# UK Cyber Security Strategy 2022

On the 16th December 2021, Government published its revised Cyber Security Strategy 2022. This can be found here:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1040805/National_Cyber_Strategy_-_FINAL_VERSION.pdf

The Strategy is 130 pages long and covers a wide variety of topics that members may find of interest but are very general in nature. These include general proposals for general cyber security hygiene, skills and international engagement. However, in this note I have extracted the most relevant portions of the text and highlighted those parts that are directly relevant to BEAMA members. The strategy out a series of intentions for government to carry out by 2025. BEAMA will advise as these are announced. It is worth noting that the strategy indicates that government will be making proposals for a UK NIS2 in 2022.

Excerpts from Strategy

## Drivers

*34. We are increasingly seeing the interaction of established businesses in regulated sectors, such as telecoms and energy, with new and largely unregulated businesses,* ***such as those providing microgeneration, electric vehicle charging or 'connected places' capabilities.*** *Critical infrastructures will become much more distributed and diffuse and this fundamentally changes how regulation will impact the security of the critical functions and services we rely on. This diversification will also affect our wider national security, making it more difficult to gain access to information whether for law enforcement or cyber security. This change in environment will also affect products and services more widely outside of our traditional critical national infrastructure.*

## Our National Response

*52 ….The strategy also builds on our successful work to promote approaches that build security into new technologies, making them "secure by design". This will mean investing and making more use of regulatory and legislative levers where necessary* ***to promote more diverse, secure and resilient technology supply chains****, as we have done in telecoms….*

**Roles and responsibilities across the UK**

*Building a resilient and prosperous digital UK*

*88. …The forthcoming National Resilience Strategy, a key commitment of the Integrated Review, will set out* ***the overarching approach to national resilience****….*

*More resilient Critical National infrastructure*

> *Resilience to common attack methods and* ***more advanced protection according to risk posture***
>
> *Understand and address risk arising from* ***digitalisation and new technologies***

*More resilient Businesses and Organisations*

> *Uptake of standards such as Cyber Essentials and more transparency*

*Market incentives and more local support*

*Better regulation in targeted areas including digital services and personal data*

**Objective 1: Improve the understanding of cyber risk to drive more effective action on cyber security and resilience**

*97. ….By 2025 Government will:*

*98. have an up to date strategic understanding of the nation's cyber risk….*

*100. Across the UK's CNI, we will have a more sophisticated understanding of cyber risk.*

> *We will increase the adoption of the Cyber Assessment Framework (CAF) or equivalents across CNI sectors, and improve comparability with other cyber security assessment and reporting frameworks in use.* ***We will complete criticality reviews and map dependencies within CNI and its supply chains.*** *We will build stronger partnerships with CNI owners and operators to improve access to threat and risk information, and agree risk posture.* ***And we will work to understand new risks or where new CNI is emerging as a consequence of digitalisation and new technologies, including as part of broader priorities such as the transition to Net Zero.***

**Objective 2: Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens**

*106. Our efforts to reduce harm at scale will also include tackling systemic risks from the digital supply chain. Where necessary we will intervene to promote supply chain diversification, as we are doing in telecommunications; we will strengthen our collective economic security with improved information-sharing and robust, predictable and proportionate approaches to foreign direct investment (FDI) screening in critical sectors,* ***and establish clear requirements for critical and common suppliers to government.***

*108. Cyber risks to UK critical national infrastructure are more effectively managed. Such services are by definition those that the country relies on most. We will continue to work closely with operators to achieve resilience against common attack methods as quickly as possible and to put in place more advanced protections where appropriate. For Operators of Essential Services designated under the NIS regulations this means at least meeting the baseline standard set by the relevant Competent Authorities for each sector.*

*109. In support of this outcome, we will review the government's ability to hold CNI operators to account to ensure they invest in the cyber security of critical systems and effectively manage their risk,* ***including from their supply chains****. We will strengthen the regulatory framework, to improve its coverage, powers, and agility to adapt, within the context of broader national security risk* ***and rapidly changing threat and technology. This will start with a consultation on reforms to the NIS regulations****, implementing the new security framework for UK telecommunications providers* ***and developing a proportionate regulatory framework to ensure that the future smart and flexible energy system the UK requires to deliver Net Zero will be secure and resilient to cyber threats.***

*110. Alongside this we will: enhance the capability of regulators; invest in skills to improve CNI operators' ability to attract, develop, and retain cyber professionals (see UK Cyber Ecosystem chapter);* ***and support operators' management of supply chain risk by stepping up engagement with critical suppliers and exploring the full range of levers, from guidance to legislative and procurement related proposals.***

**Objective 3: Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks**

*121. Government and CNI are more prepared to respond to and recover from incidents, including through better incident planning and regular exercising.* ***We will help UK government and CNI operators find the cyber exercising and incident management services they need from the marketplace by expanding the NCSC's accredited scheme for Cyber Incident Response and introducing a new scheme for exercising.***

*123. Within CNI we will set out clear requirements for exercising and testing or adversary simulation across CNI operators, and* ***stimulate innovation and collaboration in incident response and exercising****, considering application of models such as the Financial Sector Cyber Collaboration Centre. And as part of our ambitions on technology (outlined in the next chapter)* ***we will establish a national laboratory for operational technology security as a centre of excellence for testing, exercising and training on critical industrial technologies*** *to build capability in this area, in collaboration with industry, academia and international partners.*

## Taking the lead in the technologies vital to cyber power

135. The UK is regarded as a world leader in research into the **security of operational technologies and critical industrial control systems,** and in our ability to test and exercise them in the UK. We will establish a **national laboratory for operational technology security in partnership with industry and academia.** It will host world leading research programmes and provide government, military, industry and international partners with the facilities for exercising and testing these technologies here in the UK. And as confirmed in the 5G Telecoms Supply Chain Diversification Strategy, we will establish the UK Telecoms Lab, bringing together the government and the regulator with industry to support the new telecoms security framework and help to increase the diversity of telecoms equipment vendors in the UK's supply chain.

Objective 3: Secure the next generation of connected technologies, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply

144. Consumer connectable products sold across the UK **meet essential cyber security standards**. We will **introduce and implement the Product Security and Telecommunications Infrastructure Bill** to enable enforcement of minimum security standards in all new consumer connectable products sold in the UK. **We will support a cyber secure transition to a smart and flexible energy system, including smart electric vehicle charge-points and energy smart appliances. We will work with standards bodies, industry and international partners to influence the global consensus on technical standards.** And we will help UK organisations to procure, deploy and manage connected devices in a more secure way, including by means of new security guidance for enterprise connected devices.

## Related Government Policy Areas:

The Integrated Review
The National Data Strategy
The plan for growth
The Innovation Strategy
The Plan for Digital Regulation
The National AI Strategy

The Net Zero Strategy
Forthcoming National Resilience Strategy
Forthcoming Digital Strategy
The Beating Crime Plan
Forthcoming Government Cyber Security Strategy
Forthcoming Incentives & Regulations Review 2021