Office for
Nuclear Regulation

Welcome
ONR NGO Forum meeting
23 September 2020

Office for Nuclear Regulation

Chief Nuclear Inspector's Update

Mark Foy - CNI

Office for Nuclear Regulation

NGO requested topics

- Hunterston B R3 decision;
- Broader AGR consideration;
- Regulatory news/updates from across the defence sites;
- Latest news in relation to SZC, Bradwell and Wylfa;
- Update on any enforcement action;
- ONR view/update on changes announced at PHE.

Office for Nuclear Regulation

Other topics from the CNI

- ONR site attendance during Covid;
- Recent incidents;
- Judicial review of AWE REPPIR determination;
- CNI annual report on safety security safeguards performance

Office for Nuclear Regulation

Hunterston B Reactor 3 decision

- **ONR has given permission** for EDF NGL to return Reactor 3 back to service for a limited period (16.425 TW days which is approximately six months' operation).
- **ONR assessment focussed on** ensuring that the reactor could maintain safety requirements in operational and fault conditions.
- **ONR inspectors engaged extensively** with EDF NGL to discuss the technical challenges and issues posed.
- **ONR is satisfied** with the detailed safety justification developed by EDF NGL over the preceding two years.

Office for Nuclear Regulation

Remainder of AGR Reactor Fleet

- **12 further AGR reactors** in addition to the 2 at HNB operate in GB.
- **These reactors all use graphite** moderated cores and are expected to experience similar cracking behaviour.
- **ONR will assess each reactor individually.** Any further safety cases would be analysed thoroughly to ensure they provide an adequate justification that the reactor in question can operate safely.
- We expect to make a decision soon on whether to permission the restart of Hunterston B Reactor 4.

Office for Nuclear Regulation

Update from the Defence sector

- **AWE to face prosecution** by ONR under section 3 of HSWA 74 after a contractor narrowly avoided injury from a 415V electrical source.
- **ONR has issued DRDL** an improvement notice related to shortfalls in maintenance procedures.
- **Along with the Devonport Senior User Group** ONR have established a Boat-Acquisition Senior User Group. We will seek to influence the right investment in support of nuclear safety .

Office for Nuclear Regulation

Sizewell C, Bradwell B and Wylfa

- **NNB SZC - Nuclear Site Licence application submitted** 30th June 2020. Assessment of the application is underway.
- **Step 4 of the Generic Design Assessment** of the Chinese HPR 1000 continues. The completion of GDA and the submission of the Bradwell Nuclear Site Licence application are expected in 2022
- **Hitachi is withdrawing from the UK nuclear market** and the future of the Wylfa Site is uncertain

Office for Nuclear Regulation

Update on announced changes to PHE

- **ONR does not have significant concerns** at the present time.
- **We have monitored the impact** on the areas of PHE that deal with radiation research/advice, commercial radiation services and emergency radiological response.
- **Plans appear** to be to retain PHE's UK radiological function in the new reorganisation.
- **ONR will maintain continued interest** in the change and will continue to monitor how the changes may impact the functions PHE delivered and ONR.

Office for Nuclear Regulation

ONR Site attendance during COVID-19 Pandemic

ONR principles for on-site attendance

- Obtain adequate assurance on key areas of compliance – intelligence based and risk informed;
- Inform the delivery of assessment/permissioning activities;
- Conduct investigations where the work cannot be done remotely;
- Enable understanding of plant where this is not possible remotely;
- Access classified information that cannot be done remotely;
- Enable staff handovers and site familiarisation;
- Respond to whistleblowing cases;
- Gain independent assurance of supply chain activities;
- Engender stakeholder confidence in our regulation.

Office for Nuclear Regulation

Recent incidents

- **Sellafield site electrical storms** in August, led to power dips, this impacted steam supplies that support operational activities, resulted in safe shutdown of various facilities.

- **Potentially unstable chemical discovered** by Sellafield as part of a routine inspection, the chemicals disposed of in a controlled manner, no potential impact on nuclear safety.

Office for Nuclear Regulation

CNI Annual Report on Great Britain's Nuclear Industry

Regulatory priorities remain:

- Management of ageing facilities
- Conventional health and safety performance
- Delivering a holistic approach to nuclear security

In light of Covid-19 will be adding a fourth theme:

- Ensuring adequate pandemic resilience

Publication – November 2020

Office for
Nuclear Regulation

Thank you for listening

Questions and Discussion

Office for Nuclear Regulation

Refreshment break

Office for
Nuclear Regulation

Hinkley Point C Update

Mike Finnerty, Deputy Chief Inspector and Director,
New Reactors Division

Office for Nuclear Regulation

ONR On-Site Presence at HPC

General principles for HPC on-site interventions:

- Obtain assurance on key areas of compliance, particularly those associated with construction activities
- To inform decisions to permit ongoing construction
- Conduct investigations where the work can't be done remotely
- Gain independent assurance of supply chain activities

From lockdown to June – 2 onsite interventions plus 8 remote inspections

Gradual increase in on-site presence from July

Office for Nuclear Regulation

Ground Granulated Blast-Furnace Slag (GGBS) Silo Collapse Investigation

- We continue to work with HSE experts gathering our own evidence from site
- Awaiting outcome of licensee's own investigation in full - this is just one source of evidence to help inform our regulatory response.
- Gathering of evidence is a painstaking exercise, with all silo components retained
- Still too early to speculate on causes of incident
- We will form an independent view once all evidence has been gathered

Office for Nuclear Regulation

ONR Focus at HPC

- We continue to seek assurances that construction is progressing with required levels of quality to meet nuclear safety and security standards
- Continue to focus on supply chain activities to ensure equipment manufactured to right levels of quality
- Gain assurance that HPC continues to focus on conventional safety to ensure no accidents on site
- Gain evidence that HPC continues to meet Covid-19 public health guidelines

Office for
Nuclear Regulation

Thank you for listening
Questions and Discussion

Office for Nuclear Regulation

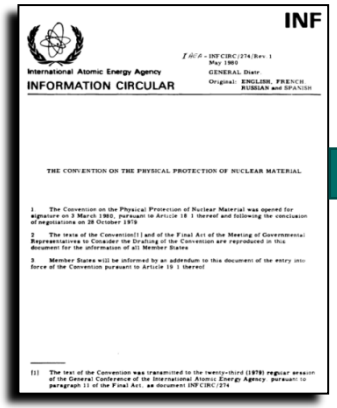
Regulation of Cyber Security across the Civil Nuclear Sector

Paul Fyfe
Deputy Chief Inspector & Director
Civil Nuclear Security & Safeguards

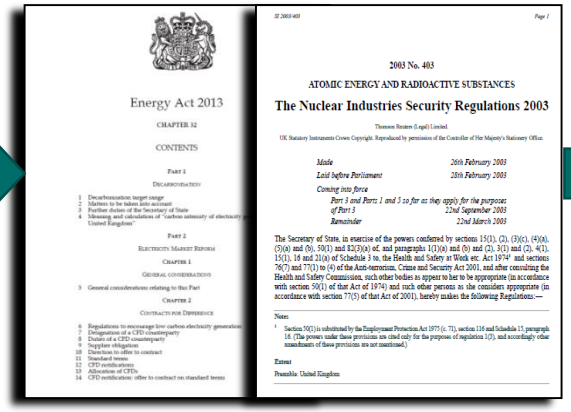
Office for Nuclear Regulation

Background to Security Regulation

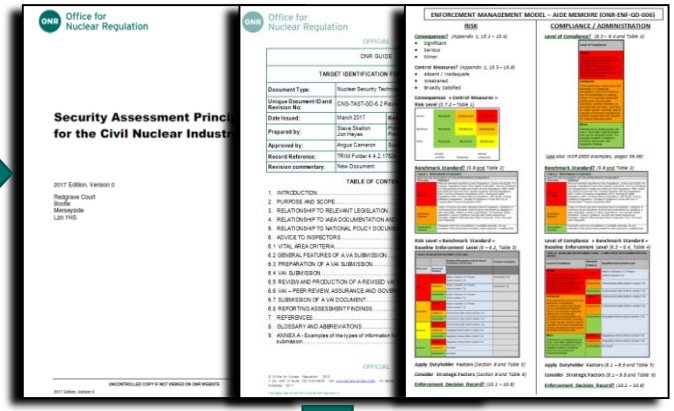
International Legislation



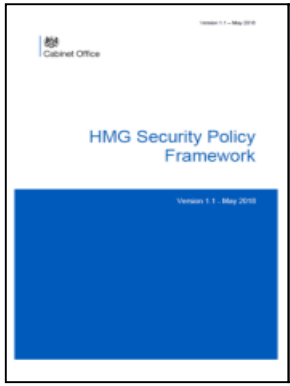
National Legislation

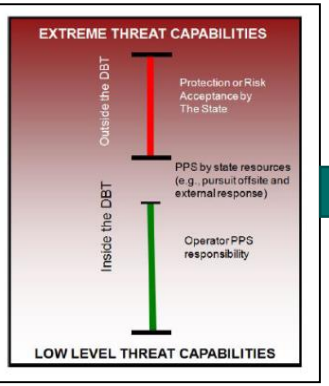


Regulatory Approach



Risk Appetite





Office for Nuclear Regulation

Our Scope – NISR 2003

✓ Those who Store Category I – IV nuclear material on **civil** nuclear licensed sites
✓ Other radioactive material on **nuclear licensed sites** e.g. radioactive sources, waste streams
✓ Use or storage of category I – III nuclear material at other premises
✓ Nuclear construction sites within 5 km of existing nuclear premises
✓ Security of Category I-III quantities of nuclear material in transit
✓ Holders of Sensitive Nuclear Information (including the Supply Chain)
✓ Those employed in the civil nuclear industry

✗ Security of radioactive sources held outside nuclear licensed sites
✗ Nuclear premises operated primarily or exclusively by MOD or its contractors

Ministry of Defence

Environment Agency

Office for Nuclear Regulation

Outcome Focused Cyber Regulation

- We ensure duty holders' cyber and information security arrangements are aligned and coherent with broader security activities.
- We require duty holders to have a mature understanding of their security risks, informed by current threat intelligence.
- We encourage duty holders to implement an appropriate balance between cyber 'protection' and 'detection/response/recovery.'
- We expect dutyholders to undertake an intelligence-led programme of assurance activities including auditing, monitoring, and testing of cyber defences, and exercising incident response capabilities.
- ONR has a dedicated cyber security specialism, and increased the team under a dedicated Professional Lead.
- Our cyber inspectors work closely with other security and safety specialists to deliver comprehensive and effective regulation.

Office for Nuclear Regulation

Security Assessment Principles

Strategic Enablers - Objectives focused on creation of the right conditions to support high reliability, disciplined operations.		**Secure Operations** - Objectives focused on the implementation and maintenance of nuclear security.	
FSyP I	Leadership and Management for Security	**FSyP VI**	Physical Protection Systems
FSyP II	Organisational Culture	**FSyP VII**	Cyber Security & Information Assurance
FSyP III	Competence Management	**FSyP VIII**	Workforce Trustworthiness
FSyP IV	Nuclear Supply Chain Management	**FSyP IX**	Policing & Guarding
FSyP V	Reliability, Resilience and Sustainability	**FSyP X**	Emergency Preparedness and Response Arrangements

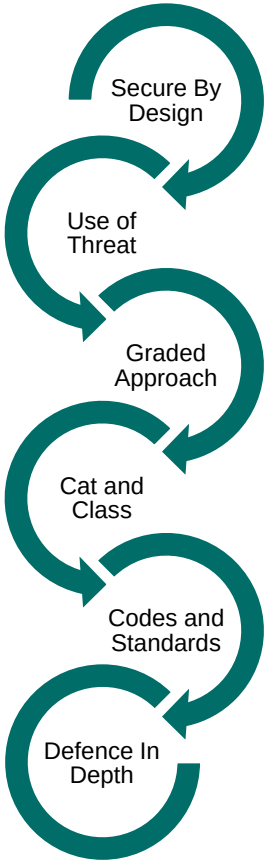
Office for Nuclear Regulation

Fundamental Security Principle - 7

FSyP 7 - Cyber Security and Information Assurance	Effective Cyber and Information Risk Management	SyDP 7.1
Dutyholders should maintain arrangements to ensure that CS&IA risk is managed effectively.		
FSyP 7 - Cyber Security and Information Assurance	Information Security	SyDP 7.2
Dutyholders should maintain the confidentiality, integrity and availability of sensitive nuclear information and associated assets.		
FSyP 7 - Cyber Security and Information Assurance	Protection of Nuclear Technology and Operations	SyDP 7.3
Dutyholders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities.		
FSyP 7 - Cyber Security and Information Assurance	Physical Protection of Information	SyDP 7.4
Dutyholders should adopt appropriate physical protection measures to ensure that information and associated assets are protected against a wide range of threats.		
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.		

Office for Nuclear Regulation

The Graded Approach to Cyber Security



1. Dutyholders categorise assets:

OFFICIAL	SECRET	TOP SECRET
The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.	HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

SNI (includes IT)

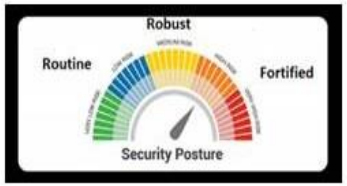
Critical	Large Off Site Release
Major	Limited offsite release
Significant	Significant release in area of plant not expected by design
Minor	Minor Contamination in plant area not expected by design

OT

2. Determine Outcome:

1	Complete confidence it will protect against attack
2	High level of confidence it will protect against attack
3	Resistance to attack
4	Identify an attack has taken place

3. Apply:



Posture

to each

Identify
Protect
Detect
Respond
Recover

Function

Office for Nuclear Regulation

Relevant Good Practice – ‘Standards’

Standard	Definition	
Defined	Minimum standard specified by Acts, Regulations, Orders and Approved Codes of Practice (ACoP). e.g. Nuclear Industries Security Regulations 2003.	
Established	Codes of Practice and other standards linked to legislation, published or commonly known standards of performance interpreted by regulators or other specialists, industry or other organisations. e.g. Licence Conditions, Security and Safety Assessment Principles, Cabinet Office Security Policy Framework, TIGs, TAGs, IAEA Standards, NIST, ISO Standards, NCSCs CAF, Cyber Essentials, CPNIs CMAT.	
Interpretative	Standards which are not published or available generally, but are examples of the performance needed to meet a general or qualified duty. e.g. Industry Cloud Security Principles.	

Office for Nuclear Regulation

NTI BUILDING A SAFER WORLD

2020 NTI Report

- The UK scores high in every category over which ONR has influence, and has maintained (from the 2018 index) its first place ranking for ‘nuclear security and control measures’ – the measure that is the closest reflection of our regulatory framework.
- The Index is a recognised ‘assessment and tracking’ of global nuclear security conditions. It promotes actions to strengthen nuclear security and build confidence, and it highlights progress and trends over time.
- One of the objectives of the index is to identify those countries which demonstrate good practice in nuclear security, which those less developed nations could seek advice and guidance from. The UK falls into that top category.
- The scoring from NTI can be quite rigid, e.g. expecting dutyholders to conduct annual penetration testing. Our approach adopts an intelligence-led programme of assurance activities.

Office for Nuclear Regulation

Current and Future Challenges…

- Legacy OT systems weren't designed to be exposed to the internet, and it isn't always obvious when they have been.
- Convergence with enterprise IT – new OT can be attacked like enterprise IT.
- Complexity and rate of change of technology – we lack natural instincts.
- Software can have millions of lines of human written code. This makes eradicating errors and vulnerabilities and gaining requisite assurance increasingly challenging.
- Vulnerabilities in the supply chain – an ever increasing problem.
- High risk vendors vs the need for dutyholders to encourage innovation.
- Vulnerability data available from governments, vendors, specialist companies, presenting both an opportunity and a challenge.
- Insufficient cyber-trained staff (globally), and large proportions of the population (globally and within nuclear businesses) do not understand the implications of their personal actions on organizational cyber security.

Office for
Nuclear Regulation

Thank you for listening

Questions and Discussion