



October 2016

NATIONAL CYBER SECURITY CENTRE

The National Cyber Security Centre was launched on 1st October. The NCSC has 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. The NCSC 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. 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.

When a serious cyber incident occurs, the NCSC 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. The NCSC will help by connecting victims with commercial companies who excel at cyber incident response. At the same time it 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 society 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.

How the NCSC works

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. Partners will be needed including 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.

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. The NCSC's systems and working practices will enable the Centre 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.

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, the Centre proposes 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).