

Regulatory Triage Assessment

Title of measure	Changes to Civil Nuclear Security Regulations
Lead Department/Agency	Department of Business, Energy and Industrial Strategy
Expected date of implementation	31 March 2017
Origin	Domestic
Date	November 2016
Lead Departmental Contact	Mike Sugden
Departmental Triage Assessment	Low-cost regulation (fast track)

Rationale for intervention and intended effects

Policy Background

Government plays a lead role in ensuring that the UK civil nuclear security regime is functioning effectively. The purpose of the nuclear security regime in the UK is to ensure that nuclear facilities are protected from threats, and that nuclear material both at sites and in transit, together with sensitive information and technology, are protected from theft and sabotage.

The UK has international obligations under the Convention on the Physical Protection of Nuclear Material (CPPNM). The CPPNM is an international legally binding treaty to which the UK is a party that sets the basic legal framework for the security of civil nuclear materials during use, storage and transportation. It places certain obligations on 'State Parties' to make provision for civil nuclear security. Among other obligations, it places obligations on State Parties to have a legislative and regulatory regime to govern civil nuclear security, which is kept under review.

The Nuclear Industries Security Regulations 2003 (NISRs) is the primary piece of legislation regulating security in the UK's civil nuclear industry. These regulations require all nuclear licensed sites and sensitive nuclear information to be subject to security plans, and all transportation of nuclear material subject to transport security statements, such plans and statements having been approved by the independent statutory regulator, the Office for Nuclear Regulation (ONR).

The NISRs are overseen and enforced by the ONR and have been amended several times since 2003 to ensure that they remain robust and effective. The ONR has produced supporting guidance, known as the National Objectives, Requirements and Model Standards (NORMS), for the civil nuclear industry. The NORMS provide more detail about how duty holders can comply with their statutory obligations contained in the NISRs.

The ONR are in the process of producing new security guidance, known as the Security Assessment Principles (SyAPs) that will replace NORMS. SyAPs will continue the move to more outcome-focused regulation for security, as well as placing more emphasis on mitigating emerging threats, in particular that relating to Cyber Security and Information Assurance (CS&IA). SyAPs is due to be issued to the nuclear industry in March 2017. The development of SyAPs has led BEIS to review the NISRs to ensure that SyAPs requirements are consistent with the statutory requirements in NISRs.

The review established that no specific amendments to the NISRs were required to ensure consistency with SyAPs. However, several changes were identified to ensure that the statutory regime remains comprehensive and robust. These changes will be complementary to, but not dependent on, the new SyAPs guidance.

Policy Objectives and Intended effects

These regulations will further clarify roles and responsibilities in the civil nuclear sector,

ensure that changes in government policy on nuclear security are fully implemented, and ensure industry is properly mitigating risks.

These regulations:

- Ensure that a responsible person in relation to the premises now has a duty to ensure that there is an approved security plan in place for their premises
- Extend the contingency requirements for the site security plans and transport security plans to include clearer references to cyber threats
- Modify the ONR's responsibilities regarding the personnel security regime so that they are in line with the current regulatory approach.
- Remove reference to extraneous classification guidance for Sensitive Nuclear Information

More detail on the policy objectives and intended effects is below:

1. **Responsible Person for an Approved Nuclear Site Security Plan** – This change relates to the requirement in Regulation 4 of the NISRs that an approved nuclear site security plan be in place for each nuclear premises. The current requirement does not specify upon whom the duty is placed. These regulations clarify the position by specifying that it is the responsible person in relation to each nuclear premises who has the duty to ensure that there is an approved nuclear site security plan in place, and make it a criminal offence for the responsible person to fail to do so. There is a linked amendment to Regulation 25 to create an offence when there is no approved Nuclear Site Security Plan in place for nuclear premises. This is consistent with the general approach within the 2003 Regulations, where non-compliance by a responsible person with any of the obligations placed on them constitutes an offence. These changes create a new criminal offence. A Justice Impact test has been completed in respect of this change which has been approved by the MOJ, and also approved in Scotland and sent for information to Northern Ireland. (NI has no nuclear sites).
2. **Cyber Security and Information Assurance** – This change is aimed at mitigating emerging threats in the field of Cyber Security and Information Assurance, in particular the threat of cyber attack and the loss of Sensitive Nuclear Information. These regulations will require nuclear site security plans to set out the steps to be taken in the event of theft, loss or unauthorised disclosure of, or unauthorised access to, Sensitive Nuclear Information, or any attempt to do so. It is hoped that building such steps, which the Government anticipates will include contingency arrangements and mitigations, into nuclear site security plans will ensure that information security risks are effectively managed.
3. **Personnel Security** – This change is aimed at allowing for changes in practice in the process by which nuclear premises' 'relevant personnel' are approved as suitable in security terms. Instead of solely approving all 'relevant personnel' itself, these regulations provide for the ONR to approve a broader personnel security regime in an organisation which, as well as ONR approval of 'relevant personnel', will include approving aftercare and review processes for those individuals. In addition it allows for the responsible person at nuclear premises to approve some 'relevant personnel' in limited circumstances. This change is to ensure consistency with the current approach to personnel security regulation in the sector where, as well as undertaking vetting functions, the ONR will assess the industry's broader arrangements to ensure effective personnel security which is undertaken in line with HM Government personnel security policy.
4. **Information Security Guidance** – The final change would remove an extraneous reference to documentation which in the past has provided requirements to the nuclear industry on classifying Sensitive Nuclear Information. The nuclear industry will continue to be obliged to comply with the HM Government Security Policy Framework classification policy.

Viable policy options (including alternatives to regulation)

Option 1: (preferred) amend regulations in order to help ensure the continued security of nuclear facilities, nuclear material in transport and sensitive nuclear information. This will maintain public and parliamentary acceptability of continued security in the civil nuclear sector, as well as ensuring continued compliance with the UK's international obligations under the CPPNM.

Option 2: Voluntary compliance by the nuclear industry with a looser regulatory regime. Nuclear sites have a vested commercial interest in maintaining robust site security. It is highly likely that even without regulation that nuclear sites would maintain significant site security. However this would also run the risk that security cuts would be made for cost saving reasons at some sites, and that significant gaps would appear, without regulation. In addition the UK would be in contravention of its international obligations under the CPPNM. This is therefore not judged to be a viable option.

Initial assessment of impact on business

The regulations will impact the UK civil nuclear industry including decommissioning nuclear sites, operating nuclear power stations all run by EDF, nuclear fuel cycle sites at approved carriers of nuclear material, and nuclear new build companies. The regulations will also impact on the ONR, the Nuclear Decommissioning Authority and any holders of Sensitive Nuclear Information. Defence sites are exempt.

A 4-week consultation was held in July 2016, which consulted 13 key organisations including EDF, the Nuclear Decommissioning Authority (NDA) (who in turn consulted each NDA Site Licence Company and subsidiary affected by the amendments), and nuclear fuel cycle sites at Springfields and Capenhurst. In addition two representative bodies for the sector - the Nuclear Industry Association and Safety Directors Forum – were consulted, who in turn consulted their members. Those invited to respond to the consultation were asked to provide an assessment of the impact of the costs and benefits of the regulatory changes to their organisation.

Cyber Security and Information Assurance

Some respondents to the consultation said that there would be costs associated from implementing the CS&IA requirements in these regulations. We assess that costs of the CS&IA requirements in these regulations will be minimal: The ONR already have the powers in the NISRs to require organisations in the civil nuclear sector to have contingency arrangements and mitigations in the event of theft, loss or unauthorised disclosure of, or unauthorised access to, Sensitive Nuclear Information, or any attempt to do so. These regulations make it a requirement for these arrangements to be included in Nuclear Site Security Plans, and therefore there will be administrative costs for those organisations affected to update these plans as a result (see 'costs' section).

Responsible Person for an approved Nuclear Site Security Plan

This change will have no cost on business. Relevant civil nuclear organisations are already required by the NISRs to have an approved Nuclear Site Security Plan in place. These regulations clarify whose responsibility within an organisation this requirement falls to, and has no impact on industry obligations.

Personnel Security

These changes will have no cost on business. Civil nuclear organisations are already required to have a personnel security regime in place, which the ONR oversee and approve. These regulations will lead to no change in obligations for the civil nuclear sector organisations.

Information Security Guidance

There will be no cost to business as a result of this change. As the relevant guidance set out in the regulations is being withdrawn by the ONR, these regulations remove the statutory requirement for the civil nuclear sector to comply with it. The civil nuclear sector will continue to need to comply with HMG classification policy requirements as required by the NISRs.

Benefits

There are potential benefits that will accrue to organisations from the regulations, but these are difficult to quantify in financial terms: Having robust and effective security arrangements in the sector, that are subject to continual review and are in line with our international obligations, is a key element of ensuring public acceptability for civil nuclear activity in the UK. These regulations are in line with this approach, and there will be reputational benefits to civil nuclear organisations that are able to demonstrate they operate securely in a well regulated sector.

Costs

The issuing of the new regulations is expected to lead to some administrative costs to the civil nuclear sector, specifically with regard to:

- Staff time associated with security managers reading and understanding the new legislative requirements, and ensuring that they are trained and compliant with the new obligations;
- Administrative costs associated with modifying Nuclear Site Security Plans to include CS&IA contingency arrangements; and
- Administrative changes to procedural documents by organisations affected.

21% of consultation respondents anticipated there to be some form of small administration cost, though did not specify exactly the magnitude of these costs nor the estimated additional resource involved. We understand the costs will be subsumed within existing business as usual processes within security teams in relevant organisations, Nuclear Site Security Plans and procedural documents are regularly updated in the course of business at nuclear sites, and would form part of the role and responsibilities of those in civil nuclear organisations having responsibility for security.

While in this assessment it is considered existing business will be able to subsume the changes into their existing business practices and would not need to employ any additional resource to make changes, we can look at a scenario where a proportion are unable to absorb these costs, to help guide what a downside level of overall cost might be:

Assuming 21% of businesses are unable to absorb costs within existing processes, an approximation from needing to employ up to an additional FTE energy industry staff for half a year to cover these additional administration costs, suggests that the costs for the whole industry would be less than £0.1m on a one-off, transition basis. This is on the basis of our wider engagement with the industry that this would constitute a reasonable additional resource requirement for the work described, though we would anticipate existing security managers working with their organisations to implement the changes to ensure business processes are up to date anyway i.e. form part of their current job descriptions.

It is worth noting that any accurate cost estimate on this basis may likely overestimate the time involved, as businesses will be updating their processes in parallel due to wider reforms of SyAPs that are being undertaken by the ONR.

BIT status/score

This is a Qualifying Regulatory Provision because it is a domestic update to an international obligation (CPPNM). The BIT and ['EANDCB' expand] scores are £0m as this will impose little cost to business. The £0.1m transition cost rounds to £0m for BIT and EANDCB, as confirmed by the impact assessment calculator.

Rationale for Triage rating

As annual gross costs to business are likely to be below £1m, this qualifies as low cost regulation.

Departmental signoff (SCS): Zilla Howell

Date: 15.11.2016

Economist signoff (*senior analyst*): Joel Davis

Date: 14.11.2016

Better Regulation Unit signoff: Tom Bradbury

Date: 10.11.2016

