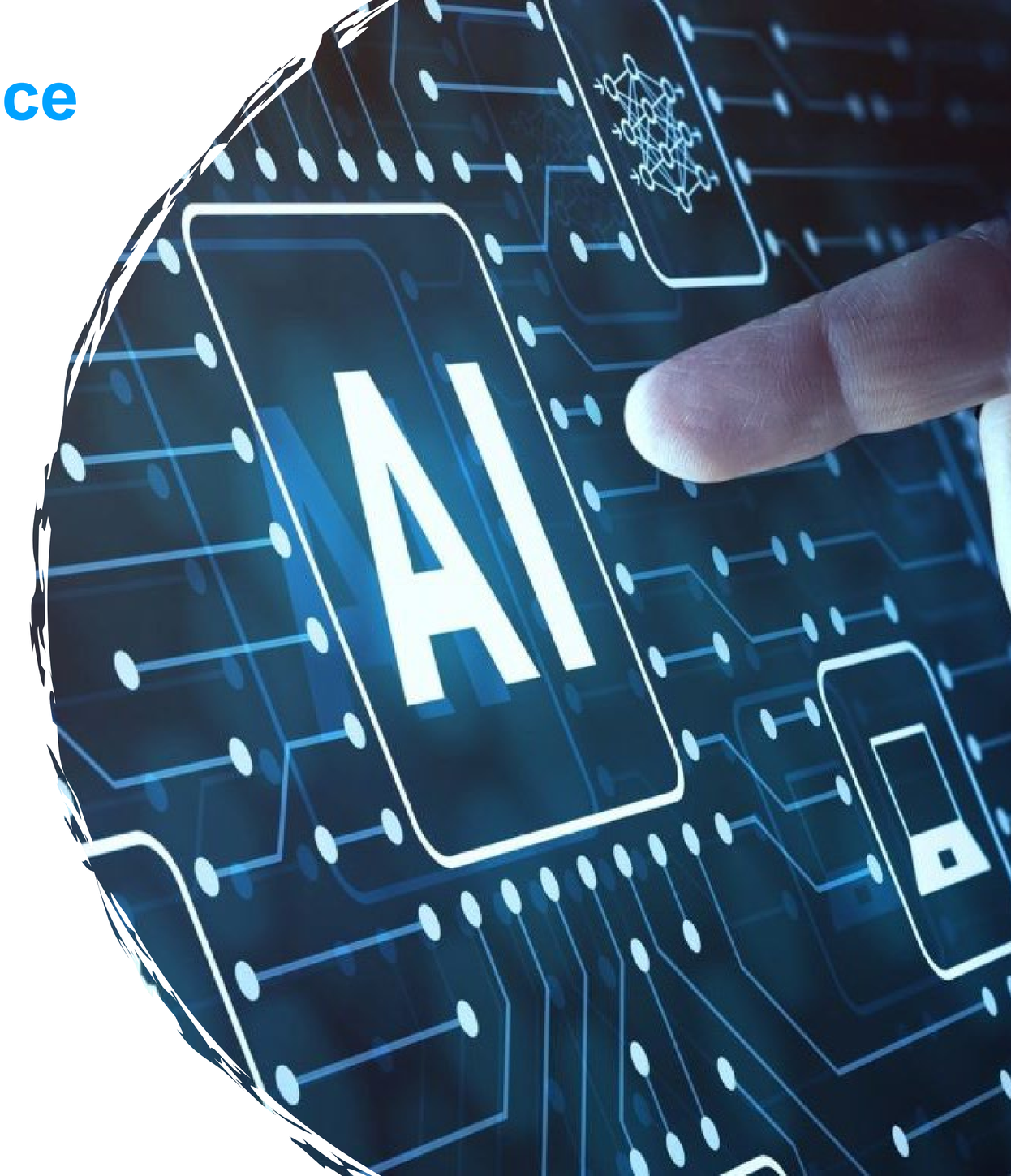
ETSI AI Conference 2024

The UK Government's Approach to the Cyber Security of AI



Presented by: James Deacon, DSIT

Department for Science, Innovation & Technology

5th February 2024

Department for
Science, Innovation
& Technology

Purpose of this presentation

PROVIDE AN OVERVIEW ON OUR POLICY WORK TO DATE ON THE CYBER SECURITY OF AI

OUTLINE OUR APPROACH GOING FORWARD AND OUR OBJECTIVES

SHARE OUR STANDARDS AMBITIONS AND THE POTENTIAL ROLE OF ETSI TC SAI

Background to our work

Department for Science, Innovation & Technology

- National Cyber Strategy to **make AI systems more secure.**
- Cyber security was an important part of the **AI Safety Summit.**
- **NCSC's Secure AI Guidelines** published in November 2023, followed by an NCSC-Assessment on 16 January.
- DSIT compiling a robust **evidence base** including literature reviews, a risk assessment and a business survey.
- Links to DSIT’s broader work on a ‘secure-by-design’ approach to emerging and critical technologies

Department for Science, Innovation & Technology

Objectives

- **Users are protected.**
- **Economy** can securely benefit from AI technologies.
- **International alignment** for security requirements.

Department for
Science, Innovation
& Technology

Scope for our work

- Cyber security risks to **AI models and systems**, rather than the safety and security risks that stem from their use

- All AI technologies

Department for
Science, Innovation
& Technology

Our approach

- Develop a **Code of Practice**, building from the NCSC's Guidelines for Secure AI System Development
- Hold a **Call for Views** on the Code of Practice and use of an international standard
- **Promote international alignment** to encourage cooperation and the use of standards

Department for
Science, Innovation
& Technology

International Standards

National Cyber Strategy ambition to build international support for a secure by design approach.

Standards as an effective lever to encourage adoption of good practices**.**

Multi-stakeholder model supported by industry that can reduce barriers.

International appetite for an aligned approach

Department for Science, Innovation & Technology

Call for Views

- Call for Views should launch in **Spring 2024**
- We welcome views from **all relevant parties**
- The responses will **inform the development** of a Code of Practice and the use of an international standard

Department for
Science, Innovation
& Technology

Contacts

James Deacon

AI standards lead

James.Deacon@dsit.gov.uk

Issy Hall

Emerging technology standards

Issy.Hall@dsit.gov.uk