House of Lords
House of Commons

Joint Committee on the National Security Strategy

Cyber Security of the UK's Critical National Infrastructure: Government Response to the Committee's Third Report of Session 2017–2019

Third Special Report of Session 2017–19

Ordered by the House of Lords to be printed 4 March 2019

Ordered by the House of Commons to be printed 4 March 2019

HL Paper 304
HC 2003
Published on 10 March 2019
by authority of the House of Lords
and House of Commons

The Joint Committee on the National Security Strategy

The Joint Committee on the National Security Strategy is appointed by the House of Lords and the House of Commons to consider the National Security Strategy.

Current membership

House of Lords

Lord Brennan *(Labour)*

Lord Campbell of Pittenweem (*Liberal Democrat*)

Lord Hamilton of Epsom (*Conservative*)

Lord Harris of Haringey (*Labour*)

Baroness Healy of Primrose Hill (*Labour*)

Baroness Henig (*Labour*)

Lord King of Bridgwater (*Conservative*)

Baroness Lane-Fox of Soho (*Crossbench*)

Lord Powell of Bayswater (*Crossbench*)

Lord Trimble (*Conservative*)

House of Commons

Margaret Beckett MP (*Labour, Derby South*) (Chair)

Yvette Cooper MP (*Labour, Normanton, Pontefract and Castleford*)

James Gray MP (*Conservative, North Wiltshire*)

Mr Dominic Grieve MP (*Conservative, Beaconsfield*)

Dan Jarvis MP (*Labour, Barnsley Central*)

Dr Julian Lewis MP (*Conservative, New Forest East)*

Angus Brendan MacNeil MP (*Scottish National Party, Na h-Eileanan an Iar*)

Robert Neill MP (*Conservative, Bromley and Chislehurst*)

Rachel Reeves MP (*Labour, Leeds West*)

Tom Tugendhat MP (*Conservative, Tonbridge and Malling*)

Stephen Twigg MP (*Labour (Co-op), Liverpool, West Derby*)

Theresa Villiers MP (*Conservative, Chipping Barnet*)

Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place within the United Kingdom, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

Publications

The Reports of the Committee are published by Order of both Houses. All publications of the Committee are on the Internet at www.parliament.uk/jcnss.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Simon Fiander (Commons Clerk), Eva George (Lords Clerk), Ashlee Godwin (Commons Senior Committee Specialist), Carolyn Bowes (Commons Committee Assistant), Breda Twomey (Lords Committee Assistant) and Estelle Currie (Press Officer).

Contacts

All correspondence should be addressed to the Commons Clerk of the Joint Committee on the National Security Strategy, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 8092; the Committee's email address is jcnss@parliament.uk.

You can follow the Committee on Twitter using @JointCtteeNSS

Third Special Report

The Committee published its Third Report of Session 2017–19, *Cyber Security of the UK's Critical National Infrastructure* (HL Paper 222, HC 1708), on 19 November 2018. The Government's response was received on 15 February 2019 and is appended to this report.

Appendix: Government Response

The Government is grateful to the Committee for its work on this inquiry.

To respond to the challenge posed by increasing threat and changing technologies, in 2011 we launched the first comprehensive UK Cyber Security Strategy 2011 – 2016. We have continued to build on this work with our National Cyber Security Strategy 2016 – 2021, which sets out our whole of government approach to defend our citizens, organisations and institutions, deter those who would harm us and our interests and develop the tools and capabilities the UK needs to protect itself from the cyber threat. The Strategy is supported by £1.9bn of transformational investment through the National Cyber Security Programme.

Ensuring our Critical National Infrastructure (CNI) is secure and resilient to cyber threats is a key commitment under the strategy. Our approach focuses on enabling CNI organisations to understand the level of threat they face and implement proportionate cyber security practices. CNI organisations are supported by government through advice, guidance and threat information, including from the specialist National Cyber Security Centre (NCSC) we established in 2016. We are putting in place measures to understand of the level of cyber security across our CNI and are implementing the regulatory frameworks needed to drive improvements in the national interest.

However, while government can create the incentives and frameworks to drive good behaviours and support CNI organisations, ultimately the Boards of these organisations are responsible for assessing the cyber risks to their critical systems and investing to properly manage them, as the technology and threat evolve.

Conclusions and recommendations

Protecting CNI against cyber attack: a 'wicked' problem

1. **The cyber threat to the UK's CNI is growing. It is also evolving: hostile states are becoming more aggressive in their behaviour, with some states—especially Russia—starting to explore ways of disrupting CNI, in addition to conducting espionage and theft of intellectual property. Furthermore, while states still represent the most acute and direct cyber threat, non-state actors such as organised crime groups are developing increasingly sophisticated capabilities. (Paragraph 18)**

2. **Fast-changing threats and the rapid emergence of new vulnerabilities make it impossible to secure CNI networks and systems completely. Continually updated plans for improving CNI defences and reducing the potential impact of attacks must therefore be the 'new normal' if the Government and operators are to be agile in responding to this changing environment and in taking advantage of constant**

technological innovation. Building the resilience of CNI to cyber attacks in this way will make it harder for an attacker to achieve their objective—whoever that attacker may be, whatever their motive and however they choose to attack. (Paragraph 19)

The Government agrees that protecting our CNI necessitates an approach that is sufficiently flexible to counter a growing and evolving cyber threat, and agile in responding to the changing environment and technological innovation. We have therefore developed a principles and outcome-based approach for key regulations with a cyber security impact, so that CNI organisations are assessing and managing their risks in an appropriate and proportionate manner that reflects each sector's needs and changing contexts. We also take this approach in the provision of advice and guidance. The Government will keep its approach under review so that it continues to address the threat and remains effective in future.

Defining 'critical' national infrastructure

3. **'Critical' national infrastructure is, by definition, a priority for the Government and industry. However, as the economy becomes more interconnected, it is increasingly difficult to determine which elements are truly critical. The 2016 National Cyber Security Strategy provides few clues as to how the Government is managing this issue or how it is prioritising its efforts between CNI sectors. It also fails to acknowledge the varying complexity of the CNI sectors and the bearing this should have on the Government's approach. Asserting that the UK is at the forefront of international efforts on cyber security is not sufficient. (Paragraph 26)**

4. ***The next National Cyber Security Strategy, due for publication in 2021 should be informed by a mapping of the key interdependencies between CNI sectors—and therefore of national-level cyber risk to CNI—which the Government should complete as soon as possible and keep under continual review. The priorities identified in the next Strategy should also take account of the CNI sectors' respective maturity in terms of cyber resilience and the varying levels of Government influence over operators in each sector.*** **(Paragraph 27)**

The National Cyber Security Strategy (NCSS) 2016 - 2021 sets out our strategic ambition to ensure our CNI is secure and resilient from cyber threats. The delivery of the strategy is underpinned by significant programmes of work across Government, industry and academia, supported by cyber security expertise from the NCSC and funding from the National Cyber Security Programme (NCSP). Priorities reflect the context and relative maturity of each critical sector in terms of resilience to cyber threats, and are set out as part of annual Sector Security and Resilience Plans, public summaries of which are published annually.

The Government recognises the importance of understanding what is critical and therefore, that our definition of CNI and the assessment of the relative criticality of our assets remains effective. We revised the definition of CNI in 2014 to reflect our increasing dependency on digital and interconnected infrastructure in the economy, and the associated risks. Likewise, in 2015, we designated Space and Chemicals as new Critical Sectors.

We agree that it is also crucial for government and CNI organisations to work together to identify interdependencies, particularly those which could cause a cascading impact across multiple sectors. We continue to build and review our understanding of the critical systems that are vital to the everyday operation of the CNI and the interconnectedness of the various sectors, in order to improve their resilience.

As part of this effort, the guidance which supports the identification and classification of CNI was updated in 2018 to reflect our improved understanding of cyber security risk and the role of digital and logical systems. This updated guidance will inform reviews of what is critical to our CNI within each sector and dependencies between sectors. This work will enable government and industry to prioritise their cyber security efforts even more effectively.

At a more strategic level, the UK's National Security Risk Assessment process provides an overarching assessment of the key risks that have the potential to cause significant disruption to the UK, or UK interests abroad. Specific cyber risks in CNI sectors have been considered and assessed as part of this, within the wider 'all risk' context. The process also assesses the common consequences of the different risks. And where the consequence of one risk is likely to have a cascading effect on other risks within different CNI sectors, these effects are brought out within the assessment. The Cabinet Office plays a key role in bringing together Departments so that, once identified, these types of risks, their links and their interdependencies are adequately understood and planned for.

This work is reflected in our approach to CNI cyber security now and will inform its development in future.

Setting and delivering strategic objectives, and measuring progress

5. **The 2016 National Cyber Security Strategy states that ensuring the resilience of the UK's critical national infrastructure to cyber attack is a priority for the Government. But the Strategy does not set out (a) what specifically the Government wants to achieve; (b) over what timeframe; or (c) how it intends to measure progress. We are therefore concerned that despite the designation of major cyber attacks as a top-tier threat to UK national security, the Government does not have clearly defined objectives for the five-year period covered by the Strategy nor a structured plan for delivering them. This echoes our findings specifically in relation to cyber security skills, which we set out in our July Report. (Paragraph 34)**

6. **The Government is unwilling to publish any information about the 2016–2021 National Cyber Security Programme other than its total budget of £1.9 billion. While we accept that some elements of the NCSP are security-sensitive and therefore should not be made public, such lack of transparency about such large sums of public money is of serious concern. It is also a backwards step, given that the previous Government published Annual Reports and high-level budget breakdowns by activity for the earlier 2011–2016 NCSP. (Paragraph 35)**

7. ***The Government should resume publishing Annual Reports for the National Cyber Security Programme to improve transparency and aid external scrutiny. These should set out progress made, the challenges faced, and a breakdown of the budget by type of activity and by department or agency; it would also present a regular opportunity to***

review and adjust plans in response to changing threats, vulnerabilities and technological innovation (as we concluded in paragraph 19). Given the relatively large sum of public money and the many departments and agencies involved, the Government should also support a programme-wide audit of the NCSP by the National Audit Office to provide public and Parliamentary assurance. **(Paragraph 36)**

The National Cyber Security Strategy 2016 - 2021 is underpinned by 13 Strategic Outcomes, annexed to the Strategy, that define the precise aims of the NCSS. Governance and delivery arrangements are structured around the Strategic Outcomes, with regular stocktakes undertaken to determine progress toward these objectives.

These Strategic Outcomes also define the structure of the NCSS and NCSP performance management and monitoring system. This draws together a wide range of performance indicators to provide an evidence based assessment of performance. The performance system was revised in 2018 in line with recommendations in the National Security Capability Review, and continues to develop.

A breakdown of how the £1.9 billion National Cyber Security Programme is allocated is not made public for national security reasons. Funding in support of CNI cyber security also comes from sources outside of the Programme, including departmental budgets and investment by CNI organisations.

The National Audit Office (NAO) is currently conducting an audit of the National Cyber Security Programme, to be published later this year. The Government notes the Committee's comments and will also wish to consider the outcome of the NAO audit before determining whether further information could be made available to improve transparency, whilst balancing national security considerations.

An "expanded role" for the Government on CNI?

8. **The Government's current approach to improving the cyber resilience of the UK's critical national infrastructure is long on aspiration but short on delivery. Establishing the National Cyber Security Centre as the national technical authority and introducing more robust regulation for some CNI sectors were both important steps. The latter was mandatory for the UK as an EU member state, however. It appears that the Government is reluctant to move more forcefully and, by default, continues to rely on market forces to improve operators' cyber resilience, despite recognising the previous failure of this approach. Its efforts so far certainly fail to do justice to the status of major cyber attacks as a top-tier threat to national security or to the importance of CNI to the economy. Greater urgency is required if the UK is to 'get ahead' and 'stay ahead' of the cyber threats to its CNI. (Paragraph 43)**

9. ***As we concluded in relation to cyber security skills in our July Report, the Government must first understand the problem before it can address it. The Government should therefore immediately commission work to understand how and why the market has failed to deliver improved cyber resilience of CNI in both the public and private sectors. Only then will it be in a position to identify the targeted interventions and incentives—whether regulatory or otherwise—that will drive up cyber resilience of CNI, while also establishing the culture and practices necessary for continual improvement in the long term.*** **(Paragraph 44)**

In the National Cyber Security Strategy 2016 - 2021 the Government set out an ambitious vision for the cyber security of UK CNI, including committing to putting in place the right framework of incentives and regulation, with measures to intervene where necessary to drive improvement in the national interest. This reflected our experience from the 2011 Strategy, that while progress had been made, market forces and government encouragement had not proved sufficient in themselves to drive the scale of behaviour change and investment needed for CNI. We have also drawn upon learning from the 2016 Cyber Security Regulation and Incentives Review.

As part of delivering on this commitment since 2016 we have strengthened wider regulation with a cyber security impact through new legislation including the Data Protection Act, GDPR (General Data Protection Regulation), the Network and Information Systems (NIS) Regulations, as well as improving the effectiveness of existing sectoral regulatory frameworks. We are continuing to work with every CNI sector to put in place effective frameworks.

We are not complacent. We continue to improve our understanding of the level of cyber security across our CNI, in order to be better able to target support and intervene where necessary. We are doing this through developing, piloting and carrying out cyber security assessment and testing programmes which will deliver a step-change in the data available by 2021. We conduct extensive engagement and collaboration with CNI organisations through Information Exchanges and other fora which give us valuable insights into the challenges these organisations face in improving their cyber security.

More widely, the Government recognises that changing the cyber security behaviours and practices of individuals and organisations can be difficult and requires a range of approaches from nudge techniques, communications, and education, through to law enforcement and legislative action. We are currently undertaking new research to understand better the barriers and motivations around taking action on cyber security. The results of this will help inform future policy and regulatory interventions and the necessary underpinning advice and guidance.

Regulation: fixing market failure by setting a higher benchmark

10. **The Network and Information Systems Regulations offer a more robust regulatory framework for many CNI sectors, especially in making it mandatory for operators to report incidents where their impact exceeds a predetermined threshold. Although these regulations have only recently come into force, we expect them to set a higher benchmark for cyber risk management in those CNI sectors where they apply. They should also, we hope, foster a culture of proactive and continual risk management by CNI operators, moving away from a 'tick-box compliance' approach. (Paragraph 51)**

11. **Nevertheless, the NIS Regulations are not a 'silver bullet':**

- **the NIS Regulations are limited in scope, leaving some CNI sectors still without statutory regulation and enforcement powers for cyber risk management;**
- **the fragmented responsibility for the NIS Regulations' implementation across Whitehall, Devolved Administrations and regulators remains confusing and**

acts as a barrier to cross-sector consistency and collaboration—in particular, the introduction of joint Competent Authorities in some sectors clouds accountability and effectiveness; and

- **some designated 'Competent Authorities' currently lack the expertise and capacity to provide credible assurance of operators' efforts—an issue we addressed directly in our July Report on cyber security skills.**

We are therefore concerned that the NIS Regulations will not be enough in themselves to achieve the required leap forward in cyber resilience across all CNI sectors (Paragraph 52)

The Government welcomes the Committee's recognition that the Network and Information Systems (NIS) Regulations will set a higher benchmark for cyber risk management in those sectors. The UK Implementation of the NIS Directive is one of the most comprehensive and advanced implementations in Europe.

The government held a public consultation on the proposed approach to implementing the NIS Regulations in the UK, and received broad support for a multiple competent authority approach. The focus of our implementation is rightly on what steps are appropriate and proportionate to protect an essential service. In general the organisations in scope already sit within sectors that provide a particular type of essential service and which are already regulated for purposes such as safety, security, service provision or economics. The multiple competent authority approach therefore benefits from the significant sectoral understanding, expertise and relationships that sector specific regulators can draw on to drive improvement and minimises the creation of new burdens on regulated organisations. It is the most appropriate way to integrate cyber security as part of the mainstream regulation of each sector.

NCSC provides a consistent source of expert cyber security advice and support to all Competent Authorities across a number of areas of NIS implementation. The Competent Authorities closely collaborate on NIS implementation, co-ordinated by the Department for Digital, Culture, Media and Sport.

Where Joint Competent Authorities have been established, they are able to benefit from the shared resources and wider range of capabilities offered by both organisations. But we agree that they should be taking active steps to avoid any potential confusion around accountability. Competent Authorities should agree a division of roles and responsibilities and provide clear guidance to Operators of Essential Services (OES) on how they should be engaging.

The Government acknowledges the challenge of having access to the skills we need in both government and industry to protect our CNI. Competent Authorities are currently determining their skills requirements and building capability in accordance with their planned implementation models, which may include drawing on both 'in house' and external technical expertise. The NCSC provides considerable specialist support to Competent Authorities including through the publication of technical guidance, the development of the Cyber Assessment Framework and approaches to critical systems identification.

The Transforming Government Security programme is improving how security is managed in government. This includes establishment of a Government Security Profession Unit (GSPU) to support the drive to attract, retain and develop a highly skilled security workforce for government including on cyber security. This should contribute to improvements in capability across Government, including in Competent Authorities. We have also taken steps to understand the skills Competent Authorities will need in house to implement the NIS Regulations and are supporting them through relevant training.

We have already committed to review the NIS regulations in 2020 following the initial period of implementation. Drawing on this evidence and that from other regulatory frameworks we will consider the case for adjusting the regulations at that stage. The government will also keep the impact and effectiveness of wider interventions to improve cyber resilience under review.

12. **Threat- and intelligence-led penetration testing shows promise as a mechanism for providing technical assurance of CNI operators' cyber risk management—all the more important in the absence of agreed metrics for cyber risk and resilience. However, such testing should be used in combination with other methods of regulatory assurance because it only provides a snapshot of operational resilience at a particular moment in time against a particular set of threats. (Paragraph 56)**

13. ***The Government should establish a plan (a) for the development of threat- and intelligence-led penetration testing and its roll-out across all CNI sectors that takes account of the mixed maturity of the sectors in terms of their cyber resilience; (b) for the development of the test methodology; and (c) for developing the cyber security industry's capacity to deliver such advanced and accredited testing at scale. It should address the last point in its forthcoming cyber security skills strategy which, as we urged in our July Report, should be published as a matter of priority.*** **(Paragraph 57)**

The Government is committed to understanding the level of cyber security in our CNI and improving the management of cyber risk. In order to achieve that, it is essential for CNI regulators to be able to assure cyber risk management by organisations. There are a range of approaches which are being developed and deployed.

The NCSC have developed and published a set of fourteen outcome-based cyber security principles and a detailed Cyber Assessment Framework (CAF) incorporating a comprehensive set of Indicators of Good Practice to assist Competent Authorities in assessing the extent to which organisations are taking appropriate and proportionate steps under the NIS Regulations. Although the approach and precise requirements will be necessarily tailored to each sector, the CAF will provide a consistent point of reference in understanding the level of cyber security across our CNI.

We agree that penetration testing schemes that simulate the capabilities and attack methods of cyber adversaries have promise as part of the approach to cyber security assurance. The CBEST model of such testing has been developed and piloted within the Finance sector and has become a regular component of supervisory assessment of firms. We have already actively been developing and piloting similar schemes for the Government sector and the Telecommunications sector. We are considering the contribution this type of testing could make to cyber security assurance within further CNI sectors, reflecting factors including sector maturity, cost and capacity.

NCSC also supports CNI organisations in accessing penetration testing by providing guidance for testers and maintaining an accreditation scheme of penetration testing companies (known as the CHECK scheme), which provides assurance that services hired in by client companies have a high degree of competence. This guidance is currently being updated to reflect the latest progress in the development of these attack simulation and testing methods.

Other key approaches the Government has implemented as part of cyber security assurance include in-depth technical risk reviews and "red teaming" activities.

Our proposed longer term plan to give the UK the cyber security skills it needs is outlined in the recently published Initial National Cyber Security Skills Strategy. We are currently consulting widely on this.

14. **The NIS Regulations will continue to apply in the UK following Brexit. However, the mechanism for UK participation in EU-wide information-sharing and capacity-building is still subject to negotiation.** ***Given that cyber threats do not stop at national borders, the Government should prioritise maintaining access to the EU's NIS Coordination Group and its workstreams to facilitate continued information-sharing and collaboration with EU Member States.*** **(Paragraph 60)**

We recognise that the cyber threat the UK and its European allies face remains significant and knows no international boundaries. Continued cooperation with the EU is not only in our UK interest, but is firmly in the interest of the EU as we look to respond to hostile state and non-state actors in cyberspace. We therefore intend to seek continued co-operation with EU partners in the NIS Cooperation Group, its associated work streams, and with the network of Computer Security Incident Response Teams, after we exit the EU.

Cultural change: creating an environment for continual improvement

15. ***The Government should set out in its response to this Report its assessment of how, and how effectively, the Huawei Cyber Security Evaluation Centre Oversight Board provides additional assurance in relation to the UK's cyber security.*** **(Paragraph 66)**

The Huawei Cyber Security Evaluation Centre Oversight Board is a cross-government and industry body whose role is to evaluate the effectiveness of the Huawei Cyber Security Evaluation Centre (HCSEC) as a mitigation for the UK on the use of Huawei in critical telecommunications infrastructure.

The HCSEC opened in November 2010 under a set of arrangements to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's CNI. HCSEC undertakes detailed technical assessments of a range of Huawei products used in the UK telecommunications market, with access to information and insight from Huawei that is unavailable to any other facility. These assessments give UK operators and the NCSC a rich source of evidence to inform commercial and national security risk management. We are not aware of any comparable mechanism in another country.

The role of the Oversight Board is to oversee and ensure the independence, competence and therefore overall effectiveness of the HCSEC in carrying out its role. It does this through scrutiny of HCSEC's competence by considering recruitment levels, skills and performance. It oversees the ongoing programme of technical work, including the number

of assessments undertaken by HCSEC, how they were carried out, and the main findings. To scrutinise the independence of HCSEC's operations from Huawei HQ, the Oversight Board commissions an assessment from a globally respected audit firm (currently EY) annually. The Oversight Board also independently oversees the effectiveness of HCSEC's technical insight into equipment and processes, in order to get assurance that this part of the mitigation strategy is operating correctly.

The Oversight Board incorporates a range of senior executives and stakeholders from across Government and Industry. This includes the CEO of the NCSC as Chair, a senior Huawei executive as the Deputy Chair, two senior executives representing the UK telecommunications sector (currently from BT and Vodafone) and other Government members.

The Government takes the view that the Oversight Board is therefore fulfilling its intended purpose. Importantly, the assurance it provides is given transparently in the annual report which is published. To date, the Oversight Board has published four such reports, the last being in July 2018, which found serious deficiencies in Huawei's development, engineering and support processes, with implications for cyber security. The Government is in intensive discussions with Huawei about how to rectify these deficiencies.

16. **A more holistic and effective approach to strengthening the cyber resilience of CNI requires changing the culture of CNI operators and their extended supply chains. Embedding the view that cyber risk is another business risk, which must be proactively managed, will be central to this process. It is especially important for those private-sector operators whose commercial interests may not always align with the demands of national security. (Paragraph 73)**

17. ***The Government should give urgent consideration to non-regulatory incentives and interventions that have the potential to drive cultural change across CNI sectors, establishing an environment in which continual improvement is encouraged. The issues it should consider include:***

- ***how managing cyber risk through and within the extended supply chains of CNI operators could be encouraged;***
- ***how the Government can best support operators in managing cyber risk associated with hardware, software and services bought 'off the shelf', especially those procured from major international suppliers;***
- ***improving board-level expertise and accountability. This includes identifying an expert board member with specific responsibility for cyber resilience and mandatory corporate reporting on cyber resilience, in accordance with the spirit of forthcoming reforms to the Companies Act 2006; and***
- ***how cyber insurance might be used to improve operators' cyber practices, and how the Government can support the market in maturing more quickly.*** **(Paragraph 74)**

The Government is taking forward a number of strands of work with the intent of improving cyber risk management across organisations, and considering the market drivers or incentives necessary to support that.

We have already taken significant steps to embed supply chain risk management, including through setting minimum cyber security standards for government departments, requirements under the Network and Information Systems (NIS) Regulations and the publication of guidance. Accreditation schemes and standards also play an important role. The Cyber Essentials scheme has also gone some way to put basic technical protections in place.

We continue to build our understanding of these risks and develop further policy to drive improvement drawing on established schemes, such as the Defence Cyber Protection Partnership, which protects our military capability by improving cyber defence within the supply chain. We are also considering how the desired outcomes can be reflected in commercial contracts and procurement decisions, and continue to engage with major suppliers to improve their level of cyber security resilience.

We have been working to improve the security of internet-connected products within the wider marketplace. The Government recently published the Code of Practice for Consumer 'Internet of Things' (IoT) Security to support industry in the development of internet-connected products which will better protect the online security and privacy of consumers, and reduce the increasing threat of cyber attacks launched from insecure devices.

As ultimate responsibility for protecting CNI against cyber threats sits with the boards of CNI organisations, the Government agrees that improving board level awareness, expertise and accountability is essential to drive improvement. Within government, appropriate senior level governance is already required under the government Security Policy Framework and Minimum Cyber Security Standard and is also integrated within the principles and Cyber Assessment Framework developed for the NIS Regulations.

We undertake considerable engagement with industry through briefings and discussions in various fora. At board level we are engaging with a variety of organisations, including CNI and government suppliers, to support cyber security awareness and understanding.

More broadly, we are supporting boards through developing a toolkit to generate constructive conversations and a health check to understand how risks are being managed. We note the recommendation regarding mandatory corporate reporting on cyber resilience, and will give this further consideration, building on analysis undertaken as part of the 2016 Cyber Security Regulation and Incentives Review.

The Government agrees that cyber insurance has a part to play in reducing cyber risk. We work closely with the insurance industry; for example through the Cyber Insurance Forum, which has supported the development of the UK insurance sector in offering leading cyber security expertise and services.

Political leadership: driving change across Government and CNI sectors

18. **Focused and proactive political leadership from the centre of Government is essential in driving change and ensuring a consistent approach across the many departments and agencies with responsibility for the resilience of CNI to cyber threats. We are concerned that the current complex arrangements for ministerial**

responsibility mean that day-to-day oversight of cross-government efforts is, in reality, led by officials, with Ministers only occasionally 'checking in'. This is wholly inadequate to the scale of the task facing the Government, and inappropriate in view of the Government's own assessment that major cyber attacks are a top-tier national security threat. (Paragraph 79)

19. ***There should be a Cabinet Office Minister designated as cyber security lead who, as in a war situation, has the exclusive task of assembling the resources—in both the public and private sectors—and executing the measures needed to defend against the threat. This Minister should therefore be responsible and accountable for the cross-government development and delivery of the National Cyber Security Strategy and Programme, including those elements relating to CNI. This Minister should therefore:***

- ***be empowered to hold departmental Ministers to account;***
- ***sit on the National Security Council (NSC) and relevant NSC sub-committees; and***
- ***oversee the work of the National Cyber Security Centre and the relevant section of the National Security Secretariat.* (Paragraph 80)**

20. ***The Government should also provide our Committee with evidence of the NSC sub-committees' active oversight of cross-government efforts to improve the cyber resilience of the UK's CNI. Its recent decision to share summaries of the agendas for relevant NSC sub-committees with us, in confidence and on a regular basis, is a welcome starting point.* (Paragraph 81)**

The Government considers that the existing arrangements already fulfil the requirements outlined by the Committee and are the most effective way of achieving our vision of cyber security as a core, embedded part of Government policy for every CNI sector.

Ministerial responsibilities are clearly defined and, given that improving the resilience of CNI to cyber threats requires a cross-cutting government response, necessarily distributed across departments.

The Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office is responsible to Parliament for the National Cyber Security Strategy and Programme, and also has overall responsibility for improving the security and resilience of CNI.

As a member of the National Security Council, its NSC(SDSR) sub-Committee and chair of the NSC(THRC) sub-Committee he is able to hold departmental Ministers to account. The NCSC is accountable to him for its delivery as part of the wider National Cyber Security Strategy and Programme, and the National Security Secretariat already reports to him.

Details relating to the proceedings of Cabinet Committees are generally not disclosed, as to do so could harm the frankness and candour of internal discussion.

21. **The National Cyber Security Centre has had an impressive impact in the two years since it was established as the national technical authority on cyber security. Although there are areas for improvement, it has made important contributions across a variety of Government and industry initiatives in relation to CNI, despite its**

lack of enforcement powers. However, we heard there are unresolved tensions derived from its status as part of GCHQ—an institutional relationship that also provides significant advantages. It is also essential that the NCSC's proactive leadership on the technical aspects of the cyber resilience of CNI is not treated by Ministers as a substitute for strong political leadership in driving change across CNI sectors and relevant departments. (Paragraph 89)

22. **We continue to have concerns about the capacity of the NCSC to meet growing demand for its services and expertise. As the Government's 'one-stop shop' for technical advice, the NCSC is integral to the Government's and private sector's efforts to improve the resilience of the UK's CNI to cyber attack. However, its effectiveness will be limited unless it has access to the experts it needs in the numbers it requires. Consideration must also be given to likely future demands on the NCSC's resources as technology continues to advance and the threat continues to grow. (Paragraph 90)**

23. ***The Government should publish a plan for the institutional development of the NCSC over the next decade, taking account of anticipated technological progress and setting out the resources and range of skills and expertise that the NCSC is likely to need. These requirements should be addressed in the Government's forthcoming cyber security skills strategy. Its budget—currently running to 2020–21—should be extended beyond that time horizon in next year's Spending Review as a ring-fenced fund separate from (and safe from) general departmental budget pressures.*** **(Paragraph 91)**

The Government welcomes the Committee's recognition that the NCSC has already had an impressive impact. We recognise that this success is accompanied by the challenge of addressing growing demand and keeping pace with the evolving threat.

The NCSC is a relatively new organisation, which continues to build its capability to reach its full potential and maturity. We are actively considering the future resources, including the skills and funding that will be needed to deliver our ambitions for NCSC and our vision for a UK "secure and resilient to cyber threats, prosperous and confident in the digital world". Future decisions on resourcing structures will be taken as part of the Spending Review process when this begins. We outlined our proposed longer term plan for UK cyber security skills in the recently published Initial National Cyber Security Skills Strategy.

We consider that the current arrangements, enabling NCSC to draw on the unique insight of GCHQ in understanding the threat, best support the overall resilience of UK CNI. Lead Departments and the NCSC work together so that technical advice is appropriately applied within the context of each CNI sector.

Complementary to the development of the NCSC are our plans to enable CNI organisations to better access the trusted cyber security services and products they require to protect themselves. This includes leading work to stimulate the cyber security industry to serve the CNI better with services such as exercising, training and assurance. We will also be piloting an approach to facilitate CNI organisations in identifying appropriate services and products in the marketplace, building on existing NCSC certification schemes run in partnership with industry.