Department for
Business, Energy
& Industrial Strategy

CIVIL NUCLEAR CYBER SECURITY STRATEGY

February 2017

This document is available in large print, audio and braille on request. Please email correspondence@decc.gsi.gov.uk with the version you require.

CIVIL NUCLEAR CYBER SECURITY STRATEGY

Any enquiries regarding this publication should be sent to us at [insert contact for department].

This publication is available for download at www.gov.uk/government/publications.

Contents

Executive Summary

Civil nuclear is essential to us all, individually, and nationally

The civil nuclear sector is part of the UK's Critical National Infrastructure (CNI)[1]. It generates essential baseload, low carbon electricity critical to families and businesses. It offers significant benefits in terms of security of electricity supply. The civil nuclear sector also stores, processes and transports some of the most dangerous radioactive material.

Tackling cyber threats to civil nuclear means looking at risks posed by legacy systems as well as future equipment

Nuclear safety and nuclear security are essential to any nuclear operation. Computers and electronic controls play a part in all civil nuclear facilities – in design, commissioning, and operation. As the UK is on the verge of constructing a new fleet of nuclear reactors to take us through to the middle of this century, the sector is facing the challenge of protecting legacy facilities, new build projects and supply chains for civil nuclear from cyber attacks. These attacks could disrupt supply, damage facilities, delay hazard and risk reduction, and risk adverse impacts to workers, the public or the environment.

This strategy sets out what cyber risks will be addressed, by whom, when, and how success will be measured

The National Cyber Security Strategy set out the Government's overarching plan "to make Britain confident, capable and resilient in a fast-moving digital world."[2] This strategy specifically supports the Government in ensuring that the UK has a secure and resilient energy system, by ensuring that the civil nuclear sector is able to defend against, recover from, and is resilient to evolving cyber threats. This enables the sector to continue to produce secure, affordable and clean energy. The strategy will also support the safe, responsible and cost effective management of the UK's energy legacy.

This strategy sets out a path to keeping the UK civil nuclear sector ahead of rapidly evolving threats to, and vulnerabilities in, software and equipment in the next five years. It sets out clear expectations, and what roles the industry, Government, and regulators need to play. It has been produced with sector consultation, to set stretching but achievable ambitions to address the risks to safe and secure operation of civil nuclear facilities and

[1] http://www.cpni.gov.uk/about/cni/

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

the transportation and storage of nuclear material and Sensitive Nuclear Information (SNI)[3] as well as the management of legacy and waste facilities. The strategy also includes some measures of effectiveness, while recognising that the nature of cyber means these may need to be adjusted and priorities may need to change over the period the strategy covers.

Success at a strategic level will be the demonstrable transformation of the civil nuclear industry's approach to cyber security (the ability to deter and protect against a cyber attack) and its cyber resilience (the ability to detect, contain, mitigate the effects of, defeat and recover from a cyber attack). Operational success will be the continued safe and secure operation of legacy and future nuclear facilities in the face of growing cyber threats. Tactical success will be an increasing capability, capacity and agility of stakeholders to deal with all aspects of the cyber security challenges faced by the UK civil nuclear sector.

Our commitment to the Civil Nuclear Cyber Security Strategy:

- To work in partnership to transform the UK civil nuclear sector's approach to cyber security (the ability to deter and protect against a cyber attack) and its cyber resilience (the ability to detect, contain, mitigate the effects of, defeat and recover from a cyber attack).
- The UK civil nuclear duty holders[4] will:
    - Establish and sustain robust, effective, agile and assurable cyber security governance arrangements;
    - Undertake appropriate risk management processes that pre-emptively reduce the associated risks;
    - Increase the sector's capability and capacity to understand and manage cyber security risks where required;
    - Ensure that known cyber security vulnerabilities are mitigated, so far as is reasonably practicable;
    - Ensure that they are resilient to, and defend themselves against, evolving cyber threats; and,
    - Work with their supply chain to support and encourage them to manage and mitigate their cyber vulnerabilities.

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365957/Nuclear_Industries_Security_Regulations.pdf

[4] The term 'Duty Holder' is used to define responsible persons' on civil licensed nuclear sites and other (unlicensed) nuclear premises subject to security regulation, as defined in the Nuclear Industries Security Regulations (NISR) 2003. It is also used to refer to a 'Licensee' as defined in paragraph 1 of a Nuclear Site Licence granted under the provisions of the Nuclear Installations Act 1965, or a 'developer' carrying out work on a nuclear construction site, as described in the Nuclear Industries Security (Amendment) Regulations 2013.

- The UK civil nuclear supply chain will:
  - Increase its capability and capacity to understand and manage cyber security risks where required;
  - Ensure that they have processes in place to notify duty holders of cyber incidents or vulnerabilities;
  - Ensure that known cyber security vulnerabilities are mitigated, so far as is reasonably practicable; and,
  - Undertake appropriate risk management processes that pre-emptively reduce the associated risks.

- HM Government will:
  - Enable cyber transformation by the UK civil nuclear sector;
  - Contribute to, and influence international and national policy, guidance and regulation for the good and benefit of all;
  - Provide an appropriate national and civil nuclear sector policy and regulatory framework;
  - Provide timely threat and vulnerability intelligence to stakeholders;
  - Use National Cyber Security Programme funding to support the overall purpose, aims and responsibilities of this strategy; and,
  - Lead the management of major cyber security incidents that are both serious and affect more than one member of the UK civil nuclear sector.

- The Office for Nuclear Regulation and Information Commissioner will:
  - Enable cyber transformation by the UK civil nuclear sector;
  - Develop and implement outcome focussed regulation of cyber security and cyber resilience;
  - Adopt a proportionate, accountable, consistent, targeted, and transparent approach to regulation, in accordance with The Regulators Code[5];
  - Hold the civil nuclear sector to account, on behalf of the public, for delivery of a safe, secure civil nuclear sector; and,
  - Contribute to and influence international and national policy guidance and regulation.

[5] https://www.gov.uk/government/publications/regulators-code

Introduction and strategic context

1. The civil nuclear sector (CNS)[6] is currently responsible for generating around 18 per cent of the UK's electricity needs. The next generation of nuclear power stations will play an increasingly important role in the security of supply and will be a key part of the Government's drive to move to a clean low carbon generation, meeting the legally binding targets set out in the Climate Change Act 2008[7], and Paris agreement[8], whilst protecting consumers' bills. For nuclear to fulfil this role, public confidence in new nuclear must be maintained.

2. Cyber security represents an enduring challenge for the civil nuclear sector and the rest of the UK's CNI. The volume and complexity of cyber attacks against the UK are growing and the range of actors is widening. The threat is becoming increasingly global and asymmetric. Both states and non-state actors can use easily-available cyber tools for destructive purposes.

3. This is demonstrated in the 2015 National Security Strategy and Strategic Defence and Security Review[9] which highlighted cyber threats as one of the four most serious national security challenges facing the UK, alongside international terrorism, state based threats, and changes in the established international order. Additionally, the 2015 National Risk Register[10] also identified that the risk of malicious cyber attacks against critical infrastructure is growing.

4. The independent regulator, the Office for Nuclear Regulation (ONR), ensures the sector meets the threats through a framework of regulations set out by Government. This framework is currently being reviewed and strengthened, particularly in relation to cyber security.

5. This five-year strategy has been developed in collaboration with industry, the ONR and other stakeholders and is in line with the proposed new regulations as well as wider European guidelines. It sets out a voluntary roadmap to enable organisations within the civil nuclear sector to meet the increasing threat from cyber and will support the

[6] The civil nuclear sector covers existing electricity generation and legacy facilities, as well as supporting supply chains, and a nascent new build programme, all of which have some shared, as well as some unique characteristics, and challenges.

[7] http://www.legislation.gov.uk/ukpga/2008/27/contents

[8] https://unfccc.int/resource/docs/2015/cop21/eng/l09r01.pdf

[9] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

[10] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf

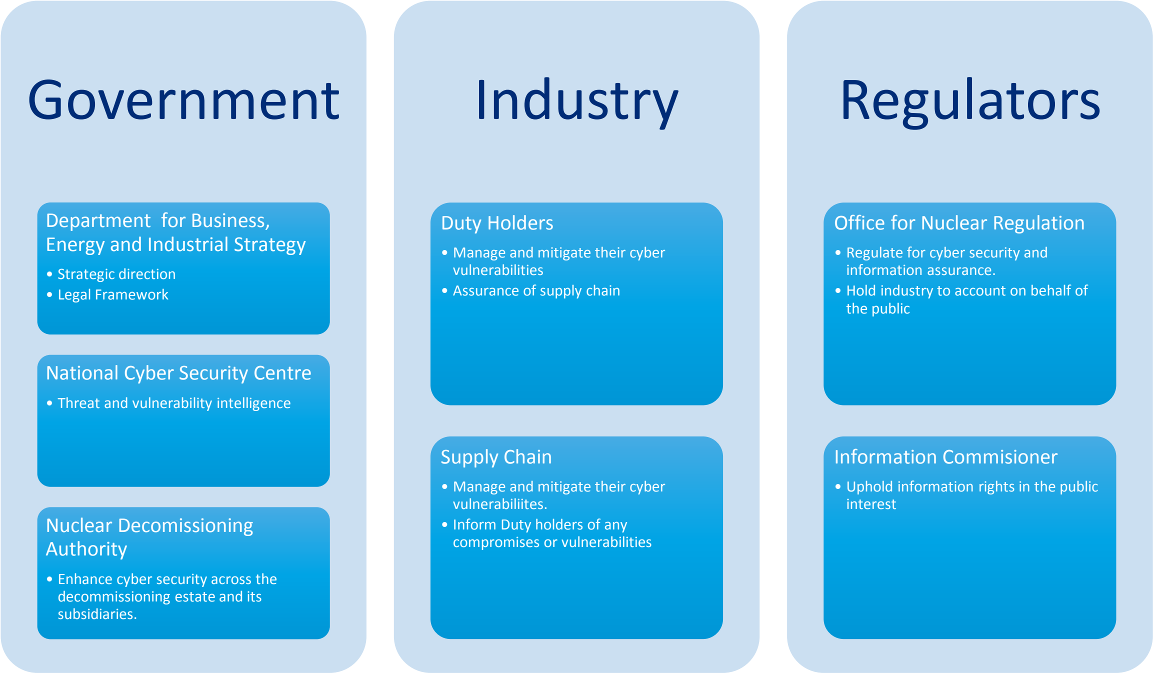
development of cyber security capability of the sector, ensuring that organisations will be able to comply with current and new regulation as well as being able to recover from compromises.

6. For this to be achieved the civil nuclear sector needs to work as a partnership between the Government, regulator and industry, with clear roles and responsibilities which are understood and agreed. Current mechanisms for sharing information in relation to vulnerabilities and how compromises have been addressed will need to be strengthened and enhanced to ensure good practice is shared and continuous improvement can be made. In this respect positive lessons can be learned from the delivery of mature physical security measures.

7. The Government, regulator and industry will regularly review whether the strategy is effectively supporting industry in meeting its objectives. This will also be an opportunity to help identify any areas that require additional industry resources or Government support. The strategy will be refreshed at the end of the five year period it covers to ensure that any emerging cyber threats are being appropriately managed and mitigated.

Roles and Responsibilities

8. Meeting the current and future risks of compromise efficiently and effectively requires a joined up approach between the Government, regulators, operators and the supply chain. It is a balance of the right legislative framework, timely and accurate intelligence, capability and capacity to implement change and deal with the unexpected. The key roles of each of the partners in delivering this can be illustrated in the following diagram:



Government

Department for Business, Energy and Industrial Strategy
- Strategic direction
- Legal Framework

National Cyber Security Centre
- Threat and vulnerability intelligence

Nuclear Decomissioning Authority
- Enhance cyber security across the decommissioning estate and its subsidiaries.

Industry

Duty Holders
- Manage and mitigate their cyber vulnerabilities
- Assurance of supply chain

Supply Chain
- Manage and mitigate their cyber vulnerabiliites.
- Inform Duty holders of any compromises or vulnerabilities

Regulators

Office for Nuclear Regulation
- Regulate for cyber security and information assurance.
- Hold industry to account on behalf of the public

Information Commisioner
- Uphold information rights in the public interest

Government

9. Government, through BEIS as the lead Government department for the sector, sets the strategic direction and legal framework while also bringing together threat information for the sector to be able to inform the measures they need to meet both regulatory requirements as well as their own personal risk concerns. Through the National Cyber Security Centre (NCSC) the Government also supports UK business, including the nuclear sector, in incident management and response. Finally, through the National Cyber Security Programme BEIS is supporting industry, with c£1.2m in 2015/16 to directly assist in increasing capability and capacity in the sector. The Government also

has a role in setting the outcomes expected from its arm's length bodies operating in the civil nuclear sector, particularly the Nuclear Decommissioning Authority (NDA) and the Civil Nuclear Constabulary (CNC)[11].

Nuclear Decommissioning Authority

10. The NDA will enhance cyber security across the decommissioning estate and its subsidiaries. The NDA will also continue to develop its decommissioning estate wide cyber incident response policy.

Civil Nuclear Constabulary

11. The CNC will manage their own cyber security and have appropriate plans in place to help deter, detect and prevent a blended attack.

Office for Nuclear Regulation

12. The ONR is responsible for independent regulation of cyber security and information assurance ensuring that industry is held to account on behalf of the public for managing and mitigating cyber risks. The ONR will also manage their own cyber security and have appropriate plans in place to help deter, detect and prevent a blended attack.

Industry

13. The civil nuclear duty holders and supply chain will, as the subject matter expert for their systems, manage and mitigate their cyber vulnerabilities. This will be achieved by the organisation's boards owning and managing their cyber risks. This will enable the industry to own and develop security solutions which most appropriately meet their unique situations as well as any risks not associated directly to nuclear regulations for safety and security (for example their own intellectual property, or issues of commercial sensitivity).

14. In addition they will work with the Government and ONR to measure whether the strategy is effectively improving cyber security in the sector. This will support industry and Government in targeting areas or workstreams to deliver the most significant improvements in cyber security.

Duty Holders

[11] The Civil Nuclear Constabulary is managed by the Civil Nuclear Police Authority, an NDPB.

15. Duty holders will work with Government and their supply chain to identify how they can improve cyber security in their supply chain. This will include identifying best practices from other sectors and developing a solution which enables the supply chain to achieve an appropriate level of cyber security to the risk posed them.

Supply Chain

16. The supply chain will work with Government and industry to improve their own cyber security, and where appropriate take part in sector wide exercise programmes, threat briefings and forums.

Cyber Security Sector

17. As with any complex discipline, there is a clear market for a variety of technical cyber advice which the nuclear industry will need to take advantage of. This could include provision of initial training and capability building through to complete solutions.

The Threat

18. The starting point in developing a cyber strategy for the civil nuclear sector is an assessment of the threat. The Government is clear that there is a credible cyber threat to the UK CNI, including the UK's civil nuclear sector, and that without mitigation or prevention these threats could lead to potentially serious consequences.

19. A number of threat actors including terrorists, hacktivists, criminals and foreign intelligence services can use cyberspace as a means to exploit vulnerabilities and cause damage or disruption. Such disruption could manifest itself in interruption of power generation or the compromise of SNI and other critical information. Technological developments have increased attackers' reach and made their identification more difficult.

20. Cyber threats should not, however, be viewed in isolation. Capable adversaries could also seek to employ cyber methods as part of a 'blended attack' to enable or reinforce a physical attack, or to seek to control industrial plant and control systems on nuclear facilities.

21. In addition the civil nuclear sector faces cyber risks that are outside of regulation (for example the potential compromise of intellectual property, reputational risk, website defacement). Whilst the potential compromises of this information may not be as detrimental to the UK as a compromise to areas that are regulated may be, it is still important that industry practices good cyber hygiene. This is because there is still potential for a cyber incident to cause significant financial and reputational consequences.

22. The Government Cyber Security Breach Survey demonstrated the increasing risk that cyber poses. The survey found that 65% per cent of large organisations reported detecting a cyber security breach in the last 12 months, with 25% reporting that they were detecting a breach at least once a month. Cyber breaches are increasingly costly, with the most costly breach identified in the survey being £3m.[12]

23. The cyber threat is evolving rapidly as technological advancements increase opportunities for hostile actors. Within the next decade, cyber tools and techniques that are presently the preserve of nation states will be much more widely available and the offensive cyber capabilities of state actors will improve. The potential for terrorist cyber

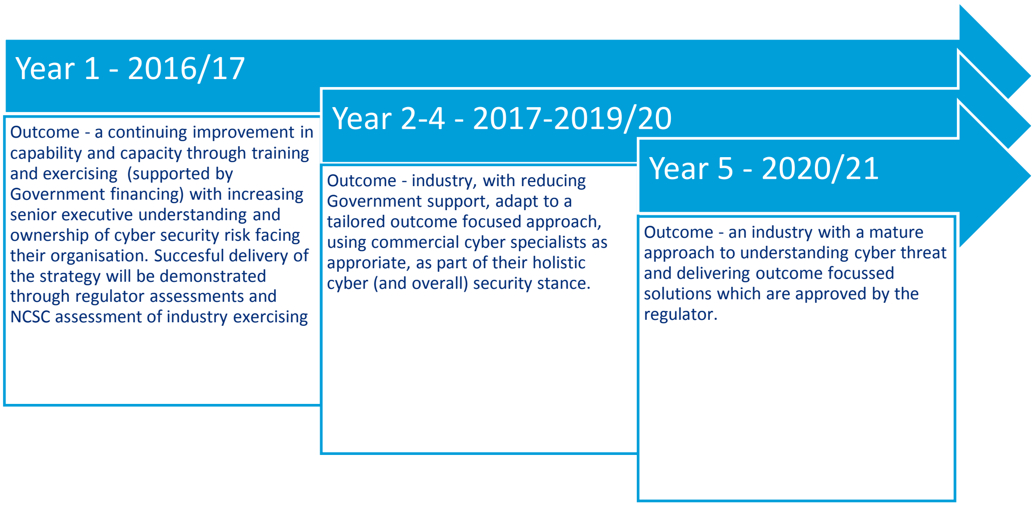
[12] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

attacks capable of exploiting vulnerabilities in the UK’s CNI and causing some limited disruption are therefore likely to increase if defences are deficient.

24. As the threat increases so too must the industry’s ability to defend itself. Over time, exploitation of cyber vulnerabilities in the UK’s civil nuclear sector, either to access and remove sensitive information or support more complex attacks will become more likely as will the potential for greater resultant impact. Compromises could result in reputational damage for the Government and the civil nuclear industry in the UK, including a loss of public confidence in civil nuclear (which could seriously damage the UK’s economic wellbeing).

Strategic outcomes and delivery

25. The ambitions of this strategy can be split into three tranches, covering the next year, the middle years, and then the final year of the strategy, to reflect the technical challenge as well as where legislative and fiscal opportunities are available. Building on the investment from Government, BEIS has secured additional funding in 2016/17 from the National Cyber Security Programme (NCSP) to deliver further support and increase capacity and capability within the sector. In the next five years the ambition is to ultimately deliver an industry which has a mature approach to understanding the cyber threat, and is able to produce solutions which efficiently and effectively address that threat. This will require in the first instance continuous professional development within the sector, the delivery of a new fit for purpose legislative framework supported by a skilled regulatory function, and a cyber specialist consultancy capability to assist the sector.



Year 1 - 2016/17

Outcome - a continuing improvement in capability and capacity through training and exercising (supported by Government financing) with increasing senior executive understanding and ownership of cyber security risk facing their organisation. Succesful delivery of the strategy will be demonstrated through regulator assessments and NCSC assessment of industry exercising

Year 2-4 - 2017-2019/20

Outcome - industry, with reducing Government support, adapt to a tailored outcome focused approach, using commercial cyber specialists as approriate, as part of their holistic cyber (and overall) security stance.

Year 5 - 2020/21

Outcome - an industry with a mature approach to understanding cyber threat and delivering outcome focussed solutions which are approved by the regulator.

26. This strategy identifies four specific activities which will support the delivery of these outcomes (overleaf).

1. Delivering a comprehensive understanding of the cyber vulnerabilities across the civil nuclear sector

Current situation

27. The civil nuclear sector have been supported by NCSP funded work to identify their key cyber assets, and identifying ways that they can improve their cyber security and ability to recover from a cyber attack.

Aim

- **Industry**: Will ensure that their organisation has a clear cyber security governance chain, which includes a board member who is able to champion cyber security at board level discussions. They will be supported by a suitably qualified and experienced Chief Information Security Officer (CISO) who can effectively explain to the board the vulnerabilities that cyber poses to their organisation and the mitigation plan that they have in place.

- Industry will also conduct a review of all the risks that cyber poses to their organisation (safety, security, operational, financial and reputational). This will then be used to prioritise intervention by the perceived threat and potential consequence of compromise.

- **Government:** Will work with agencies to ensure that briefing provided by agencies enables industry to understand the risk, and thereby assign the appropriate level of resources to manage and mitigate any risks. The Government will also facilitate industry forums where the sector can discuss the issues their organisations face and share best practice.

- **Regulator**: Will work with the NCSC and BEIS to ensure that its cyber security capability continues to develop so it can continue to provide assurance to Government and the general public that sites are identifying vulnerabilities through their multi-function inspection programme.

2. Continuously mitigate identified issues and vulnerabilities

Current situation

28. The work from the NCSP has identified areas where the CNS or individual duty holders could improve their cyber security. The CNS industry have been managing or addressing these as part of their security enhancement programmes and risk management.

Aim

- **Industry:** Will improve their management of cyber vulnerabilities by ensuring that they have identified and maintain a list of all their critical digital assets and vulnerabilities across their organisation and their supply chain. The management and mitigation of these assets will be proportional to threat of compromise and the potential consequences.

- As industry's cyber security maturity improves it will develop cyber security metrics to determine how it is performing. These metrics will have a clear reporting line to raise issues and concerns and will be discussed regularly in board meetings.

- **Government:** Will support industry by commissioning reviews of sector wide issues, such as supply chain, and in the creation of best practice guidance. We will also facilitate support from agencies to key sites and to provide advice/assurance of mitigations when appropriate.

- **Regulator:** Will provide assurance to Government and the general public that the safety and security risks that have been identified at sites are being effectively managed and mitigated.

3. Improve the sector’s capability to detect, respond, and recover from cyber incidents

Current situation

29. The civil nuclear sector has well-established security and safety exercise programmes. However, these programmes inclusion of cyber as a vector for an incident is less mature.

Aim

- **Industry:** Will work with Government and the regulator to develop its existing exercise programme so that cyber is included as a potential vector. This will allow duty holders to test that its plans, policy and procedures enable the organisation to identify, manage, defeat and recover from a cyber incident.

- Industry will have identified all of its critical assets and have plans in place for how they can be recovered from a failure, and how they would provide assurance that they achieved this. In addition industry will where appropriate have solutions in place to identify whether a hostile actor has gained access to their Information Technology (IT) or Operational Technology (OT) estate.

- **Government:** Will provide best practice guidance on how industry can detect, defeat and recover from a cyber incident. Government will also continue to develop the civil nuclear cyber security exercise programme, taking into account lessons learnt from any relevant cyber incidents.

- **Regulator:** Will provide assurance that duty holders have appropriate measures in place to detect, respond and recover from a cyber incident.

4. Ensure sufficient resources are allocated to cyber security and resilience to transform capability in the sector

Current situation

30. Duty holders are regulated by the independent ONR and are subject to inspections to ensure that they meeting their security and safety obligation. All sites have programmes in place to improve both their cyber and physical security. However, the resources allocated to cyber are usually a small percentage of the total budget.

Aim

- **Industry:** Will ensure that cyber security is considered as part of decisions to improve physical security and safety. This will potentially identify cost savings where the desired outcome can be achieved by a more optimal mix of the three areas.

- Industry will also work with Government to develop a clearly defined career development path and further development opportunities for a cyber security professional in the civil nuclear sector. This will grow both the pool of suitably qualified and experienced cyber security personnel in the sector, as well as raising personnel’s cyber security capability.

- **Government:** Will support industry in identifying blockers to resources being allocated to cyber and support industry-wide working to reduce costs and provide better value for money where appropriate. Government will also work with industry to raise industry personnel’s cyber security capability. This will include building cyber into existing and new apprenticeship and graduate programme into the sector and identify gaps within existing cyber security training, and working with international partners to ensure that these gaps are covered.

- **Regulator**: Will continue to develop their cyber security training programme and implement outcome focussed regulation of cyber security and cyber resilience. This will allow industry to own their cyber security risk and make informed decisions on the level of the resources required to address the vulnerability.

Annex A: Key activities for the delivery of the strategy

1. Develop a comprehensive understanding of the cyber risks across the civil nuclear sector

What is happening now?

The Centre for the Protection of National Infrastructure (CPNI) and CESG gather intelligence and provide advice upon on the current and future threat that cyber poses to the civil nuclear sector. This information is being shared with industry via senior boards, and on the CISP Platform. In addition CPNI host information exchanges where organisations discuss where issues have arisen on-site and solutions they are using to mitigate these risks. These outputs will be delivered by the National Cyber Security Centre following its launch in autumn 2016.

Aim

For the civil nuclear sector to share and receive threat information within the sector and with Government in an effective and timely manner. The improvement in the distribution of threat information will raise senior managers’ and boards’ awareness and understanding of the threat cyber attacks pose to their organisation. This can include changing the way this information is presented to include further guidance on the potential financial and reputational cost of a successful cyber attack if the issue is not mitigated.

The improvement of information sharing within the sector will allow organisations to change their threat posture, and benefit from the other sites experiences of how to manage and mitigate cyber issues. As organisations are reliant on the credibility of the civil nuclear sector as a whole, all parties are incentivised to agree to a solution

For the civil nuclear sector to have identified all of its critical cyber assets and systems, for these assets and systems to have an owner, incident response and recovery plan. As part of the move to outcome focused regulation, duty holders are required to understand and own the risk that cyber poses to them. To achieve this industry are required to identify all of critical cyber assets and identify the risk of compromise and the potential impact of compromise. Duty holder will use this information to prioritise resources to assets that represent that cyber poses the biggest impact[13]. Areas of vulnerability can be effectively managed and mitigated by improving cyber hygiene (for

[13] Impact is equal to risk of compromise multiplied by potential consequence of compromise.

example; hardening systems and improving intrusion detection systems) or by strengthen physical security around an asset (for example restricting access to servers).

Our approach

- Identifying the sector's most critical systems and the potential impacts should these systems be subject to a cyber attack
- Identifying and assessing vulnerabilities
- Monitoring cyber threats by assessing and analysing pertinent intelligence
- Sharing intelligence and assessments
- Promoting uptake of threat intelligence
- Working with international partners to leverage and share expertise and knowledge

2. Continuously mitigate identified issues and vulnerabilities

What is happening now?

The civil nuclear sector have identified assets that are critical for nuclear safety and have processes in place for managing any risks identified in there systems. Successfully mitigating cyber risks is a process of continuous improvement, and the flexible approach afforded by outcome-focused regulation used in the UK offers real benefits to making this possible. It enables the industry to own and develop security solutions which most appropriately meet their unique situations as well as any risks not associated directly to nuclear regulations for safety and security (for example their own intellectual property, or issues of commercial sensitivity).

Aim

For amendments to nuclear plants and the new generation of nuclear plants to be cyber secure by design and implementation. The nuclear new build programme offers an opportunity to mitigate the cyber security risk in the design phase by a combination of both physical and cyber controls so that nuclear new build will be cyber secure by design.

For duty holders to work with the civil nuclear supply chain to ensure that the supply chain to have the appropriate level of cyber security in their risk profile. It is important that as the civil nuclear sector improves their civil nuclear capability they also work to improve the capability of their supply chain. Duty holders are best placed to work with their supply chain to support this change. This will allow duty holders to better understand the cyber risk that they are carrying in their supply chain whilst simultaneously ensuring that the appropriate standard is being met.

Our approach

- Implementing and refreshing appropriate good practice, controls, and mitigations
- Ensuring that systems and digital assets (including data) are proportionately and appropriately protected
- Supporting industry with access to technical assistance and tools
- Developing nuclear new build and other new facilities so that they are cyber secure by design
- Enhancing cyber security throughout the civil nuclear supply chain
- Identifying processes to provide appropriate assurance for (critical) digital assets

3. Improve the sector’s capability to detect, respond, and recover from cyber incidents

What is happening now?

The civil nuclear sector has a strong safety culture and a mature exercising programme. To date these programmes have focused on a safety incident or mechanical failure. However industry is in the process of building up its experience in responding to a cyber incident. This has included a number of table top exercises where the communication channels between duty holders and Government have been tested. The lessons learned from these exercise have been tested as part of a technical exercise. This raised personnel’s understanding of the challenges a cyber incident poses for governance (for example smaller command chains, and the importance of record keeping), communication between the different parts of incident response (for example personnel manning perimeter defence and intrusion detection systems) as well as the need to fully understand what is on your network.

Aim

For organisations in the civil nuclear sector to include cyber within their exercise programme. The sector will benefit from including cyber within their incident response progamme. This would include ensuring that as part of all incidents cyber is considered as a potential vector and the necessary precautions are taken before it is ruled out. In addition, Government, industry, the regulator and other stakeholders should develop appropriate lines for a cyber incident (including speculation that cyber is the cause for a non-cyber incident).

For the civil nuclear sector to be resilient to a cyber attack. By taking part in technical exercising the sector will gain an understanding of what an adversary will do when attempting to compromise a system, and test whether they would detect an intrusion. This should result in sites being able to improve their protective monitoring and detection systems as well as provide a potential opportunity for Information Technology and Operational Technology personnel to get a broader understanding of the difference between their roles. In addition, the sector will develop plans to identify how it will respond and recover from an incident effecting one of its critical digital assets.

Our approach

- Ensuring that the sector has the capability to detect, defend against, and effectively respond to cyber security incidents
- Ensuring that robust incident management procedures are in place, mature, and well implemented across the sector
- Testing complex cyber incident response capability through exercising

- Promoting industry’s sharing of vulnerability/incident information and good practice
- Sharing lessons learned across CNI sectors

4. Ensure sufficient resources are allocated to cyber security and resilience to transform capability in the sector

What is happening now?

The sector currently has a mature and established safety culture, which has supported their cyber position. Sites are subject to inspections to ensure that they meeting their security and safety obligation. All sites have programmes in place to improve both their cyber and physical security. However, the resources allocated to cyber are usually a small percentage of the total budget

Aim

Ensuring that boards and executive directors understand their cyber risk leadership responsibilities. The improvement in the distribution of threat information from objective one will support this objective. This will allow non-executive directors to hold boards to account, and boards to make better decisions on how much resource to provide to mitigate the cyber risks, and ensure that organisations future plans are not increasing the organisation cyber risk without taking appropriate action.

Growing the base of civil nuclear cyber security personnel. The civil nuclear sector needs to attract cyber security professionals now and in the future. To achieve this there needs to be a clear career path for cyber security professionals that are interested in joining the sector. This will be achieved by the sector taking an active role in the Cabinet Office's cyber apprentice scheme. This will need to include a clear path for how a job holder can develop their capability and gain increasing responsibility if desired. This will be supported by providing cyber training to all professionals within the organisation, including graduates and operational technology personnel as well as encouraging regular UK personnel attendance at appropriate IAEA courses.

Our approach

- Ensuring that the regulatory framework is enabling and fit for purpose
- Promoting an integrated approach to security and safety
- Ensuring that boards and executive directors understand their cyber risk leadership responsibilities and accountabilities with regard to controls and mitigations
- Ensuring that boards fully understand cyber risks, risk controls and risk appetite
- Growing the base of suitably qualified cyber security professionals in the sector
- Improving the cyber security proficiency and awareness of both specialists and generalist staff
- Growing cyber security as a fundamental component within existing organisational cultures

Annex B: Acronyms

BEIS	Department for Business, Energy and Industrial Strategy
CERT-UK	Computer Emergency Response Team UK
CISO	Chief Information Security Officer
CNC	Civil Nuclear Constabulary
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
CNS	Civil Nuclear Sector
IT	Information Technology
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NCSP	National Cyber Security Programme
NDA	Nuclear Decommissioning Authority
ONR	Office for Nuclear Regulation
OT	Operational Technology
SIA	Security and Intelligence Agencies

Department for Business, Energy & Industrial Strategy
3 Whitehall Place, London SW1A 2AW
www.gov.uk/beis

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu