HM Government

Prospectus
Introducing the National Cyber Security Centre

Foreword

The internet is an increasingly intrinsic part of our lives. The UK's digital economy is strong, with companies of all sizes and sectors using online opportunities to increase their reach and productivity. In government, we are increasingly enabling the public to access services online, cutting costs and making it easier to interact with the state. In short, the world is a more open and connected place.

So cyber security is increasingly important too. As the 2015 National Security Strategy set out, cyber is a Tier One threat to the UK's national and economic security.

We have almost doubled the investment the Government will make in cyber security, to £1.9 billion over the next five years. But government cannot act alone. Partnership with industry and academia is vital, and everyone who goes online has an important role to play. Public and private organisations need to protect their data and safeguard their computer systems.

At the heart of our strategy is a new National Cyber Security Centre which we will launch in autumn 2016. The Centre will be the bridge between industry and government, simplifying the current complex structures, providing a unified source of advice and support, including on managing incidents. It will be a single point of contact for the private and public sectors alike.

I am delighted that Ciaran Martin has agreed to lead the new Centre, reporting into GCHQ.

This prospectus gives details of the new Centre's proposed scope and focus. It is vital that the Centre works with industry from the very start. We want to hear your views on this proposed design, and we look forward to working with you to make it a reality.

Rt Hon Matt Hancock MP
Minister for the Cabinet Office
May 2016

Welcome to the National Cyber Security Centre (NCSC) Prospectus. Ahead of the Centre's formal launch later this year, and the opening of our new London headquarters, this sets out our proposed vision and goals, describes who we are, and the work we will do to transform cyber security in the UK.

Together with our customers and partners, the NCSC will be at the heart of the Government's new strategy for making the UK the safest place to live and work online. Along with the rest of my team, I look forward to working with you. The first part of this process is inviting you to engage with us on what you want to get out of the Centre. We look forward to hearing from you.

Our vision

The UK is a digital society. Information technology is increasingly integrated into every aspect of our lives. Our economy and daily lives are the richer for it. But this transformation brings new dependencies: the economy, the administration of government and the provision of essential services all rely on the integrity of cyberspace and the infrastructure, systems and data which underpin it.

The 2015 National Security Strategy reaffirmed cyber-related threats as one of the most significant risks to UK interests. The Government has set out its intent to address the cyber threat, to put tough and innovative new approaches in place, and to be a world leader in cyber security. The National Cyber Security Centre will be at the heart of this new approach. The Centre will bring together the capabilities already developed by CESG – the Information Security arm of GCHQ – the Centre for the Protection of National Infrastructure, CERT-UK and the Centre for Cyber Assessment, allowing us to build on the best of what we already have, whilst significantly simplifying the current arrangements.

Ciaran Martin, CEO,
National Cyber Security Centre

What we do

The National Cyber Security Centre will have four key objectives:

- To understand the cyber security environment, share knowledge, and use that expertise to identify and address systemic vulnerabilities.

  The NCSC will be the centre of government expertise on what is happening in cyberspace, combining the knowledge gathered from incidents and intelligence with that shared through the close relationships with industry, academia and international partners. We will use that knowledge to provide best practice advice and guidance, and to tackle systemic vulnerabilities to enhance cyber security for all.

- To reduce risks to the UK by working with public and private sector organisations to improve their cyber security.

  The NCSC will support the most critical organisations in the UK across government and the private sector to secure and defend their networks. We are planning that this will include the provision of bespoke advice and guidance, help to design and test networks, and exercise response arrangements.

- To respond to cyber security incidents to reduce the harm they cause to the UK.

  We recognise that despite all our efforts to reduce the risks and enhance security, incidents will still happen. When a serious cyber incident occurs, we will work with victims to minimise the damage, to help with recovery, and to learn lessons to reduce the chance of recurrence and minimise future impact. Often we will help by connecting victims with commercial companies who we know are excellent at cyber incident response. At the same time we will ensure that the wider response of government and law enforcement is well co-ordinated. And in the case of very serious incidents this might mean communicating publicly about consequences and the steps people and businesses should take to protect themselves.

- To nurture and grow our national cyber security capability, and provide leadership on critical national cyber security issues.

  Cyber security and information technology continues to develop and evolve at a rapid pace. As the Centre within government for cyber knowledge, the NCSC will have the best possible visibility of what is happening today – in terms of threats, vulnerabilities and technology trends. This means cutting edge technical research teams, combining the best of government, industry and academic expertise, scanning the horizon and helping us plan for what could challenge us tomorrow. The NCSC will lead the UK's thinking across the range of initiatives and developments, ensuring that the UK Government, organisations and the public can harness the advantages that new technologies bring in a safe and secure manner.

We will help to ensure the resilience of the UK's Critical National Infrastructure against cyber attack, for example in energy, telecoms and the finance sector, working closely with the organisations that own the key networks, and the relevant Lead Government Departments and Regulators.

The NCSC will address systemic vulnerabilities through root cause analysis (similar to those undertaken for other systemic risk management systems) and then work with key stakeholders and incentivise the market to address them.

As government puts more services to the citizen online, NCSC cyber security advisors will work alongside delivery teams in government departments to help ensure security is built in from the start. Our cyber security professionals will compliment expertise and business knowledge in departments, and bring a unique perspective based on our knowledge of threats and vulnerabilities.

When we offer cyber security advice to organisations, we are looking to support the customer's processes and ambitions. Our advice will make sense in the real world, providing practical solutions that enable business outcomes through good cyber security.

Our assessment team will review everything we learn from cyber incidents and from our engagement with customers and partners. They will combine this with data from all sources, including intelligence, and with the latest knowledge of emerging trends across the cyber security sector. This will provide for authoritative, independent assessments of evolving threats and vulnerabilities.

How we work

Collaborative

The establishment of the National Cyber Security Centre will bring a new level of coherence and effectiveness to how government does cyber security. But the new Centre cannot work in isolation. We want partners to include government agencies and departments, the devolved administrations, and the wider public sector. At the same time the Centre will work in close partnership with Law Enforcement to support their efforts to tackle cyber crime, and with the UK's security and intelligence agencies and the Ministry of Defence to identify and counter the full range of threats in cyber space.

But the Government cannot act alone. Most important of all are our partnerships beyond government. We want to engage with the full spectrum of organisations with a stake in cyber security – in the wider public and private sectors; in the third sector; in the Critical National Infrastructure and academia. We must work together, focused on where the greatest risk lies, with the simple goal of doing cyber security better.

International

Cyber security is a global challenge. The Government works with international partners to share threat information and improve our shared defences. The NCSC will support the government's wider security and prosperity agenda by engaging with international partners on incident handling, situational awareness, building technical capabilities and capacity (for example through exercising), and contributing to broader cyber security discussions.

Diverse

The NCSC will bring together a unique range of talents, skills and experiences to tackle some of the hardest security questions that we face. This range of work will go far beyond what any one organisation does today, harnessing the full range of capabilities, both within government and beyond.

Open and Accountable

The NCSC will have access to some of the most sophisticated capabilities of government, including in the intelligence and security agencies. But at the same time we propose to make these benefits available to as wide an audience as possible. The NCSC's systems and working practices will enable us to engage as effectively and seamlessly with the private sector as intelligence and security agencies have, traditionally, engaged with central government departments on cyber security. We will operate strictly within the law and a strong ethical framework and be accountable for our work.

Expert and Looking to the Future

The NCSC will be an expert organisation, with world class knowledge, experience and expertise on cyber security and relevant technologies, and on the application of cyber security in the business world. As part of this we propose to exchange talent with other sectors through secondments and interchanges.

The NCSC will also support the wider national campaign to grow the UK's cyber security capability and capacity, working alongside other government departments including Cabinet Office, Home Office and Department for Culture, Media and Sport (DCMS).

Who we work for

The National Cyber Security Centre serves a wide range of UK organisations across the entire spectrum of cyber security issues.

Consequently the service provided will be multi-layered, reflecting the different threats that organisations face, and the skills and resources they have to address them. Owners of networks, systems and data will remain responsible for managing the risks to their organisations; the NCSC will not represent a change to this principle of risk-ownership.

We have defined four categories of engagement to describe the scope of our offer:

The NCSC will provide general advice and guidance. The NCSC will be the lead cyber security technical authority in the UK, with overall responsibility for the technical content of all cyber security advice issued by HMG. The NCSC will work closely with Home Office, Law Enforcement, DCMS and other partners to ensure these messages are deployed as effectively as possible.

For organisations that have their own networks, **the NCSC will run the Cyber Security Information Sharing Partnership (CiSP)**. This will enable organisations to share information with each other and the NCSC about what they are seeing on their networks, and provide a forum for discussion from beginner through to expert level.

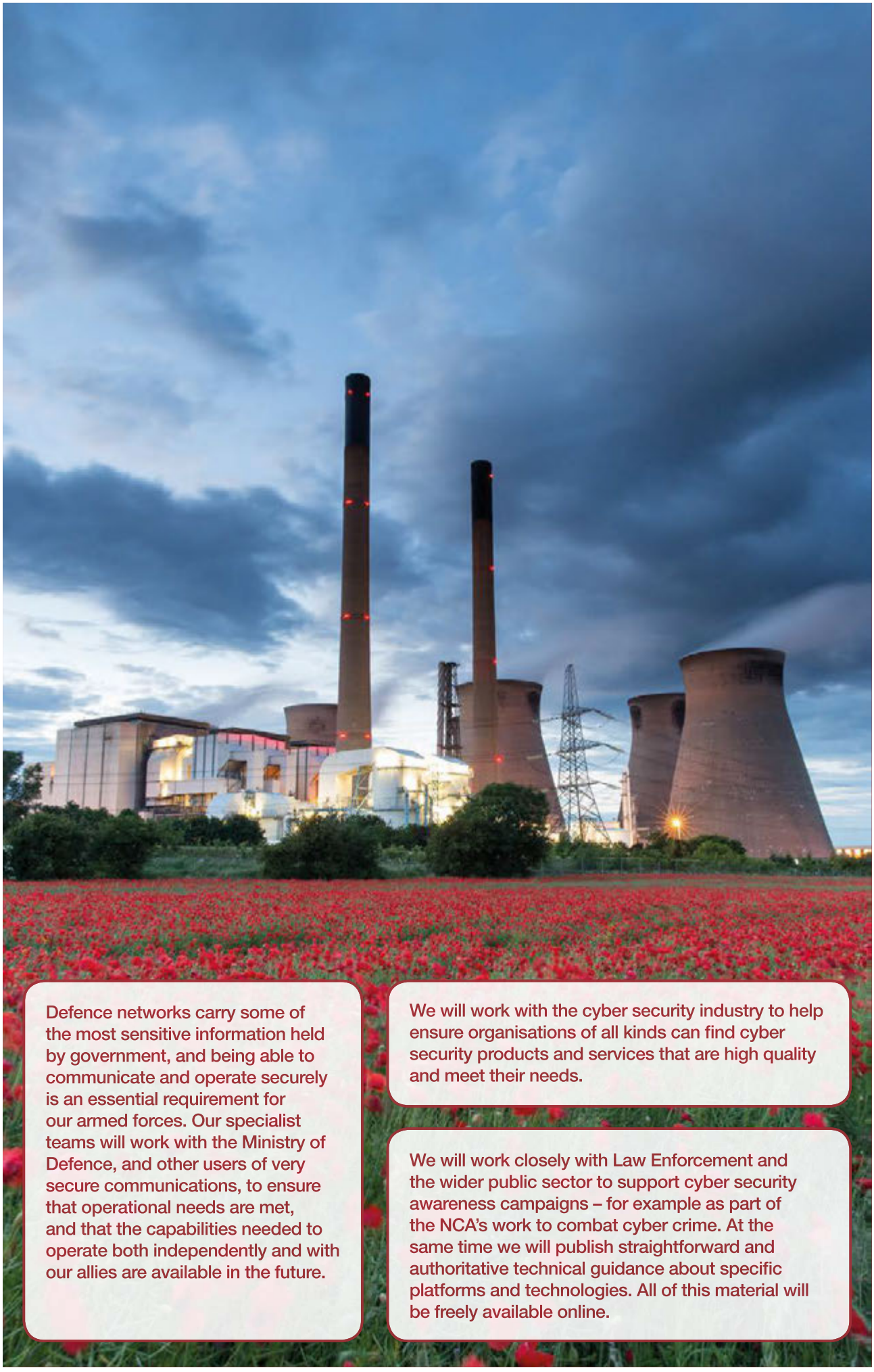
We propose that **the NCSC produce tailored advice and guidance to identified sectors, and proactively work with companies on this**. At launch, we propose that the NCSC focuses on sectors which form the Critical National Infrastructure of the UK, alongside those of strategic or significant economic importance, or the delivery of key public services.

The NCSC will also provide bespoke support to a small number of the most critical organisations in the UK, whose effective functioning is part of the UK's wider national security and resilience.

The NCSC will not offer an enquiries line for the general public:

"Action Fraud will continue to be the first port of call for victims to report suspected cyber crime".

However, when there is a significant cyber incident affecting the UK, the NCSC will have the leading role for government in communicating to the public, to provide reassurance and guidance on what individuals and organisations can do to better protect themselves



Defence networks carry some of the most sensitive information held by government, and being able to communicate and operate securely is an essential requirement for our armed forces. Our specialist teams will work with the Ministry of Defence, and other users of very secure communications, to ensure that operational needs are met, and that the capabilities needed to operate both independently and with our allies are available in the future.

We will work with the cyber security industry to help ensure organisations of all kinds can find cyber security products and services that are high quality and meet their needs.

We will work closely with Law Enforcement and the wider public sector to support cyber security awareness campaigns – for example as part of the NCA's work to combat cyber crime. At the same time we will publish straightforward and authoritative technical guidance about specific platforms and technologies. All of this material will be freely available online.

Chancellor of the Exchequer announcing National Cyber Security Centre

"Getting cyber security right requires new thinking. But certain principles remain true in cyberspace as they are true about security in the physical world. Citizens need to follow basic rules of keeping themselves safe – installing security software, downloading software updates, using strong passwords. Companies need to protect their own networks, and harden themselves against cyber attack. The starting point must be that every British company is a target, that every British network will be attacked, and that cyber crime is not something that happens to other people."

"Now we need to bring more coherence to our efforts, so that businesses know there is a single place they can go for advice and help. Today [17 Nov 2015] I can announce that in 2016 we will establish a single National Cyber Centre, which will report to the Director of GCHQ. The Centre will be a unified source of advice and support for the economy, replacing the current array of bodies with a single point of contact.

"The Centre will make it easier for industry to get the support it needs from government. And make it easier for government and industry to share information on the cyber threat to protect the UK. Reporting to GCHQ will mean the Centre can draw on the necessarily secret world-class expertise within this organisation. But the Centre will also have a strong public face and will work hand in hand with industry, academia and international partners to keep the UK protected against cyber attacks.

"And over time, we will build several important capabilities in the new Centre. It will give us a unified platform to handle incidents as they arise, ensuring a faster and more effective response to major attacks. And we will build in the National Cyber Centre a series of teams, expert in the cyber security of their own sectors, from banking to aviation, but able to draw on the deep expertise here, and advise companies, regulators, and government departments. Building the National Cyber Centre will be a hugely ambitious and important undertaking that reflects this government's commitment to making the UK secure in cyberspace."

Rt. Hon. George Osborne MP
Chancellor of the Exchequer

"The cyber threats to the UK are significant and varied. They include cyber terrorism, fraud and serious and organised crime, espionage, and disruption of CNI as it becomes more networked and dependent on technology, including networks and data held overseas. Cyber risks underpin many of the other risks we face."

NSS Risk Annex on Cyber

How to get involved

Contact:
opendoor@ncsc.gov.uk

Any enquiries regarding this publication should be sent to us at opendoor@ncsc.gov.uk.

This publication is available for download at www.official-documents.gov.uk.