Cabinet Office

The National Cyber Security Strategy Our Forward Plans – December 2013

Cabinet Office

The UK Cyber Security Strategy
Report on progress – December 2013
Our Forward Plans

Two years have passed since we first set out our goals in the National Cyber Security Strategy. Much has been done towards delivering the four Strategy objectives:

- making the UK one of the most secure places in the world to do business in cyberspace;
- making the UK more resilient to cyber attack and better able to protect our interests in cyberspace;
- helping shape an open, vibrant and stable cyberspace that supports open societies;
- building the UK's cyber security knowledge, skills and capability.

The first year saw activity across a wide range of areas and with many partners, generating increasing momentum across the National Cyber Security Programme (NCSP). Key enabling structures and capabilities were introduced or enhanced, and groundwork laid. Over the past year we built on this groundwork to deliver real progress. This year will be about cementing that progress and filling gaps where work to date has shown us there is more to do. This document gives an outline of these forward plans, which focus on our core goals of:

- further deepening our national sovereign capability to detect and defeat high-end threats;
- ensuring law enforcement has the skills and capabilities needed to tackle cyber crime and maintain the confidence needed to do business on the Internet;
- ensuring critical UK systems and networks are robust and resilient;
- improving cyber awareness and risk management amongst UK business;
- ensuring members of the public know what they can do to protect themselves, and are demanding good cyber security in the products and services they consume;
- bolstering cyber security research and education, so we have the skilled people and know-how we need to keep pace with this fast-moving issue into the medium-term; and
- working with international partners to bear down on havens for cybercrime and build capacity, and to help shape international dialogue to promote an open, secure and vibrant cyberspace.

Over the coming year we will maintain the fast pace of delivery, assessing our progress and adjusting plans as necessary in response to changes in the technological and threat environment. Improving the UK's cyber security remains a top priority for Government. The 2013 Spending Review directed a further £210 million to the NCSP in 2015-16, on top of the £650 million set aside over the previous four years. Further work to meet the objectives of the Strategy will be outlined in future reports.

Objective 1: Making the UK one of the most secure places in the world to do business in cyberspace

Working in partnership with the private sector to improve cyber security in the UK continues to be central to our approach. The private sector drives innovation and investment in this area, but it also owns most of the networks which are at risk, and suffers much of the damage caused by cyber attacks.

Under the NCSP much work has been done already in reaching out to the private sector in order to raise awareness of the threat and to encourage business to embed effective cyber security risk management practices. In the coming year:

- we will expand the Cyber Security Information Sharing Partnership (CISP), with a target to include 500 member firms by the end of 2014. Launched in March 2013, CISP provides a platform for companies to share cyber threat information in real time. A fusion cell (composed of industry and government network defence analysts) examines the data and provides enriched information and advice to the CISP community. CISP already involves over 250 large firms and major organisations, with more joining each week, and has developed partnerships with organisations such as Universities UK and the Law Society to promote membership in their sectors;

- we will continue to work with businesses and their representative groups and trade associations to underline the messages set out in our Cyber Security Guidance for Business booklet – the ’10 Steps’ - ensuring these messages reach the largest possible audience. Over the past year we have worked with, amongst others, the Institute of Chartered Secretaries and Administrators, the Audit Committee Institute (Audit Chairs), the Association of General Counsel, Company Secretaries of the FTSE 100, and the Institute of Risk Management to establish cyber security as a significant business risk requiring the attention of company boards. This drive will continue over the coming months. We will continue to complement our corporate governance work through partnerships with key sector bodies to raise cyber security awareness, develop shared understanding of the impact of cyber attacks across the economy, and prompt behavioural change. Special partnerships have been established with the professional business services sector, with life sciences, retail, universities and defence;

- we will repeat the initiative we carried out this year in partnership with the UK’s biggest audit firms to provide a cyber governance health check for FTSE 350 companies. The results of this year’s health check will be used by firms’ auditors to hold more in-depth follow-up conversations with company boards;

- we will continue to work with the investor community to ensure that they have the necessary guidance and information to ask the right questions of boards and draw conclusions on firms’ competence in governing cyber risk;

- in January we will publish, with the Institute of Chartered Accountants, the Financial Conduct Authority and others, guidance for those involved in corporate finance transactions on how they can protect themselves against cyber risks. As part of a suite of supporting guidance to help firms navigate the market and ensure they are taking security into account when they contract for services, advice on cloud provision and mobile will be published by GCHQ in the new year;

- we will continue to make sure our message reaches smaller firms by providing targeted information and advice for SMEs. In April 2013 we produced a version of our business guidance suitable for smaller companies https://www.gov.uk/government/publications/cyber-security-what-small-buisnesses-need-to-know). This was supported by activity to reach out to this audience in partnership with industry and through existing channels such as Get Safe Online and Action Fraud. In the coming year we will target SMEs with a special strand of our planned public awareness campaign, to begin in January 2014 (see below under Objective 4 for details). The campaign will signpost SMEs to an internet portal where they can obtain trusted advice and guidance;

- we will roll forward the cyber security innovation voucher scheme launched last year to help small firms get access to the security support they need to protect their business ideas. Over the coming year we will make a further £500,000 available to small firms through this route from the NCSP, supported by funding from the Technology Strategy Board;

- we will work with Nominet to support their initiative to provide a tool that will help small businesses identify security issues affecting their websites. Nominet is also exploring how it can work alongside CERT-UK to offer other practical cyber security help to small businesses.

Awareness-raising activity will continue at pace. However, as we made clear in the UK Cyber Security Strategy, awareness-raising in isolation is unlikely to lead to the scale of sustained behaviour change needed to address adequately the cyber threat faced by businesses. We also want to encourage the right market structures and provide incentives to ensure that managing cyber risk is recognised as integral to good business practice. We want boards, customers and investors to think about cyber security issues when they are making purchasing or investment decisions. We want the market to identify and reward good practice.

This year the Government supported the development of an industry-led organisational standard for cyber security, to clarify what good cyber security practice looks like for companies large and small, and to enable firms who attain such a standard to make this a differentiator in the marketplace. Working with the British Standards Institute, the Information Security Forum and other stakeholders, Government will publish the completed standard at the end of March so that companies can begin to accredit themselves against it from that point. Over the coming year:

- we will encourage firms to adopt the standard themselves and to spread its adoption among their suppliers. Government will work with the CBI and trade associations to encourage use of the standard amongst their members;

- as an incentive to adoption, and to ensure that Government's own supply chain is properly protected, we will mandate the preferred standard in Government's own procurement where proportionate and relevant. Members of the Defence Cyber Protection Partnership (DCPP) who supply MoD have already said they will adopt it as a minimum for Government contracts. They are BAE Systems, BT, Cassidian, CGI Logica, General Dynamics, HP, LMUK, QinetiQ, Raytheon, Rolls-Royce, Selex Finmeccanica, and Thales UK;

- we will work with regulators to drive adoption among those companies that own and manage the UK's critical national infrastructure;

- we will work with auditors, investors and insurers to encourage them to factor the standard into their own judgements of the risk companies are carrying;

- we will work with the US and internationally to ensure alignment between standards where we can so as to increase the standard's market reach and reduce compliance costs for businesses.

Alongside this:

- we will continue the annual Information Security Breaches Survey, so we can track how the private sector is responding to cyber security threats, and allow firms to benchmark their own performance against that of their peers in order to drive up industry standards;

- we will continue to extend 'kite marking' of cyber security professionals, products and services to stimulate supply, drive up standards and help customers access and navigate the market. Over the last year GCHQ has launched its Commercial Product Assurance scheme to certify commercially-available cyber security products for use in the public and private sectors. The first products have now completed certification with more to follow in 2014. At the same time GCHQ is expanding its Service Assurance capability to cover a broad range of cyber services. A number of commercial cyber incident response providers have been certified to provide clean-up services to organisations that have fallen victim to cyber attack; in the coming year certification will be extended to other services including security monitoring services. The CESG Certified Professional scheme has already awarded over 1000 certificates to cyber security professionals.

Greater awareness of cyber risks and better understanding of how to manage them will create significant opportunities for the UK cyber security sector at home and as exporters. To ensure that business can take advantage of these, we this year launched a 'Cyber Growth Partnership', in conjunction with techUK (which represents 850 UK technology organisations). This high level group brings Government and industry together to identify and remove barriers to progress. In the coming months it will:

- promote take-up of a 'Cyber Supplier to HMG' badge which companies that supply cyber products and services to Government can use to demonstrate their credentials to potential export customers;

- co-ordinate export campaigns in key markets and a strong cyber offering at the UK's Security and Policing Exhibition planned for March;

- work with Government further to develop the provision of cyber security training and education to support the growth of the UK's cyber industry;

- through these and other initiatives, help deliver by 2016 the Government's target to secure £2 billion's worth a year of cyber export orders, increasing the UK's share of the market as that market grows.

As the volume of business conducted over the internet grows, tackling cyber crime continues to be a key area of investment for the NCSP. Responding to this threat will ensure the UK is a safe environment in which people and industry feel secure to do business online.

A key part of our response is investing in new police capabilities to pursue criminals operating in cyberspace, in line with the Pursue strand of the Serious and Organised Crime Strategy. Over the past year we have established the National Cyber Crime Unit (NCCU) as part of the new National Crime Agency, bringing together in one place the specialist cyber capabilities that had existed in separate organisations. With NCSP funding we have increased the number of specialist policemen and prosecutors working on cyber, and trained a cadre of cyber trainers to support the upskilling of our police forces. The NCCU will further develop the skills and capabilities to tackle the most serious of cyber crimes, working with national and international partners relentlessly to pursue cyber criminals, wherever they are located.

Even before it was formally launched, the NCCU helped smash a $500 million worldwide computer scamming ring through a joint operation with the FBI in over 80 countries. More recently, a joint operation between the NCCU, the FBI and other law enforcement partners led to the arrest of 11 people for crimes that are estimated to have involved over $200 million of losses to individuals and businesses. We will continue to build up the NCCU's capacity to prevent, disrupt and investigate cyber attacks. With NCSP funding the NCA is investing in specialist expertise and state of the art equipment, but is also ensuring that cyber is a key strand of its broader work. Half of the NCA's 4,000 officers are being trained to become digital investigators.

In addition to investing in a national specialist capability, we are building new teams in each of the nine Association of Chief Police Officers (ACPO) regions to provide a regional cyber expertise across England and Wales. These teams, based in each of the Regional Organised Crime Units (ROCUs), will run investigations and provide advice and support to the public and businesses across their region. The NCSP is investing in staff, specialist training and equipment for these teams. However this is not enough: we will also fund specialised training courses from February 2014 providing capacity to train 360 police officers a month. This will give a total of over 5,000 trained officers by March 2015. This is in addition to the existing suite of e-learning courses, which will support frontline officers in responding effectively to reported fraud and online crime. A programme board co-chaired by the ACPO National Policing lead and the head of the NCCU will oversee this work and ensure that all work on infrastructure, capabilities and skills to tackle cyber crime is fully co-ordinated and delivered to a common plan.

We have delivered an enhanced reporting tool for Action Fraud, as the UK's central reporting hub for cyber fraud, making it easier for the public to report cyber crime to a central point. We will further invest in developing this system so that those making reports will be provided with more feedback. Specific data on known frauds will be shared through the Counter Fraud Checking Service.

As well as relentlessly pursuing cyber criminals, the Government's strategy also involves preventing crime through better protecting citizens and businesses. Law enforcement has forged new links with industry including through the CISP, further improving information-sharing and joint work with the private sector to protect against cyber crime. The NCA will share intelligence on organised crime groups engaged in cyber crime with the private sector, including through participation in CISP.

The Home Office's Cyber Crime Reduction Partnership (CCRP) brings together government, industry, academia and law enforcement agencies to co-ordinate efforts on reducing cyber crime. The Partnership - which is chaired by the Security Minister (Home Office) and the Minister for Universities and Science (BIS) - will look for other opportunities to work together to design out cyber crime and provide practical help to SMEs and citizens.

Internationally, we will build on co-operation between the UK and international law enforcement agencies, including more joint operations. This will include developing a model for proactive global cyber investigations, with shared assessment of threats, joint prioritisation of targets, and burden-sharing with close international law enforcement partners.

Objective 2: Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace

A significant proportion of NCSP funds has been invested in strengthening GCHQ's ability to detect cyber attacks on UK interests. This has transformed our situational awareness in cyberspace. We have been using this increased visibility of the threat to target defensive measures and protect the UK's national and economic security interests.

We have taken steps to increase the security of Government's own computer networks. Over the last year we have been building the new Public Sector Network (PSN) to create a new security model for the sharing of services. This includes a common and standardised approach to information assurance; security monitoring; more effective policing of compliance; and greater network resilience. In order to join the PSN public sector organisations need to meet strict entrance criteria to demonstrate they have management of cyber risks in place and are not inadvertently importing cyber risk into the Network. Two-thirds of target organisations are already fully compliant, with the rest on track to meet full compliance by March 2014.

As more government service delivery moves online it is vital that our systems are secure at the same time as being straightforward to use for the public. HMRC will continue to develop its dedicated cyber capabilities to protect its customers and taxpayer revenue. It will also continue to develop its anti-phishing technology and reduce the average time between detection of fraudulent websites and take-down, which has already been reduced to 7.5 hours.

GCHQ is working with the Universal Credit programme and with other digital service programmes in DWP such as State Pension Online, the Personal Independence Payment and the Carers Allowance to make sure they are robust against attempted fraud. GCHQ will continue to work with other key public sector delivery programmes to ensure that they are acting on the best security advice.

Across Government a new identity assurance service will enable people safely and securely to verify their identity to use online services and allow Government to be confident that those using online services are who they say they are. Contracts with five identity providers have been signed and the first services using identity assurance will go live in early 2014.

At the strategic level all Government department boards and the boards of key government agencies have incorporated cyber risk into their risk management regimes. All boards will report on their cyber risk preparedness annually. This information will be shared with the National Audit Office who will scrutinise it as part of their audit of corporate controls.

As well as government's own systems we have been working to strengthen the resilience of the UK's critical private sector infrastructure to cyber attack, building on the lessons learned in successfully delivering the Olympic Games. Last year we undertook to:

- move in partnership with industry to establish CERT-UK, a national Computer Emergency Response Team, to help critical infrastructure providers and Government co-ordinate responses to cyber incidents;

- roll out the CISP as a platform for sharing situational awareness of cyber threats among critical infrastructure providers;

- work closely with key allies and like-minded partner countries on the development of security policy, co-ordinating domestic action where we can to bring mutual enhancements to national security.

All these strands of action are on track. CERT-UK will open for business early in 2014. CISP already involves over 250 organisations, with more joining each week, and is already demonstrating value. The UK has worked closely with our principal allies and partners on common security policies and approaches, including contributing to the US's National Institute of Science and Technology (NIST) framework for cyber security.

In the coming year the Centre for the Protection of the National Infrastructure, working closely with GCHQ, will continue its outreach to national infrastructure companies, ensuring that they benefit from the latest advice and guidance on potential vulnerabilities and their mitigation. As noted above, CISP will aim to double its membership to 500 organisations sharing real-time information on cyber threats. CERT-UK will become operational, helping improving national co-ordination on incident response and providing a focal point for international sharing of technical information on cyber security.

CERT-UK will deliver an expanded exercise programme to make sure that critical sectors understand and are prepared for the potential impact of a destructive cyber attack. This will build on the recent successful Exercise Waking Shark II in the finance sector, run with the Bank of England (and using the CISP platform).

Government will also work with the regulators to ensure that the companies that own and operate our critical national infrastructure are well protected against the cyber risks they face, as part of their responsibilities to ensure resilience and availability of supply. A number of regulators are already very active in driving cyber security, including the Bank of England where a recommendation from the Financial Policy Committee has led to a wide programme of work across the financial sector. Government remains committed to supporting this agenda, and is developing an enhanced offer of support on cyber to regulators and infrastructure owners and operators through GCHQ and CPNI. The Secretary of State for Business will host a summit in February for regulators and Government to agree next steps.

Objective 3: Helping shape an open, vibrant and stable cyberspace that supports open societies

The nature of the Internet means that we cannot focus our efforts on the UK alone. Cyberspace is borderless. Internationally our priority is to promote the UK's vision of an open, vibrant, stable and secure cyberspace, so that the economic and social benefits of cyberspace are protected and available for all. To do this we are working in partnership with other nations and organisations to help shape norms of behaviour for cyberspace while promoting the UK as a leader in cyberspace technology and policy. We will:

- continue to expand and strengthen the UK's bilateral and multilateral networks, and to develop international collaboration through the work of the EU, NATO, the Commonwealth and other bodies. The UK played a major part in shaping the EU Cyber Strategy adopted in June 2013, which reflected not just security, but also the important broader social and economic aspects. We will continue to work closely with EU Member States and Brussels on its implementation. We have launched formal cyber dialogues with India, Japan, Korea and Singapore, and hope to do so this year with Brazil, Chile and South Africa. The UK has also agreed to hold a formal dialogue on cyber with China;

- seize key opportunities in the year ahead to help safeguard the free and open future of the Internet. Through the series of conferences on cyberspace which started in London in November 2011, followed by Budapest in 2012 and Seoul in 2013, the UK continues to help shape international debate about the future of cyberspace. Progress on specific areas from Internet Governance to international cyber crime co-operation will now be taken forward in a range of international discussions, including the Brazil Conference in early 2014. The next conference in the London Process will take place in the Netherlands in Spring 2015;

- progress the international debate on 'rules of the road' in cyberspace, building on our role in delivering recently a successful outcome to the UN Group of Government Experts (UNGGE), which for the first time reached consensus on the applicability of International Law in cyberspace. We will support the work of the next UNGGE in further consideration of these issues. Earlier this year the UK also helped the OSCE (Organisation for Security and Co-operation in Europe) agree the first ever set of multilateral Confidence Building Measures to reduce the risk of cyber conflict through improved understanding and communication, and will continue to work constructively as an OSCE participating state in the implementation of these measures;

- continue to strengthen trans-border law enforcement co-operation on cyber crime. By November 2013, 40 countries had ratified and a further 11 had signed the Council of Europe's Budapest Convention on Cybercrime, which the UK strongly supports. UK law enforcement agencies will expand further international partnership building and joint operations;

- keep working with other countries to build up their capacity to tackle cyber threats and bear down on what could otherwise become safe havens for cyber criminals. Our Cyber Capacity Building Fund will continue to focus on producing real-world outcomes through investment in partners and international co-operation mechanisms, including the Commonwealth Cybercrime Initiative and through the Commonwealth Telecoms Organisation. UK funding will also continue to back the new Global Cyber Security Capacity Centre at Oxford University launched in November 2013: over the next year it will develop research to improve the global co-ordination and impact of practical capacity building efforts. The UK will also be working closely with global partners to ensure burden-sharing and effective co-operation, including with International Development agencies which are already involved in initiatives such as the Alliance for Affordable Internet;

- as part of this, play our part in ensuring that future cadres of global leaders will have a good understanding of cyber security issues. Each year a number of Chevening, Commonwealth and Marshall scholars from Africa, Asia, and America will attend the annual Academic Centres of Excellence in Cyber Research Conference in December and enrol in an international cyber policy course at Cranfield University.

Objective 4: Building the UK's cyber security knowledge, skills and capability

While the online world has grown exponentially, cyber security skills and capability are not increasing at a comparable rate. Our ability to defend ourselves in cyberspace depends upon a strong skills and knowledge base. The UK has a world-class cyber security sector, where the current demand for new talent is set to grow. In both the long and short term so we can match this demand we must ensure that there is a sustained supply of competent cyber security professionals who have achieved the requisite standards and certification.

Under the NCSP, Government has worked with its partners in the education sector, academia and in business to broaden the pipeline of new talent entering the field, as well as helping ensure that all people leaving education have at least a basic understanding of cyber security before entering the workforce.

In schools we are:

- supporting the "Make IT Happy" programme in primary schools. Make IT Happy is run by the Parliamentary ICT Forum (PICTFOR) with support from e-skills UK, the Institute for Engineering and Technology, the Nominet Trust and many other sponsors. Now in its seventh year of encouraging young people to learn through technology, Make IT Happy 2013 had a "Make IT Safe" theme, with free teaching resources covering internet, email and password safety available. Over 600 primary schools registered, and over 60 competition entries were submitted. Winners attended an awards ceremony in the Houses of Parliament in June;

- working with others to ensure that the new computing curriculum in secondary schools has a greater focus on how computers work and the basics of programming, as well as digital literacy and the application of IT. The new curriculum will emphasise the importance of security in the design, development and implementation of information systems, including the importance of secure coding;

- making available interactive teaching and learning materials for cyber security to all schools through the e-Skills 'Behind the Screen' initiative, aimed at GCSE and A-Level students;

- sponsoring the National Cipher Challenge through GCHQ, an online code-breaking competition run by Southampton University;

- supporting the Cyber Security Challenge to allow them to run their Schools Competition regionally and nationally twice a year. The Competition aims to inspire pupils to take more interest in computer science, gain useful skills, and encourage them to consider a career in cyber security. Close to 600 schools took part in a pilot: this will now be rolled out across the UK. The competition element will encourage pupils to submit their own ciphers. The best teams will take part in an engaging, 'face-to-face' national competition against other schools in Spring 2014;

- working with e-skills UK and cyber security professionals on their 'SecureFutures' programme, designed to demonstrate to young people how exciting cyber careers can be. The sessions emphasise the link between cyber security, risk and the law. Included are two cyber games which give young people a chance to test their skills in real-life scenarios. As part of the initiative, schools are also offered the chance to host a secure futures creative curriculum day with cyber security as the unifying topic;

In universities we are:

- building cyber security into university degrees: Government is partnering with the Institution of Engineering and Technology (IET) to support and fund the Trustworthy Software Initiative, under which teaching materials have been developed to educate students on relevant technical degree courses on why trustworthy software is important. This material will have been taught to students at eight universities by March 2014. From 2015 a module on cyber security will be a mandatory component of all software engineering degrees accredited by the IET;

- accrediting the content of cyber masters degrees with the Cyber Security Skills Alliance (IET, BCS - The Chartered Institute for IT, the Information Assurance Advisory Committee IAAC, e-skills UK and the Institute of Information Security Professionals), to provide reassurance and clarity on the content of current cyber Masters degrees;

- creating more PhDs for the benefit of the wider economy. Two Centres of Doctoral Training have been created to deliver multidisciplinary training and provide the skills needed by the next generation of doctoral-level cyber security experts. They are engaging with industry to ensure the training reflects the complex and dynamic nature of cyber threats. These centres will deliver 66 additional PhDs from 2017. The first cohort of students started in October 2013. In parallel GCHQ will continue to expand their PhD studentship programme with NCSP funds;

- developing the community of cyber security research being carried out in the UK: We have awarded 11 UK Universities the status of “Academic Centre of Excellence” in recognition of the exemplary standard of their cyber research. This year we will establish a third Research Institute to look at Trustworthy Industrial Control Systems. Industrial control systems now play a major role in ensuring the correct functioning of significant parts of the UK’s critical national infrastructure. In recognition of this the Centre for the Protection of National Infrastructure (CPNI) and the Engineering and Physical Sciences Research Council (EPSRC) will launch an Institute to help build capability and find innovative ways to ensure the protection of the industrial technologies that support our key services. This complements two previously established multi-disciplinary Institutes on Automated Program Analysis and Verification, and on the Science of Cyber Security.

To make sure we are drawing on the widest possible pool of talent, we are also working to encourage apprenticeships and other formation routes, especially those that provide people with an entry into cyber mid-career. We are:

- partnering with e-skills UK, training providers and industry to develop new cyber programmes that match private sector needs and will increase the number of apprenticeships in cyber security. This will complement the Government’s own technical apprenticeship scheme for GCHQ and the other Intelligence Agencies which aims to identify and develop talent in school and university age students. This year GCHQ have recruited 100 apprentices to be enrolled on a tailored two-year Foundation Degree course;

- raising awareness of future cyber security careers through the Cyber Security Challenge and its network of sponsors, creating opportunities for employers and talent to come together. The Challenge attracted over 2000 new joiners this year;

- increasing the number of cyber internships, working with e-skills UK. This builds on the IAAC Cyber Internships Pilot and previous best practice by e-skills UK and The Council of Registered Ethical Security Testers (CREST) and others. The programme engages with cyber security and other businesses to promote the benefits of employing interns, focussing on a targeted list of universities which deliver an industry respected degree or postgraduate cyber course. It aims to raise the profile of internships focused on cyber security and the exciting opportunities for cyber security careers. 2014 work will look further to develop best practice internship guidance and materials (based on previous e-skills UK experience) for employers, universities, students, graduates and interns;

- working with industry and e-skills UK to develop the professional formation routes for cyber security careers. A ‘Learning Pathways’ pilot project will be rolled out into a fully functioning system over the coming year. The Pathways will be particularly relevant for those individuals wishing to transition into a cyber career from other related professions and explain the skills and knowledge required to perform cyber security roles such as Security Architect;

- ensuring that cyber professionals have clearly defined career development through the CESG Certified Professional Scheme established by GCHQ: this will help them improve their skills as well as help Government and industry recruit people with the right skills at the right level to the right jobs;

- constantly examining new ways to harness and attract the talents of the cyber security specialists that are needed for critical areas of work. To this end, the Ministry of Defence has launched its Cyber Reserve. Its aim is to harness the talent and skills of the nation in the cyber field, drawing not only from those already possessing the skills required in industry, but also those who have achieved a level of technical interest as part of self-education.

We are using Internet-enabled approaches to make sure we reach the largest possible catchment:

- with NCSP funding, the Open University is developing a Massive Open Online Course (MOOC) in cyber security, to be run for the first time by summer 2014. The course has the potential to reach 200,000 students, including internationally. The MOOC is intended to run over an eight week period and will be presented four times a year for three years. The goal is to help raise awareness of cyber security among a mass audience as well as providing a high quality course which will make the subject accessible to non-specialist learners and encourage those with an interest in the subject to study further.

We are determined to ensure that consumers are better informed of the potential risks and what they can do to reduce them, so that they can take steps to protect themselves online and are in a position to demand better cyber security in the products and services they buy:

- from January 2014 the Home Office will deliver a major public awareness campaign together with a range of private sector partners including Facebook, BT, a number of anti-virus companies such as Sophos, and banks as well as community and trade organisations. This campaign builds on the work of GetSafeOnline and the National Fraud Authority, and on previous successful campaigns such as Devils in Your Details;

- the campaign aims to help consumers adopt a range of behaviours which should leave them better protected, such as keeping their anti-virus software up to date and using strong passwords. The campaign will signpost consumers to an internet portal providing further trusted advice and guidance;

- Internet Service Providers will play their part in helping their customers get safer online. The UK internet industry and Government have co-developed a series of Guiding Principles to improve the online security of the ISPs' customers and limit the rise in cyber attacks. These Guiding Principles recognise that the ISPs and other service providers have a role, alongside consumers themselves and the Government, in minimising and mitigating the cyber threats inherent in using the internet. They provide a consistent and best practice approach to help inform, educate, and protect ISPs' customers from online threats;

- to measure impact we will use our "Cyber Confidence tracker", which tracks online safety perceptions and behaviours, providing both a benchmark and measurement of success for all awareness and behaviour change activities.

We have set out above key elements of our planned activity over the next 12 months in support of the National Cyber Security Strategy. In a year's time we will again review progress against the aims and objectives of the Strategy, learning lessons and responding to new threats and challenges, with the aim of protecting UK interests in cyberspace and making this country one of the best places in the world to do business online.