NDA Estate Cyber Incident Reporting and Response Policy

Doc No SCP06

Nuclear Decommissioning Authority

Rev 2
Date August 2016

Introduction

1. This document sets out the policy for the reporting of, and response to, Cyber Incidents originating in, or impacting on, the NDA Estate. It is intended to assist with the identification of Cyber Incidents, and the reporting of them to the appropriate authorities. Whilst responsibility for responding to Cyber Incidents within the NDA lies with duty holders, any incident in one part of the Estate could impact on others and so this policy also aims to ensure that risk owners across the Estate have the information that they require to protect themselves from comparable attacks. Equally, this policy also aims to identify the processes by which NDA, and the rest of the Estate, might render assistance to each other in the event of a Cyber Incident.

2. Cyber Incidents have the potential to cause significant harm and it is therefore likely that UK government, ONR and the UK's security and intelligence agencies will have a close interest in any Cyber Incident that occurs within the UK's Critical National Infrastructure, and in particular within the Civil Nuclear Sector (CNS). This policy has, therefore, been designed to complement and support the UK's National Cyber Incident Response Policy[1] – it should enable the seamless reporting of incidents to CERT-UK and enable UK national assets to provide support where this is deemed to be necessary and appropriate. It also expands on and amplifies the guidance given by the Department for Business, Energy and Industrial Strategy (BEIS) through the "National Framework for Response to Cyber Incidents in the Civil Nuclear Sector". In order to discharge their regulatory responsibilities, ONR also require duty holders to report Cyber Incidents to them. This Policy does not include the specific requirements of ONR, and duty holders must therefore additionally familiarise themselves with ONR's policy requirements and additionally ensure that when reporting Cyber Incidents to CERT-UK that ONR are informed too.

Key Source Documents:
National Cybersecurity Incident Management Policy March 2014 Version 3.0 (CERT-UK)
National Framework for Response to Cyber Incidents in the Civil Nuclear Sector (BEIS)
ONR Policy for Cyber Security Resilience (Detection, Incident Response, Recovery)
Nuclear Industries Security regulations (2003)

Applicability of Policy

3. This policy applies to the NDA, its Site Licence Companies (SLCs) and its Subsidiary organisations.

Definitions

4. **What is a Cyber Incident?** A Cyber Incident is defined as a single or series of unwanted or unexpected cyber events that have a significant probability of compromising business operations and threatening cybersecurity. Details of the specific type of Cyber Incident that need be reported are listed at para 6.

5. **A National Cyber Incident is defined as:**
A situation or event in cyber space that threatens or causes serious: damage to human welfare; cost to the UK; sustained theft of strategically important intellectual property; disruption; or loss of reputation with impacts either in cyber space, the real world or both that require coordinated inter-agency response to manage. Some examples are:

- Credible intelligence is received that a malicious action in cyber space is imminent and likely to result in the impacts described above; or,
- The discovery of vulnerability in Information and Communications Technology (ICT) that is likely to be exploited to cause the impacts described above and for which there is no clear immediate remedy.

Key factors in successfully managing Cyber Incidents include timeliness; coordination; effective decision-making; collaboration and information sharing.

6. **What types of Cyber Incident should be reported to CERT-UK?** The following types of incident are covered by this policy and should be reported:

- **Unauthorized access** – attempted or successful logical or physical access, without permission, to a network, system, application, data or other resource.

[1] National Cybersecurity Incident Management Policy March 2014 Version 3.0

- **Denial of Service** – an attack or attempted attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This includes being a participant or victim in a denial of service attack.
- **Malicious code** – deliberate or accidental installation of malicious software (virus, worm, Trojan, other code-based malicious entity) that infects an operating system or application.
  Improper usage – violation of acceptable computing use policies. Organisations should take a judgement, based on severity, on thresholds for reporting these types of incidents.
- **Scans/Probes/Attempted access** – activity that seeks to access or identify machines, open ports, protocols, running services, or any combination for later exploitation. This activity would not directly result in compromise or denial of service, which would fall under different categories, but could for example include blocked spear phishing attacks.
- **Investigation** – unconfirmed incidents that are potentially malicious or anomalous activity deemed to warrant further review.
- **Technical failure/Misconfiguration issues** – although not strictly a cybersecurity issue, this form of incident will be of interest if it is likely to result in significant public interest or where the affected systems provide a critical process or function. **This form of incident will always be of interest, and should be reported, unless it has been demonstrated that it occurred as a result of a technical error, rather the deliberate act of an insider**.
  If in doubt **– report it!**
  And also remember to **– notify ONR!**

Why should Cyber Incidents be Reported?

7. There are a number of reasons for reporting cybersecurity incidents, including:
   - To help protect other elements of the NDA from similar attacks.
   - The regulatory requirement is that **all** cybersecurity incidents that have an adverse impact on a computer or on nuclear security, or have the potential to do so, should be reported.
   - To support the effective investigation, including forensics, and prosecution of online fraud and cyber-enabled crime.
   - To seek assistance or advice, potentially including technical analysis, to support incident response and remediation; and/or provide context to inform understanding of ongoing or recently occurred incidents. In the case of the CNS national capabilities may be deployed in response to the incident.
   - To enable UK authorities to build an informed understanding of the types of threats affecting UK industry, and for this information to be shared across industry sectors to inform network defenders and risk owners.
   - Contractual obligation.

Responsibility for Reporting Cybersecurity Incidents

8. Responsibility for reporting Cyber Incidents, or any incident that could be cyber-related, lies with duty holders.

How should Incidents be Reported and to Whom?

9. Incidents should be reported to CERT-UK using the reporting template and distribution list at Appendix 1. Duty holders should also make an initial verbal report to the NDA and ONR.

CERT-UK

10. CERT-UK is the UK National Computer Emergency Response Team, formed in March 2014 in response to the National Cyber Security Strategy. CERT-UK has four main responsibilities that flow from the UK's Cyber Security Strategy:

- National cyber-security incident management
- Support to Critical National Infrastructure companies to handle cybersecurity incidents
- Promoting cyber-security situational awareness across industry, academia, and the public sector
- Providing the single international point of contact for co-ordination and collaboration between national CERTs.

More details of how CERT-UK responds to Cyber Incidents can be found at Appendix 2.

It is possible that the first indication that a duty holder has that a cyber-attack has occurred will come in the form of a report from CERT-UK, GOVCERT or another government department or agency. In order to ensure that all key addressees are kept informed of Cyber Incidents and response all duty holders should ensure that all such incidents are reported using the form and distribution list at Appendix 1.

National Cyber Incidents

11. Details of how the CERT-UK classifies and manages Cyber Incidents can be found at Appendix 2.

Cyber Incident Management within the NDA Estate

12. **Primary responsibility for responding to Cyber Incidents lies with duty holders, as does the responsibility for developing the capability to detect, deter and respond to such incidents**. Equally, responsibility the production of incidents response plans and for exercising those plans on a regular basis also lies with duty holders. The role of NDA is to:

a. Provide support to duty holders.

b. Ensure that appropriate Cyber Incident threat and response information is disseminated across the estate in a timely manner.

c. Assist duty holders, CERT-UK, ONR and government to develop a clear understanding of the impact of any Cyber Incident on the NDA, its Site Licence Companies and/or its Subsidiaries.

d. Help co-ordinate the development of key messages for government Ministers and the media.

e. Help identify what additional resources duty holders might need in order to respond adequately to a Cyber Incident.

13. When an organisation within the Estate reports an incident to CERT-UK and the NDA, the NDA will consider convening the NDA Cyber Incident Response Co-ordination Committee (NCIRCC). The decision to convene the NCIRCC will be the responsibility of the NDA's Director of Security, Safety, Safeguards & Environment (Dir SSSE) or, in his absence, the NDA's Head of Security. The NCIRCC will co-ordinate the wider NDA response to an incident.

Core members of the NCIRCC are:

Chair: Director Business Services/NDA SIRO	
Director Business Services (or nominated deputy)	Director SSSE
Director Communications (or nominated deputy)	Head of Legal Services
Head of Security	SLC/NDA subsidiary representatives
Information Security Operations Manager - Secretariat	Information Security Assurance Manager – Secretariat
Head of IT (for incidents impacting on NDA's network)	ONR Representative
Other NDA personnel as required	CNC Representative (if required)

14. Meetings of the NCIRCC will be timed to be co-ordinated with those of the target SLC (normally the NCIRCC will be timed to follow any SLC Cyber Incident response meeting so that it can be informed by the findings of that meeting). The NCIRCC will seek to:

Develop an Understanding of the Incident

The Incident
What has happened?

Who has it been reported to?

Is the incident still ongoing?

Does the SLC/subsidiary think that the incident and its impacts been contained?

Are we confident in that assessment?

What action has CERT-UK taken and what further action is planned?

Is the incident being treated as an 'extraordinary occurrence or national incident?

What are the 'known unknowns?

What is the level of ministerial interest?

What is the level of media interest?

Do we need to revise our media lines and, if so, how?

Identify

Additional Information requirements

Determine

What are the SLC's requirements for support?

What, if any, are the implications for the rest of the estate and rest of the CNS?

Have any requirements been laid on NDA by CERT-UK, DECC or wider Govt?

What is the status of agreed actions?

Have we identified any new actions?

15. A set of minutes and a list of actions will be produced after each NCIRCC by Information Security Operations Manager or Information Security Assurance Manager. The Chair of the NCIRCC will set the distribution list for the minutes and action list; as a minimum the minutes will be distributed to:
BEIS
CERT-UK
GOVCERT UK
ONR
CNC
Target SLC
Other NDA SLCs
EDF (if appropriate)

16. The NCIRCC Chair will set the frequency of NCIRCC meetings to meet the tempo of incident response activity. It is likely that the frequency of meetings will reduce as the incident moves into the investigation and recovery phases. At an appropriate point the NCIRCC chair will stand the NCIRCC down. All incident participants will be informed in writing of the date/time that the NCIRCC will stand down. The closing down e-mail/note will also detail the process that will be adopted for identifying the lessons that all participants can draw from the incident and the response to it.

Appendices:
1. Template for reporting incidents to CERT-UK.
2. National Cyber Incident Management.

Appendix 1

TEMPLATE FOR REPORTING INCIDENTS TO CERT-UK

This template is provided to assist organisations report incidents in to CERT-UK. This can be done by email to incidents@cert.gov.uk or verbally on 0207 147 4411. Reporting using the categories below is not essential, but will assist us in triaging and responding to the information provided. Please provide as much detail as possible.
A PGP key can be provided prior to submitting this report; please contact the Incident Handling team using the contact details above.

REPORTING ORGANISATION NAME:	
YOUR REFERENCE:	

TECHNICAL POINT OF CONTACT:

Name:		Tel:	
Role:		Email:	

TIMINGS (WHERE KNOWN ALL IN UTC USING DD/MM/YYYY FORMAT):

FIRST MALICIOUS ACTION:	DD/MM/YYYY
INITIAL COMPROMISE:	DD/MM/YYYY
FIRST DATA EXFLITRATION:	DD/MM/YYYY
INCIDENT DISCOVERY:	DD/MM/YYYY
INCIDENT CONTAINED:	DD/MM/YYYY

WHICH SYSTEM(S) ARE AFFECTED?

HOW IS THIS INCIDENT AFFECTING THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF THOSE SYSTEMS?

TECHNICAL DETAIL (Please include as much detail as possible, including observables such as IP addresses, domain names, file hashes etc.):

ACTION TAKEN SO FAR:

THE FOLLOWING SAMPLES ARE AVAILABLE FOR FURTHER ANALYSIS ON THIS INCIDENT IF REQUESTED (Malware samples, pcaps, log files etc.):

Distribution of Incident Reports:

CERT – UK	incidents@cert.gov.uk
CNC	ccc@cnc.pnn.police.uk
BEIS	*TBC*
ONR	cns.infosec@onr.gsi.gov.uk
NDA	security.incident.response@nda.gov.uk
SSA	ssa.cyber.incident@magnoxsites.com
EDF	*Optional – is the incident of interest to the generating sector?*

Appendix 2 – National Cyber Incident Management

1. The National Cybersecurity Incident Management policy describes the roles and responsibilities of the national organisations that have a responsibility for responding to national-level Cyber Incidents. Responsibility for coordinating that overall national response lies with CERT-UK. Cyber Incidents will be categorized by CERT-UK and will, depending on the assessed severity of the incident, generate varied levels of response from government.

2. CERT-UK is not resourced to provide incident responders to assist with on-site investigation and remediation efforts, but liaises closely with specialist incident response companies such as those sponsored by CPNI and CESG who are. However, where possible the CERT-UK Incident Handling team will support initial technical triage to confirm the nature and possible scope of an incident; provide additional context around incidents, drawing on the various information sources to which it has access; and provide a point of contact for the duration of the incident response effort. Depending on the severity of the incident, or the assets that are at risk, other national strategic capabilities may be deployed in support of the response.

3. In the **steady state** organisations respond to incidents without the need for national coordination. Information about incidents is reported to provide situational awareness and share knowledge. More serious incidents are reported to "CERT-UK" which is responsible for declaring a national incident.

Level 1 – Significant Emergency

4. The first level of response described here is the equivalent to the CONOPS definition of a Significant Emergency, it is declared by CERT-UK. This requires central government involvement or support, which will include invoking the **Cybersecurity Coordination Team** (CSCT) which is chaired by the **Cyber Incident Coordinator** (CIC). CERT-UK is responsible for convening the CSCT which brings together expertise from across government, the Security and Intelligence Agencies, and Law Enforcement. However, there is no requirement for the fast inter-agency decision making which necessitates the activation of the collective central government response in COBR.

5. This threshold can be considered to be met by any incident which:

- **a.** Impacts on networks supporting the operation of Critical National Infrastructure:
- **b**. Impacts on HMG networks with an obvious link to national security or online service delivery;
- **c.** If not contained and mitigated locally it might have serious long term impacts – sometimes known as 'Rising Tide' scenarios;
- **d**. Involves widespread theft of intellectual property or economic espionage against the UK which may result in major financial loss or loss of technical advantage;
- **e**. Has a media profile which is sufficient to undermine public trust and confidence in online services and the government cyber response; or
- **f.** Requires greater than usual levels of engagement with international allies and partners.

Level 2 – Serious Emergency

6. At emergency level 2 – **Serious Emergency** – CERT-UK may convene a group of senior officials, the Cyber Incident Management Group (CIMG), if decisions on resources, policy implications or wider positioning of the response, needs to be made or if COBR is going to be activated and additional briefing or support is required. This second level of response equates to the CONOPS definition for a Serious Emergency, which has, or threatens, a wide and/or prolonged impact requiring sustained central government co-ordination and support from a number of departments and agencies. The central government response to such an emergency would be co-ordinated from COBR(O) or COBR. CERT-UK will help inform the decision to activate COBR and then support COBR.

7. **Level 2** can be considered to be any incidents which have a:

- **a**. Significant impact on CNI or HMG systems providing critical services
- **b**. Serious harm to human welfare e.g. one effecting supply chain (such as food delivery), control systems for water or power supply, or causing disruption to national communications;
- **c**. Significant reputational impact on the UK;
- **d**. Grave public concern due to either the impact of the cybersecurity incident or its cause (e.g. terrorism or a destructive or disruptive Nation State attack); or
- **e**. The effects of the impact are beyond UK cyberspace and have an international dimension requiring action by or support from international partners beyond normal levels of engagement.

The threshold can be met by a credible and imminent threat of the above.

Level 3 – Catastrophic Emergency

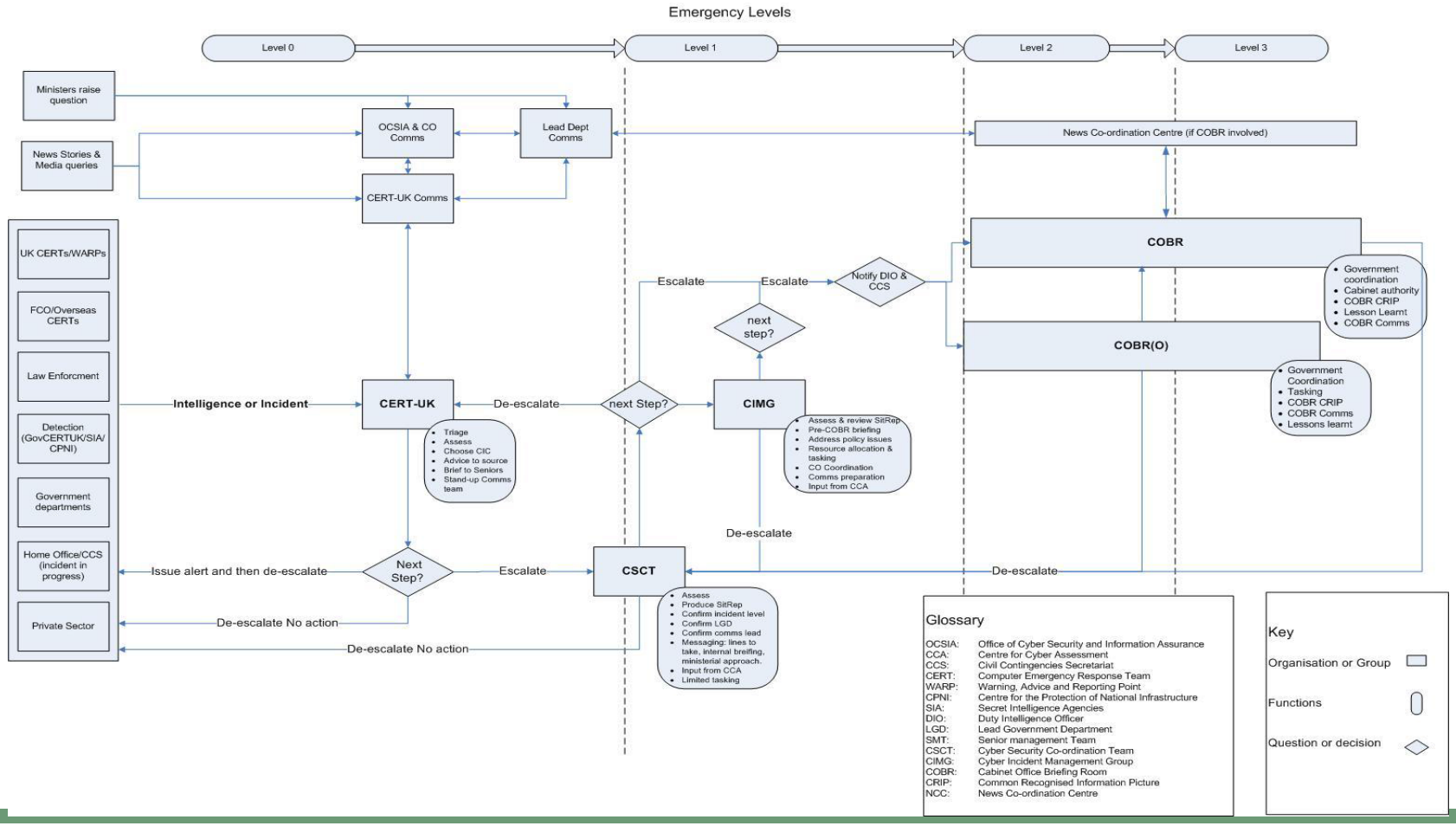
8. At emergency level 3 – **Catastrophic Emergency** – there will be a COBR chaired by the Prime Minister with CIMG providing support and CSCT continuing to coordinate the operational cyber response and feeding information into the situation report. Events of this severity are extremely rare.

9. Examples of cybersecurity incidents that might justify the calling of a Level 3 Catastrophic Emergency are:

- **a.** Events that have an extreme impact on the ICT underpinning Critical National Infrastructure affecting more than one sector providing essential services (e.g. simultaneous loss of power, water and telecommunications) affecting a single region or loss of a single essential service to the whole of the UK over a sustained period;
- **b.** When the source of the cyber-attack is assessed to be from a nation state or terrorist group and is assessed as deliberately designed to have a widespread destructive impact to the UK; or
- **c.** The effects of the impact are global.

The threshold can be met by a credible and imminent threat of the above.

10. The national structures for responding to cybersecurity incidents at each incident level are described in the diagram below.


Emergency Levels
Level 0
Level 1
Level 2
Level 3
Ministers raise question
News Stories & Media queries
OCSIA & CO Comms
Lead Dept Comms
CERT-UK Comms
News Co-ordination Centre (if COBR involved)
UK CERTs/WARPs
FCO/Overseas CERTs
Law Enforcment
Detection (GovCERTUK/SIA/ CPNI)
Government departments
Home Office/CCS (incident in progress)
Private Sector
Intelligence or Incident
CERT-UK
De-escalate
next Step?
CIMG
Escalate
Escalate
Notify DIO & CCS
next step?
COBR
COBR(O)
Triage
Assess
Choose CIC
Advice to source
Brief to Seniors
Stand-up Comms team
Assess & review SitRep
Pre-COBR briefing
Address policy issues
Resource allocation & tasking
CO Coordination
Comms preparation
Input from CCA
Government coordination
Cabinet authority
COBR CRIP
Lesson Learnt
COBR Comms
Government Coordination
Tasking
COBR CRIP
COBR Comms
Lessons learnt
De-escalate
Issue alert and then de-escalate
Next Step?
Escalate
CSCT
De-escalate
De-escalate No action
De-escalate No action
Assess
Produce SitRep
Confirm incident level
Confirm LGD
Confirm comms lead
Messaging: lines to take, internal briefing, ministerial approach.
Input from CCA
Limited tasking
Glossary
OCSIA: Office of Cyber Security and Information Assurance
CCA: Centre for Cyber Assessment
CCS: Civil Contingencies Secretariat
CERT: Computer Emergency Response Team
WARP: Warning, Advice and Reporting Point
CPNI: Centre for the Protection of National Infrastructure
SIA: Secret Intelligence Agencies
DIO: Duty Intelligence Officer
LGD: Lead Government Department
SMT: Senior management Team
CSCT: Cyber Security Co-ordination Team
CIMG: Cyber Incident Management Group
COBR: Cabinet Office Briefing Room
CRIP: Common Recognised Information Picture
NCC: News Co-ordination Centre
Key
Organisation or Group
Functions
Question or decision