.

4.4 The IAEA publishes guidance on Computer Security Incident Response Planning at Nuclear Facilities (Reference 6).

4.5 The IAEA also publishes Implementing Guide NSS No. 23-G 'Security of Nuclear Information' (Reference 7), Technical Guidance NSS No. 17 'Computer Security at Nuclear Facilities' (Reference 8) and NSS 33-T Computer Security of Instrumentation and Control Systems 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 (SyDP) 7.5 – Preparation for and Response to Cyber Security Incidents in support of FSyP 7 – CS&IA. The TAG is consistent with other CNSS TAGs and associated guidance and policy documentation.

5.2 The HMG publication Government Functional Standard GovS 007: Security (hereafter termed GovS 007) (Reference 10) describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm's length bodies or their contracted third parties. The security principles, governance, life cycle and practices detailed within GovS 007 have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not.

5.3 The Government Security Classifications document, together with the ONR Classification Policy (Reference 11) describe types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

6. ADVICE TO INSPECTORS

6.1 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.		

6.2 SyAPs reflects a range of Relevant Good Practice (RGP) (such as the NIST cyber security framework (Reference 12)) in its approach to define the security posture for sensitive nuclear information and equipment and software used in connection with activities involving nuclear material/other radioactive material. This ensures that defence in depth is provided through the implementation of plans, policies and procedures that define:

i) how assets of value should be identified and protected,

ii) how the organisation should detect and respond to a cyber security incident, and

iii) how the organisation will recover to ensure effective operations are re-established as efficiently as possible. This guidance relates to the latter two points.

6.3 Fundamentally, this Security Delivery Principle establishes an expectation that the dutyholder will make, implement, and test arrangements that enable the organisation to effectively and efficiently respond to cyber security incidents.

6.4 Current RGP described by various organisations, including SANS Institute and The US Department of Energy, and NIST defines 6 key stages of incident response. Figure 1 summarises the stages, each of which will be considered in greater detail in subsequent sections. However, there are some general principles and considerations that should be recognised during incident response

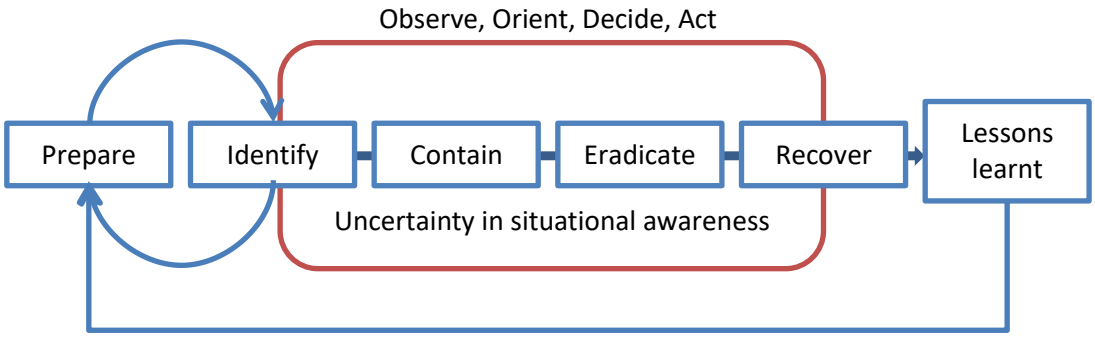

Figure 1: The Incident Response Process

6.5 Whilst this TAG bases its regulatory expectations on the framework set out in Figure 1, it is to be expected that some dutyholders may take a different approach. This is entirely reasonable, and inspectors should ensure that judgements are made against the dutyholder's ability to achieve the expected security outcome and response.

6.6 The Observe, Orient, Decide, Act (OODA) loop represents the period of intensity during incident response, and is intended to prevent spontaneous poorly considered reactions. It promotes a construct that requires the Cyber Incident Response Team (CIRT) to pause, analyse, incorporate information received from the environment and then integrate new knowledge into the next course of action.

6.7 There is significant uncertainty associated with situational awareness particularly in the early stages of a cyber incident. This is compounded by the needs of a wide range of stakeholders to understand what is happening. A successful CIRT and its leader are responsible for managing the uncertainty by keeping informed and controlling the flow of information to stakeholders but also allowing subject matter experts to focus on their tasks.

6.8 It is critical that unity of command is maintained across the entire IR process, from Preparation to Lessons Learnt, that ensures there is a solid, reliable and well-known decision-making process in place.

6.9 There are several sources of guidance and advice available, including:

- Good Practice Guide for Incident Management – ENISA (Reference 13)
- Guide to Incident Management – CERT (Reference 14)
- Incident Handler's Handbook – SANS (Reference 15)
- Computer Security Incident Handling Guide – NIST (Reference 16)
- Incident Management guidance - NCSC (Reference 17)
- Computer Security Incident Response Planning at Nuclear Facilities - IAEA (Reference 6)

6.10 As with all regulatory activity, when assessing dutyholder arrangements for cyber IR, activity should be proportionate to the potential impact. Many dutyholders will outsource large parts of their IR capability to a third party. In such cases, regulatory activity should focus around the control the dutyholder has over that contract, the separation of responsibilities as well as interfacing activities such as providing access to digital systems and assets.

6.11 Inspectors should also be cognisant of ONR's regulatory vires in this area. Dutyholders will conduct IR for a variety of reasons, but an inspector's focus should be on achieving security outcomes associated with ensuring nuclear safety and security. It is also important to keep in mind that many IR activities are associated with business continuity and disaster recovery, which will only be within regulatory scope where they are required to maintain safety or security, or to facilitate hazard and risk reduction.

6.12 The UK's nuclear estate is complex and includes aged facilities where there are many legacy systems that present challenges to conducting IR. However, this does not serve as an excuse nor abdicate the dutyholder of responsibility for conducting effective IR. Inspectors should seek assurances, that the expected security outcome and response can be achieved despite the challenges presented by legacy systems, albeit by potentially different means.

7. PREPARATION

7.1 Preparation is about readying the CIRT to handle an incident at short notice and under any reasonable conditions. An incident can range from a phishing attempt to more extreme incidents such as a violation of organisational policy by disgruntled employees or networks being infiltrated by state sponsored adversaries. Regardless of the cause, preparation is arguably the most important phase, as it will determine how well the CIRT will be able to respond in the event of a crisis.

7.2 There are several key considerations in this phase that will help to mitigate any potential issues that could hinder the CIRT's ability to handle an incident.

Incident response policies and plans

7.3 Dutyholders should develop a sound and clear incident response policy. Shaping a workable policy involves creating a set of written principles, rules and processes that act as a guide, setting out the correct actions, responsibilities and practices individuals across the organisation need to adhere to in order to maintain the risk appetite and cyber security posture the company has decided on.

7.4 Along with creating and maintaining a policy, developing a response plan is one of the very first steps organisations should take in the initial phase of the incident response methodology. An effective response plan should typically prioritise incidents by level of impact on nuclear safety and security as well as the wider business impact, and clearly define the most appropriate actions to deal with them.

7.5 The response plan should determine the CIRT team membership and rotation and should clearly articulate the command and control structure. While IR team membership will vary depending on the dutyholder expertise the following roles are typical in an incident response: cyber security, cyber security incident response, enterprise architecture, nuclear security, nuclear safety and communications. The size of the team that is stood up should be proportionate to the significance of the event or incident.

7.6 ONR TAG CNS-TAST-GD-11.4.2 (Reference 18) sets out regulatory expectations for the use of threat information against which the security regime should be designed, evaluated, and tested. Incident response plans should therefore be informed by threat assessment information from organisations such as the National Cyber Security Centre (NCSC).

7.7 If an incident response retainer exists, knowing when to use internal teams or when to 'break glass' and engage an external CIRT provider is helpful. This can and should be defined ahead of time and be documented in the incident response policy.

Inspectors should consider

- Is the incident response plan based on a clear understanding of the security risks to the networks and information systems supporting their essential function?
- Is the incident response plan comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely

impacts of both known attack patterns and of possible attacks, previously unseen?

- Does the incident response plan have senior management sponsorship, including the necessary approvals, authorities, and resources to execute the plan?
- Is there sufficient cover for each IR team role?
- Is the incident response plan documented and integrated with wider organisational business and supply chain response plans?
- Is the incident response plan communicated and understood by the business areas involved with the operation of their essential functions?
- Are there offline copies of the incident response plan and policies (e.g. in the event of a ransomware incident)?
- Is the response plan reviewed on a periodic basis?
- Are arrangements for engaging external support documented in the incident response policy?

Incident reporting

7.8 A formal cyber incident reporting system for staff and external security researchers aids with the identification of incidents.

Inspectors should consider:

- Does the dutyholder have a process that details when and how to inform relevant regulatory authorities and how to engage the National Technical Authority?
- Do the dutyholder's staff know the process to report a suspected cyber security incident?

Training and exercising

7.9 Regular practice is essential to staying calm and collected during an incident. Ongoing cyber security training, including essential techniques like attack simulation and information sessions, should be a central pillar supporting any cyber security regime.

7.10 Training should not be limited to technical skills; media and Public Relations (PR), privacy and legal all require specific training for an organisation and its people to be ready for an incident. Dutyholder organisations should also consider incident response retainers to augment their teams where certain skills are hard to find.

7.11 Organisations should also periodically involve managers and executives in their incident response training and exercises. Although they do not have to participate as

frequently as technical staff, it is prudent to have them participate on occasion to ensure they are familiar with their roles and the decisions they would be expected to make during an incident.

7.12 Dutyholders should carry out exercises to test response plans, using past incidents that affected their (and other) organisation, and scenarios that draw on threat intelligence and their risk assessment.

Inspectors should consider:

- Can the dutyholder evidence that CIRT staff have received recent and relevant response training?
- How often is training provided and how often is a training needs analysis conducted?
- Are the dutyholder's exercise scenarios based on experience and/or composed using relevant threat intelligence?
- Are exercise scenarios documented, regularly reviewed, and validated?
- Does the dutyholder ensure that exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learnt?
- Do the dutyholder's exercises test all parts of their response cycle relating to their essential functions (e.g. Restoration of normal function levels)?

Tooling

7.13 Ensuring the response team has the appropriate hardware, software and licensing is essential. These elements will likely involve a mixture of open source and licensed software, such as forensic tools, memory analysis, log parsers, scripts to interact with cloud services and something to generate a timeline. All tooling should have the appropriate hours of training invested.

7.14 The hardware can include USB hard drives, up-to-date anti-malware applications, write blocker devices, evidence bags, and an appropriate secure storage location to maintain the chain of custody. More specialised equipment can be employed for specific cases. This might include Field Programmable Gate Arrays (FPGA)-based devices that may be used together with Direct Memory Access (DMA) attack toolkits.

Inspectors should consider:

- Has the dutyholder identified tools needed for use in a computer security incident response and ensured their availability?
- Are incident response tools and supplies audited on a periodic basis to ensure kits are up to date and complete?
- Are incident response tools and supplies refreshed after use?
- Do incident response tools and supplies include an incident journal, evidence forms, evidence bags etc?

- Has the dutyholder performed the appropriate assurance activities (e.g. audit) for the incident response tools held by the third party?

7.15 ***Communication***

7.16 There are two kinds of communication that are important in the event of a cyber incident, and both should be included in a communications plan. Internal communication processes are essential to handling the incident itself. IR teams need a secure communication capability that cannot be monitored by an attacker or insider. For example, everyone on the IR team should have a mobile phone and a secondary external email account. The IR team should know the correct people within the business to help triage an incident.

7.17 External activities such as public relations require clear and timely communications. Dealing with media enquiries requires experience and should be limited to those with proper training. Any staff with public relations responsibilities should have appropriate crisis training.

7.18 An incident journal to track the who, what, where, when and why of an incident can aid with internal communication of incident status and later review as part of lessons learnt.

Inspectors should consider:

- Has an out-of-band communications capability been established?
- Have internal and external communications plans been established?
- Does the dutyholder have a mechanism for sharing a journal of the incident status?

Environment preparation

7.19 There are several technical measures that can be established ahead of time that will support and facilitate efficient and timely incident resolution.

7.20 Network Time Protocol (NTP) should be enabled for all networked devices, including routers and switches. In the corporate environment, Windows Clients should be synchronised with Active Directory (AD).

7.21 A protected logging aggregation point that has multiple terabytes of storage should be established such as a linux server running syslog-ng. All systems should be instrumented to detect an incident and report both locally and to the central server.

7.22 An accurate asset inventory is essential for IR teams to receive timely information about the assets on the network, such as operating system patch level, purpose, app usage, configuration, backup status, criticality/importance, access rules and other key data. Ownership for all generic, shared service and system accounts should be established ahead of time.

Inspectors should consider:

- Can the dutyholder identify the data, personnel, software applications, devices, systems, and facilities that enable the organisation to achieve business purposes and are managed consistent with their relative importance to organisational objectives and risk strategy?
- Has a central logging capability been established, are networked systems instrumented to detect an incident and are they configured to report locally and to the central server?
- Is NTP enabled on all networked devices, synchronised across the estate and, in the corporate environment, are all windows clients synchronised with AD?
- Have potential key decisions been identified and worked through in advance, for example, have system changes that may need to be made during an incident been pre-negotiated?
- Is there an accurate asset inventory and has ownership of all generic, shared, service and system accounts been established?

Response and recovery capability

7.23 Dutyholders should have the capability to enact their incident response plan, including effective limitation of impact on the operation of their essential function. During an incident, they should have access to timely information on which to base their response decisions.

Inspectors should consider:

- Does the dutyholder understand the resources that will likely be needed to carry out any required response activities, and ensure that arrangements are in place to make these resources available?
- Do they understand the types of information that will likely be needed to inform response decisions and ensure that arrangements are in place to make this information available?
- Do their response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and do they have the authority to carry them out?
- Does the dutyholder have a defined methodology for the prioritisation of recovery of services? Have systems been prioritised based on their importance?
- Are fail-over mechanisms available that can be readily activated to allow continued operation of their essential function (although possibly at a reduced level) if primary networks and information systems fail or are unavailable?
- Do arrangements exist to augment the dutyholder's incident response capabilities with external support if necessary (e.g. specialist cyber incident responders)?

Backup

7.24 In the event of a cyber incident, backups will be required to restore systems to a known good state. To support recovery, dutyholders should have adequate backups of systems with agreed Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). A common principle is the 3-2-1 backup strategy that states there should be 3 copies of data (production data and 2 backup copies) on two different media with one copy off-site for disaster recovery.

Inspectors should consider:

- Does the dutyholder have a policy for testing IT and OT backup systems?
- Does the dutyholder backup and test the recovery of key IT and OT systems?
- Does the recovery process include data integrity checks at completion of the recovery activity?
- What is the backup strategy, plan and testing regime for cloud systems?

8. IDENTIFICATION

8.1 Dutyholders should ensure that capabilities exist to detect/identify cyber security events affecting, or with the potential to affect, essential functions.

Security Monitoring

8.2 The organisation should monitor the security status of networks and systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures. The data sources that dutyholders include in their monitoring should allow for timely identification of security events which might affect the operation of their essential function.

Inspectors should consider:

- Is the dutyholder's monitoring based on an understanding of their network's baseline characteristics, common cyber-attack methods and what they need awareness of in order to detect potential security incidents that could affect the operation of their essential function (e.g. presence of malware, malicious emails, and user policy violations.)?
- Does their monitoring data provide enough detail to reliably detect security incidents that could affect the operation of their essential function?
- Can the dutyholder detect the presence or absence of indicators of compromise on systems delivering or supporting essential functions?
- Does extensive monitoring of user activity in relation to the operation of essential functions enable the dutyholder to detect policy violations and an agreed list of suspicious or undesirable behaviour?
- Does the dutyholder have multi-layer monitoring coverage that includes host-based monitoring and network gateways?

- Are new systems considered as potential monitoring data sources to maintain a comprehensive monitoring capability?
- Does the dutyholder provide appropriate security monitoring measures if the systems for essential functions cannot provide host-based security monitoring functions or security data?

Securing logs

8.3 Dutyholders should hold logging data securely and grant read only access to accounts with business need. No staff should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.

Inspectors should consider:

- Is the integrity of logging data protected, or is any modification detected and attributed?
- Does the logging architecture have mechanisms, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify? This should include protecting the function itself, and the data within it.
- Is log data analysis and normalisation only performed on copies of the data keeping the master copy unaltered?
- Are logging datasets synchronised, using an accurate common time source, so separate datasets can be correlated in different ways?
- Is access to logging data limited to those with business need and no others?
- Can all actions involving all logging data (e.g. copying, deleting or modification, or even viewing) be traced back to a unique user?
- Are legitimate reasons for accessing logging data given in use policies?

Generating alerts

8.4 Dutyholders should ensure that evidence of potential security incidents contained in their monitoring data is reliably identified and triggers alerts.

Inspectors should consider:

- Is logging data enriched with other network knowledge and data when investigating certain suspicious activity or alerts?
- Are a wide range of signatures and indicators of compromise used for investigations of suspicious activity and alerts?
- Can alerts be easily resolved to network assets using knowledge of networks and systems?

- Are security alerts relating to all essential functions prioritised and this information is used to support incident management?
- Are logs reviewed almost continuously, in real time?
- Are alerts tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms?

Identifying security incidents

8.5 Dutyholders should contextualise alerts with knowledge of the threat and their systems, to identify those security incidents that require some form of response. Dutyholders should have a process of categorisation based on the type and severity (impact on confidentiality, integrity and availability) to allow quick and efficient triaging of incidents. This will help to determine the urgency and escalation thresholds to support dutyholder response. A useful resource for establishing such a framework is the NCSC incident Management Guidance severity matrix and categorisation table (Reference 16)

Inspectors should consider:

- Does the dutyholder gauge the severity of impact of the incident in order to deliver a proportionate response?
- Has the dutyholder selected threat intelligence feeds using risk-based and threat-informed decisions based on their business needs and sector (e.g. Vendor reporting and patching, anti-virus providers, sector and sector-based information sharing)?
- Have they applied all new signatures and indicators of compromise within a reasonable (risk-based) time of receiving them?
- Does the dutyholder receive signature updates for all their protective technologies (e.g. anti-virus, IDS)?
- Does the dutyholder track the effectiveness of its intelligence feeds and actively share feedback on the usefulness of indicators of compromise and any other indicators with the threat community (e.g. civil nuclear sector, threat intelligence providers, government agencies)?
- Is there a process for initial determination i.e. who declares an incident based on observable events?
- Is there a process for assigning an initial handler and assigning responders?
- Have survey identification points been pre-determined?
- Is there an understanding of the limitations of the incident response capability? (knowing when to call in others)
- Have checklists been pre-prepared, for example, to check asset state against a known good baseline?

- Does the IR team have up to date network architecture diagrams?
- Is there a process for performing system and network activity consistency/baselining checks?
- Have potential key decisions been identified and worked through in advance?

Monitoring tools and skills

8.6 A dutyholder's monitoring staff must have skills, tools, and roles that reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff must have knowledge of the essential functions they need to protect.

Inspectors should consider:

- Does the dutyholder have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance?
- Do monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process?
- Are there playbooks to ensure consistency and to enable monitoring staff to make the determination regarding the initial validity of the alert in front of them as quickly as possible?
- Do monitoring staff follow processes and procedures that address all governance reporting requirements, internal and external?
- Are monitoring staff empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data?
- Do their monitoring tools make use of all logging data collected to pinpoint activity within an incident?
- Can their monitoring staff and tools drive and shape new log data collection and make wide use of it?
- Are monitoring staff aware of the operation of essential functions and related assets and can identify and prioritise alerts or investigations that relate to them?

Proactive security event and abnormality discovery

8.7 The dutyholder should detect, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable).

8.8 The dutyholder should define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.

Inspectors should consider:

- Does the dutyholder fully understand normal system behaviour to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (i.e. do they fully understand which systems should and should not communicate and when)?
- Are system abnormality descriptions from past attacks and threat intelligence, on dutyholder and other networks, used to signify malicious activity?
- Do the system abnormalities they search for consider the nature of attacks likely to impact on the networks and information systems supporting the operation of essential functions?
- Are the system abnormality descriptions they use updated to reflect changes in their networks and information systems and current threat intelligence?

Proactive attack discovery

8.9 Dutyholders should use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.

Inspectors should consider:

- Does the dutyholder routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting the operation of their essential function, generating alerts based on the results of such searches?
- Does the dutyholder have justified confidence in the effectiveness of their searches for system abnormalities indicative of malicious activity?
- Does the dutyholder routinely test the capability of the monitoring service to detect cyber incidents based on new and existing threats?

9. CONTAINMENT, ERADICATION AND RECOVERY

9.1 In line with RGP this TAG combines the Containment, Eradication and Recovery phase as there is a degree of overlap and iteration between each.

9.2 The containment phase sees responders work to limit any system damage caused by an incident and take measures to prevent further damage occurring.

Incident characterisation and containment strategy

9.3 Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g. shut down a system, disconnect it from a

network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident.

9.4 Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack.

Inspectors should consider:

- Has the dutyholder identified the major incident types that could impact its operations?
- Has the dutyholder created separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making?
- Has the dutyholder defined risk appetite for incident handling?
- Do the containment strategies enable the organisation to remain within that risk tolerance?

Incident Notification

9.5 When an incident is identified, the incident response team must make notifications both within the dutyholder organisation, and external to it. Incident response policies should include provisions for incident reporting - at a minimum, what must be reported, to whom and at what times (e.g. initial notification, regular status updates). In some cases, there are time critical legislative reporting requirements. The exact reporting requirements will vary among dutyholder organisations, but parties that are typically notified include:

- Individuals in the organisation's security vertical and relevant executives
- Other internal incident response team members
- External incident response support resource
- System owner
- Communications team
- National Cyber Security Centre
- ONR and/or other regulators as appropriate
- Police
- Anyone with whom a contractual arrangement exists e.g. a Contracting Authority.

Inspectors should consider:

- Is the dutyholder familiar with the incident reporting requirements and processes to inform regulators and third parties?

Evidence gathering and handling

9.6 Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved.

9.7 Computer based digital evidence is fragile in nature and may be altered or destroyed through improper handling or examination. Forensic processes should ensure the use of a write blocker to ensure that data is not inadvertently changed.

9.8 Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. In particular, a master copy and a working copy of the imaged data should be made in line with best forensic practice. Any forensic services provider should be accredited to ISO17025, the legal standard for admissible evidence, as a minimum.

9.9 Whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence, including the following:

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer).
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation.
- Time and date (including time zone) of each occurrence of evidence handling.
- Locations where the evidence was stored.

Inspectors should consider:

- Are dutyholder staff suitably qualified and experienced for preserving evidence?

Short-term containment

9.10 The focus of this step is to limit the damage as soon as possible. Short-term containment can be as straightforward as isolating a network segment of infected workstations to taking down production servers that were hacked and having all traffic routed to failover servers. Short-term containment is not intended to be a long-term solution to the problem; it is only intended to limit the incident before it gets worse

Inspectors should consider:

- Does the dutyholder have pre-agreed forms of containment (e.g. disconnecting networks)?
- Does the dutyholder have a process to record temporary changes?

System forensics

9.11 Before wiping and reimaging any system it is necessary to take a forensic image of the affected system(s) with tools that are well known in the computer forensics community such as Forensic Tool Kit (FTK), EnCase, et al. The reason behind this is that the forensic software will capture the affected system(s) as they were during the incident and thereby preserving evidence in the event that the incident resulted from a criminal act or to be used for observing how the system(s) were compromised during the lessons learnt phase.

Inspectors should consider:

- Do dutyholders have forensic capability or arrangements to call on a third party?

Long-term containment

9.12 In this step affected systems can be temporarily fixed in order to allow them to continue to be used in production, if necessary, while rebuilding clean systems in the next phase. The primary focus should be to remove accounts and/or backdoors left by attackers on affected systems, installing security patches on both affected and neighbouring systems, and doing other work to limit any further escalation of the incident while allowing normal business operations to continue.

9.13 Eradication is usually necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. Often threat actors will attempt to maintain persistence on systems beyond the scope of the initial incident. During eradication, it is therefore important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

9.14 The purpose of recovery is to bring affected systems back into the production environment in a controlled way to ensure that further outbreaks do not occur. It is essential that dutyholders test, monitor, and validate the systems that are being put back into production to verify that they are not being re-infected or compromised by some other means.

9.15 Eradication and recovery may involve restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists).

9.16 RGP (e.g. Reference 15) would be to use disk images that were created prior to a system being deployed into production to restore the system, and then installing patches and disabling unused services to harden the system against further attacks.

Dutyholders should also scan affected systems and/or files with anti-malware software to ensure any latent malware is removed.

Inspectors should consider:

- Does the dutyholder have in place arrangements to ensure the continuity of critical operations during a prolonged containment stage?
- Does the dutyholder have a contemporary asset inventory that identifies the system and asset categorisation?
- Does the dutyholder have pre-prepared plans for rebuilding critical systems to a known good state and returning them to service in appropriate timescales?
- Does the dutyholder have long-term containment plans that identify network segregation options, system and asset isolation strategies etc?
- Does the dutyholder have procedures in place for restoring key systems to a known good state?
- Where third party system vendors are involved does the dutyholder have SLAs in place to recover systems?

10. LESSONS LEARNT

10.1 Dutyholders should ensure that when an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.

10.2 Dutyholders should use lessons learnt from incidents to improve their security measures.

Inspectors should consider:

- Does the dutyholder ensure that root cause analysis is conducted routinely as a key part of their lessons learnt activities following an incident?
- Is the root cause analysis comprehensive, covering organisational process issue, as well as vulnerabilities in their networks, systems or software?
- Is all relevant incident data made available to the analysis team to perform root cause analysis?
- Does the dutyholder have a documented incident review process/policy which ensures that lessons learnt from each incident are identified, captured, and acted upon?
- Does the dutyholder's lessons learnt process/policy cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems?

- Do they use lessons learnt to improve security measures, including updating and retesting response plans when necessary?
- Are security improvements identified as a result of lessons learnt prioritised, with the highest priority improvements completed quickly?

11. REFERENCES

1. **Security Assessment Principles** – CM9 Ref. 2017/124772 ONR - Security Assessment Principles (SyAPs)

2. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403 The Nuclear Industries Security Regulations 2003

3. **Convention on the Physical Protection of Nuclear Material (CPPNM).** Convention on the Physical Protection of Nuclear Material | IAEA

4. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. OBJECTIVE AND ESSENTIAL ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME

5. **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.

6. **IAEA Computer Security Incident Response Planning at Nuclear Facilities** https://www.iaea.org/publications/10998/computer-security-incident-response-planning-at-nuclear-facilities

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

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

9. **IAEA Nuclear Security Series No. 33-T.** Computer Security of Instrumentation and Control Systems at Nuclear Facilities Computer Security of Instrumentation and Control Systems at Nuclear Facilities | IAEA

10. **Government Functional Standard GovS 007: Security.** https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903904/Government_Security_Standard.pdf

11. **NISR 2003 Classification Policy.** CM9 REF. 2012/243357. Classification Policy For the Civil Nuclear Industry

12. **Framework for Improving Critical Infrastructure Cybersecurity.** Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)

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

14. **Guide to Incident Management.** CERT. https://us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf

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

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

17. **NCSC Incident Management Guidance.** https://www.ncsc.gov.uk/collection/incident-management

18. **CNS-TAST-GD-11.4 Revision 0.0, The Threat**, CM9 Ref. 2020/0308652, Draft

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

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
CIRT	Cyber Incident Response Team
CAF	Cyber Assessment Framework
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
NCSC	National Cyber Security Centre
NISR	Nuclear Industries Security Regulations
NOC	Network Operations Centre
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
RGP	Relevant Good Practice
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