Department for
Science, Innovation
& Technology

Viscount Camrose

Parliamentary Under Secretary
of State (Minister for AI and
Intellectual Property)

3rd Floor, 100 Parliament
Street
London SW1A 2BQ

Rt Hon Greg Clark MP,
Chair,
Science, Innovation and Technology
Committee,
House of Commons,
London,
SW1A 0AA

W: www.gov.uk/dsit

23/01/2024

PUBLICATION OF THE GOVERNMENT'S RESPONSE TO THE CALL FOR VIEWS ON SOFTWARE RESILIENCE AND SECURITY FOR BUSINESSES AND ORGANISATIONS.

I am writing to the Science, Innovation and Technology Committee to inform them of the government's intention to publish a response to the Government call for views on software security and resilience for businesses and organisations.

Software underpins our digital economy, it plays a crucial and ever-increasing role in the UK economy, and the day-to-day lives of citizens. It is also an area of significant cyber risk, and the ever increasing complexity of software means that malicious actors are exploiting novel vulnerabilities to cause harm. In June 2023, a cyber-attack on payroll provider Zellis' MOVEit software allowed hackers to access personal details of staff and employees at a wide range of UK organisations, and only last year NHS 111 services were impacted by an attack on Advanced software.

In response to this pressing issue, in February 2023, the then Department for Digital, Culture, Media and Sport (DCMS) published a call for views which sought views from industry about the cyber security risks of software, how they are currently managed by organisations in the UK, and where government could take action to mitigate them. Over the course of twelve weeks, my department engaged with over 200 stakeholders through a series of workshops, webinars and bilateral meetings from a range of backgrounds. 136 written responses were submitted to the Call for Views from software vendors, developers and customers, academics, insurance bodies, cyber security experts and other industry stakeholders. This breadth of views has formed the basis for the analysis which has shaped the government's approach to software security and resilience moving forward.

The Government response sets out the key themes that emerged from the call for views, as well as outlining the government's proposed approach to improving software security and resilience across the UK.

The response presents an ambitious package of policy measures and interventions, centred around a voluntary Code of Practice for software vendors and developers. This will set clear expectations for software vendors, who sit at the nexus between development of software and end users, to ensure software is developed within secure development frameworks and guided by secure by design principles. This will also set clear expectations of information-sharing between customers and vendors, and require regular vulnerability testing and reporting.

In conjunction with the Code of Practice, the package of measures developed by this call for views will raise the baseline expectations of software security and resilience in the UK considerably, improving accountability and transparency across supply chains. This approach will provide the fundamental building blocks to securing the development and use of software across all applications, including in AI models, the security of which, as you know, is a key focus of my department and this government.

I will deposit copies of this letter and the official government response in the Libraries of both Houses.

Yours sincerely,

Viscount Camrose

Parliamentary Under Secretary of State (Minister for AI and Intellectual Property), Department for Science, Innovation and Technology