TRANSATLANTIC CYBER SECURITY BUSINESS NETWORK

Government Cyber Security Strategy: 2022 to 2030

The first ever UK Government Cyber Security Strategy has been published this week. It sets out a vision to ensure core government functions are resilient to cyber-attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power. Government's central aim is set out as ensuring critical functions are significantly hardened to cyber-attacks by 2025, with all Government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.

This is the first government-specific strategy, it follows the publication in 2021 of the broader National Cyber Strategy and the Integrated Review that has put cyber and technology at the heart of the UK's place in the world. Key points are as follows.

Strategic pillars

The strategy centres around two strategic pillars which define the Government's approach to achieving this central aim:

1. **Build a strong foundation of organisational cyber security resilience**: recognising that failings of one organisation can have significant implications for many others, this pillar aims to ensure all individual organisations not only build their own resilience but also recognise the criticality of the function they have responsibility for.
2. **'Defend as one'**: harnessing the value of sharing cyber security data, expertise and capabilities across Government to address cyber security issues. This is underpinned by the establishment of a Government Cyber Coordination Centre (GCCC), a joint venture between the Government Security Group, Central Digital and Data Office and the NCSC. The centre will be based in the Cabinet Office.

Objectives

The Pillars are supported by the following five objectives which provide a framework to be applied across the whole of Government:

- **Manage cyber security risk:** Information about vulnerabilities will be shared across Government to improve coordination and identify and manage cross government risks.
- **Protect against cyber-attack**: Government will develop its shared capabilities, tools and services to address common cyber security issues at scale.
- **Detect cyber security events**: enhanced coordination and monitoring will aim to ensure Government can detect at pace and facilitate coherent responses.
- **Minimise the impact of cyber security incidents**: Government will seek to establish the mechanisms to test and exercise incident response plans.
- **Develop the right cyber security skills, knowledge and culture**: Government will aim to improve cyber security awareness and knowledge across all public sector workers. They will also incentivise and promote Government cyber security careers.

The private sector

The Government notes the fundamental role that private sector partners have in the development, operation and delivery of government functions. Accordingly, the Government aims to address cyber security challenges in collaboration with the private sector and will work to strengthen partnerships with private sector organisations.

However, the strategy also notes that it cannot compete with the private sector to attract and retain cyber security professionals. It will seek to address this by adopting a single cyber capability pay framework across Government, linked to accreditation. Government believes that directly linking pay to skill level will enable it to better compete with the private sector. A drive towards strengthening a culture of inclusion and improving representation will also be a key focus to attract and retain talent.

International partners

Similarly to the private sector, the strategy recognises that Government relies on partnerships with international allies to strengthen its cyber resilience. This is because, as highlighted in the National Cyber Strategy, the cyber domain transcends international boundaries. Government will therefore continue to work with international allies to share knowledge and expertise and defend against common threats.

Implementing the strategy

The Government's implementation plan includes a range of initiatives being rolled out over the next eight years. Success will be measured by government organisations meeting the outcomes set out in the appropriate Cyber Assessment Framework (CAF) profile. This assurance framework is comprised of four objectives: managing security risk; protecting against cyber-attack; detecting cyber security events; and minimising the impact of cyber security incidents. Further details are in the annex.

2022-25 initiatives include:

Manage cyber security risk

- Investment in vulnerability management, including a vulnerability reporting service for the whole of Government.
- Further embed strategic partnerships with the private sector, academia and international partners

Protect against cyber attack

- Implementation of 'secure by design' framework across Government
- Manage, upgrade or remove legacy technology across the Government estate
- New Government classifications policy published and implemented

Detect cyber security events

- Enhanced mechanisms to share incident and cyber security event information
- Establish common language for organisations to record information about cyber security incidents and 'near misses'

Minimise the impact of cyber incidents

- Routine cyber security exercising of Government critical functions
- Independent review (lessons learnt) process for all serious and or cross Government cyber security incidents and vulnerabilities

Develop the right cyber security skills, knowledge and culture

- Establish the Government Security Learning Academy
- Developed career pathways for Government cyber professions
- Establish multiple entry points into the cyber profession
- Deliver a programme of cyber security culture improvement

2025-30 initiatives include:

Manage cyber security risk

- Enhanced automated, live threat information shared at scale across Government and wider public sector

Protect against cyber attack

- Harnessing of emerging technologies to enhance Government cyber security

Detect cyber security events

- Every Government digital system to have 24/7 security monitoring
- Harnessing future technology to grow and accelerate detection of cyber security events
- Establish a strategic threat hunting programme for Government, including the use of shared capability and deception tactics

Minimise the impact of cyber incidents

- Provision of expert exercising capability available across the public sector

Develop the right cyber security skills, knowledge and culture

- Expand the cyber apprentice and training programme
- Invest further in regional security centres for Government
- Adopt a single pay framework for cyber profession across Government