UK and US develop new global guidelines for AI security

New guidelines for secure AI system development will help developers of any systems that use AI make informed cyber security decisions at every stage of the development process.

- Agencies from 18 countries, including the US, endorse new UK-developed guidelines on AI cyber security
- Guidelines for Secure AI System Development, led by GCHQ's National Cyber Security Centre and developed with US's Cybersecurity and Infrastructure Security Agency, build on AI Safety Summit to establish global collaboration on AI
- Written in partnership with industry, guidelines advise developers on the security of AI systems

THE UK has today (Monday) published the first global guidelines to ensure the secure development of AI technology.

In testament to the UK's leadership in AI safety, agencies from 17 other countries have confirmed they will endorse and co-seal the new guidelines.

The guidelines aim to raise the cyber security levels of artificial intelligence and help ensure that it is designed, developed, and deployed securely.

The Guidelines for Secure AI System Development have been developed by the UK's National Cyber Security Centre (NCSC), a part of GCHQ, and the US's Cybersecurity and Infrastructure Security Agency (CISA) in cooperation with industry experts and 21 other international agencies and ministries from across the world – including those from all members of the G7 group of nations and from the Global South.

The new UK-led guidelines are the first of their kind to be agreed globally. They will help developers of any systems that use AI make informed cyber security decisions at every stage of the development process – whether those systems have been created from scratch or built on top of tools and service provided by

others.

The guidelines help developers ensure that cyber security is both an essential pre-condition of AI system safety and integral to the development process from the outset and throughout, known as a 'secure by design' approach.

The product will be officially launched this afternoon at an event hosted by the NCSC, at which 100 key industry, government and international partners will gather for a panel discussion on the shared challenge of securing AI. Panellists include Microsoft, the Alan Turing Institute and UK, American, Canadian, and German cyber security agencies.

NCSC CEO Lindy Cameron said:

> *We know that AI is developing at a phenomenal pace and there is a need for concerted international action, across governments and industry, to keep up.*
>
> *These guidelines mark a significant step in shaping a truly global, common understanding of the cyber risks and mitigation strategies around AI to ensure that security is not a postscript to development but a core requirement throughout.*
>
> *I'm proud that the NCSC is leading crucial efforts to raise the AI cyber security bar: a more secure global cyber space will help us all to safely and confidently realise this technology's wonderful opportunities.*

In a keynote speech at Chatham House in June, NCSC CEO Lindy Cameron warned about the perils of retrofitting security into AI systems in years to come, stressing the need to bake security into AI systems as they are developed, and not as an afterthought.

These guidelines are intended as a global, multi-stakeholder effort to address that issue, building on the UK Government's AI Safety Summit's legacy of sustained international cooperation on AI risks.

CISA Director Jen Easterly said:

The release of the Guidelines for Secure AI System Development marks a key milestone in our collective commitment—by governments across the world—to ensure the development and deployment of artificial intelligence capabilities that are secure by design.

As nations and organizations embrace the transformative power of AI, this international collaboration, led by CISA and NCSC, underscores the global dedication to fostering transparency, accountability, and secure practices. The domestic and international unity in advancing secure by design principles and cultivating a resilient foundation for the safe development of AI systems worldwide could not come at a more important time in our shared technology revolution.

This joint effort reaffirms our mission to protect critical infrastructure and reinforces the importance of international partnership in securing our digital future.

Science and Technology Secretary Michelle Donelan, said:

I believe the UK is an international standard bearer on the safe use of AI. The NCSC's publication of these new guidelines will put cyber security at the heart of AI development at every stage so protecting against risk is considered throughout.

Just weeks after we brought world-leaders together at Bletchley Park to reach the first international agreement on safe and responsible AI, we are once again uniting nations and companies in this truly global effort.

In doing so, we are driving forward in our mission to harness this decade-defining technology and seize its potential to transform our NHS, revolutionise our public services and create the new, high-skilled, high-paid jobs of the future.

Secretary of Homeland Security Alejandro Mayorkas said:

We are at an inflection point in the development of artificial intelligence, which may well be the most consequential technology of our time. Cyber

security is key to building AI systems that are safe, secure, and trustworthy.

The guidelines jointly issued today by CISA, NCSC, and our other international partners, provide a common sense path to designing, developing, deploying, and operating AI with cyber security at its core. By integrating 'secure by design' principles, these guidelines represent an historic agreement that developers must invest in, protecting customers at each step of a system's design and development.

Through global action like these guidelines, we can lead the world in harnessing the benefits while addressing the potential harms of this pioneering technology.

The guidelines are broken down into four key areas – **secure design**, **secure development**, **secure deployment**, and **secure operation and maintenance** – complete with suggested behaviours to help improve security.

The guidelines can be accessed on the NCSC website, alongside a blog later in the day (Monday) from key NCSC officials who worked on the product.

A full list of international signatories is below:

- **Australia** – Australian Signals Directorate's Australian Cyber Security Centre (ACSC)
- **Canada** – Canadian Centre for Cyber Security (CCCS)
- **Chile** - Chile's Government CSIRT
- **Czechia** - Czechia's National Cyber and Information Security Agency (NUKIB)
- **Estonia** - Information System Authority of Estonia (RIA) and National Cyber Security Centre of Estonia (NCSC-EE)
- **France** - French Cybersecurity Agency (ANSSI)
- **Germany** - Germany's Federal Office for Information Security (BSI)
- **Israel** - Israeli National Cyber Directorate (INCD)
- **Italy** - Italian National Cybersecurity Agency (ACN)

- **Japan** - Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC; Japan's Secretariat of Science, Technology and Innovation Policy, Cabinet Office
- **New Zealand** - New Zealand National Cyber Security Centre
- **Nigeria** - Nigeria's National Information Technology Development Agency (NITDA)
- **Norway** - Norwegian National Cyber Security Centre (NCSC-NO)
- **Poland** - Poland's NASK National Research Institute (NASK)
- **Republic of Korea** - Republic of Korea National Intelligence Service (NIS)
- **Singapore** - Cyber Security Agency of Singapore (CSA)
- **United Kingdom of Great Britain and Northern Ireland** – National Cyber Security Centre (NCSC)
- **United States of America** – Cybersecurity and Infrastructure Agency (CISA); National Security Agency (NSA; Federal Bureau of Investigations (FBI)

PUBLISHED

27 November 2023

WRITTEN FOR

Small & medium sized organisations

Public sector

Self employed & sole traders

Large organisations

Cyber security professionals

NEWS TYPE

General news