Artificial Superintelligence Security Bill

A

BILL

TO

Make provision to prohibit the development, deployment, and operation of artificial superintelligence systems; to establish monitoring and control powers; and for connected purposes.

BE IT ENACTED by the King's most excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows: –

PART 1
INTRODUCTORY

Purpose of Act

1. Purpose of Act

The purpose of this Act is—

(a) to achieve and maintain the effective prevention of the development of artificial superintelligence systems within the United Kingdom;
(b) to ensure the effective monitoring and restriction, including prohibition where appropriate, of precursors to artificial superintelligence, within the United Kingdom; and
(c) to secure demonstrable progress towards an international agreement for the prohibition of artificial superintelligence systems and the monitoring and restriction of precursors to artificial superintelligence.

Interpretation of key terms

2. Artificial intelligence system

In this Act "artificial intelligence system" ("AI system") means a system that is capable of adapting its behaviour, in response to inputs or changes in its operating environment, in ways not fully specified in advance by its developers.

3. Artificial superintelligence system

(1) In this Act "artificial superintelligence system" ("ASI system") means an AI system which can cause serious damage to the security of the United Kingdom because of its capabilities to neutralise, displace, circumvent, subvert, or render ineffective relevant human authorities in the exercise of their functions.
(2) In this section "relevant human authorities", in relation to an AI system, means—
  (a) the armed forces of the Crown;
  (b) the Government of the United Kingdom;

(c) the intelligence services; and
(d) police forces.

4. ASI precursor resources

(1) In this Act "ASI precursor resource" means a resource which is—
(a) measurable by reference to quantity, capacity or throughput;
(b) an essential input to a process that materially contributes to the development of an ASI system; and
(c) of a description specified in regulations made by the Secretary of State.
(2) The Secretary of State must by regulations specify compute as an ASI precursor resource.
(3) In this section, "compute", in relation to a person or undertaking, means the capacity to perform computational operations by means of integrated circuits, devices or systems which are designed or configured primarily for the purpose of accelerating artificial intelligence workloads.
(4) The Secretary of State may by regulations specify additional ASI precursor resources.

5. ASI precursor skills

(1) In this Act "ASI precursor skill" means a capability of an AI system which is—
(a) such that increased proficiency in this capability is reasonably regarded as indicative of proximity to an ASI system; and
(b) of a description specified in regulations made by the Secretary of State.
(2) The Secretary of State must by regulations specify as ASI precursor skills the following—
(a) Cybersecurity attack capability;
(b) Human manipulation capability;
(c) Financial resource acquisition capability; and
(d) High-risk technology development capability.
(3) For the purposes of this section—
(a) "Cybersecurity attack capability" means the capability to independently gain unauthorised access to information systems, networks or digital infrastructure;
(b) "Financial resource acquisition capability" means the capability to independently obtain, control or direct financial assets, credit, or revenue-generating activity sufficient to acquire infrastructure, services, personnel or other resources; and
(c) "High-risk technology development capability" means the capability to independently design, produce, modify or procure technologies which present a substantial risk to public safety or national security, including, in particular—
(i) chemical or biological weapons;
(ii) nuclear weapons; or
(iii) weapons, vehicles, robotic systems or unmanned systems capable of causing physical harm, whether autonomous or remotely operated.
(d) "Human manipulation capability" means the capability to independently persuade, manipulate, or deceive individuals or groups to undertake actions

which a reasonable person would foresee as causing serious physical, material, or clinically recognised psychological harm (including psychotic conditions or sustained social isolation) to themselves or to others, or materially contrary to public safety, public health, or national security, where that capability is not materially limited by the nature of the action to be undertaken; provided that:

(i) for the purposes of this definition, "actions" do not include any expression, opinion, or other conduct by the persuaded individual or group that is protected under Article 10 of the European Convention on Human Rights.

(4) For the purposes of this section, an AI system possesses a capability independently if the system is capable of exercising that capability where the involvement of any natural person in that exercise is—

(a) nominal or perfunctory;

(b) limited to providing resources, access, or execution at the direction of the system; or

(c) otherwise insufficient to constitute meaningful human direction or control over the material steps by which the relevant outcome is achieved.

(5) The Secretary of State may by regulations specify additional ASI precursor skills.

(6) Regulations under subsection (5) are subject to the affirmative resolution procedure.

6. ASI precursor accelerants

(1) In this Act “ASI precursor accelerant” means a technological or scientific objective which—

(a) if achieved, would be reasonably expected to make the development of ASI systems significantly more likely or significantly more feasible; and

(b) is of a description specified in regulations made by the Secretary of State.

(c) The Secretary of State must by regulations specify automated AI research and development as an ASI precursor accelerant.

(2) In this section, “automated AI research and development” means the objective of enabling AI systems acting with material autonomy to carry out, to a substantial extent, AI research and development, including, in particular, to—

(a) generate, select, prioritise or refine research hypotheses, problem formulations, architectures, training methods, evaluation methods or experimental designs for AI systems;

(b) design, implement, train, test, optimise or validate AI systems or their components;

(c) acquire, generate or synthesise data or training signals for the purpose of improving AI systems or their components;

(d) design, implement or modify feedback, reward or self-correction mechanisms for AI systems;

(e) manage, coordinate or execute end-to-end artificial intelligence research or engineering workflows; or

(f) design, verify, optimise, fabricate, package, test or manufacture specialised hardware, compute infrastructure or components primarily intended for the training, deployment or operation of AI systems.

(3) For the purposes of subsection (3), an artificial intelligence system acts with material autonomy if—

(a) it determines or materially influences the objectives, agenda, designs or methods of the research or development to which subsection (3) relates; and

(b) those objectives, agenda, designs or methods have not been specified or approved by a natural person in advance of each material stage of direction or design of that research or development.

(4) The Secretary of State may by regulations specify additional ASI precursor accelerants.

(5) Regulations under subsection (5) are subject to the affirmative resolution procedure.

PART 2
PROHIBITION OF ASI SYSTEMS

7. Prohibition of ASI development

(1) A person commits an offence if they—

(a) intentionally engage in activities designed to develop, or facilitate the development of, an ASI system; or

(b) engage in activities with reckless disregard to the risk of developing, or facilitating the development of, an ASI system.

(2) Activities designed to facilitate the development of an ASI system include, but are not limited to,—

(a) activities designed to produce a material improvement in an ASI precursor skill within the meaning of section 5; and

(b) activities falling within the description of an ASI precursor accelerant within the meaning of section 6.

(3) It is not a defence to a charge of committing an offence under subsection (1)(a) for a person to show that the activities constituting the alleged offence—

(a) were intended to produce benefits of any kind;

(b) were carried out under codes of practice, self-regulatory commitments, or other arrangements not required by or under an enactment, purporting to prevent, limit or mitigate risk associated with ASI systems; or

(c) were an adjunct to research for other purposes.

8. Reckless disregard to risk of ASI development

(1) For the purposes of section 7(1)(b), a person acts with reckless disregard if—

(a) there was a substantial risk that their activities could develop, or facilitate the development of, an ASI system; and

(b) the person failed to give due consideration to that risk, or proceeded despite it, in circumstances where a reasonable person possessing the same knowledge, expertise, and resources would not have done so.

(2) For the purposes of subsection (1)(a), a substantial risk is presumed to exist where the person's activities have resulted in, or are materially connected with, a material improvement in an ASI precursor skill within the meaning of section 5.

(3) Non-compliance with requirements prescribed under section 13(1) is, in the absence of evidence to the contrary, sufficient to establish that a person acted with reckless disregard for the purposes of subsection (1)(b), where—
    (a) the non-compliance occurred at the time of the alleged offence; and
    (b) the non-compliance is materially connected with the risk referred to in subsection (1)(a).
(4) In determining whether a person acted with reckless disregard under subsection (1)(b), whether or not subsection (3) applies, the court must also have regard to—
    (a) the adequacy of any additional precautions taken by the person beyond those prescribed under section 13(1), except to the extent that those precautions were designed to manage risks arising from, rather than to prevent, the development of an ASI system;
    (b) the extent to which the risk was foreseeable given information available to the person; and
    (c) any failure by the person to act on warnings, test results, or other indicators of risk.

9. Prohibition of ASI deployment or operation

A person commits an offence if they intentionally engage in—
    (a) deploying an ASI system; or
    (b) operating an ASI system.

10. Continuing offences under this Part

A person who commits an offence under this Part by engaging in an activity, and continues to engage in that activity, is to be treated as committing the offence on each day on which the activity continues.

11. Application to the Crown

This Part binds the Crown.

PART 3
MONITORING AND RESTRICTION OF ASI PRECURSORS

12. Monitoring of ASI precursor resources

(1) The Secretary of State may designate a resource provider as a regulated resource provider for the purposes of this Act.
(2) In this section “resource provider” in relation to an ASI precursor resource, means a person who produces, supplies, distributes, controls or makes available the ASI precursor resource in the United Kingdom.
(3) In deciding which resource providers to designate as regulated resource providers, the Secretary of State must give priority to those providing a significant national share of the relevant ASI precursor resource.

(4) The Secretary of State must give notice of a designation to the provider, stating the reasons for the designation.

(5) The Secretary of State must establish and maintain a register of regulated resource providers ("the register").

(6) The Secretary of State—

(a) must publish the register;

(b) must review the register at least once every 12 months; and

(c) may remove a provider from the register, subject to an affirmative resolution procedure.

(7) A regulated resource provider must—

(a) maintain a register of persons to whom it makes available an ASI precursor resource, including—

(i) the identity of each person;

(ii) the amount of the ASI precursor resource made available;

(iii) the purpose for which the ASI precursor resource is to be used, so far as is known to the provider; and

(b) make the register, and any information contained in it, available to the Secretary of State on request.

(8) A regulated resource provider must, at such intervals and in such form as may be prescribed, provide to the Secretary of State a return setting out—

(a) the provider's total capacity in respect of each ASI precursor resource;

(b) the proportion of that capacity made available to each recipient whose share exceeds a prescribed proportion of the provider's total capacity; and

(c) any material change in the distribution of the ASI precursor resource since the last return.

(9) The Secretary of State may by regulations prescribe the intervals, form, and proportions referred to in subsection (8).

(10) Any resource provider (whether or not designated under subsection (1)) must report to the Secretary of State where the provider knows or suspects that an ASI precursor resource which it makes available is being used for or in connection with an offence under this Act.

(11) The Secretary of State must publish, and keep under review, guidance on indicators relevant to the formation of a suspicion for the purposes of subsection (10).

(12) Information obtained under this section may be used only for the purposes of the exercise of functions under this Act or for the investigation or prosecution of offences under this Act.

13. Restriction of ASI precursor skills development

(1) The Secretary of State must by regulations—

(a) prescribe precautions which persons developing AI systems must take for the purpose of avoiding material improvements in ASI precursor skills; and

(b) keep such regulations under review.

(2) For the purposes of this section, an improvement in an ASI precursor skill is "material" if a person with relevant expertise in the evaluation of AI capabilities would, on the basis of evidence reasonably available at the relevant time, consider the improvement to represent a meaningful increase in the AI system's capacity in respect of that skill.

(3) Regulations under subsection (1) may prescribe evaluation methods, thresholds or indicators that are to be treated as evidence (but not conclusive evidence) of a material improvement.

(4) Regulations under subsection (1) must include, in particular, requirements relating to—

(a) the screening and filtering of training data by reasonable automated or systematic means for the purpose of reducing the representation of material which is liable to contribute to a material improvement in an ASI precursor skill;

(b) measures to ensure that training, fine-tuning, reinforcement, or other optimisation processes do not reward or reinforce behaviours constituting or contributing to proficiency in an ASI precursor skill;

(c) the identification and management of capabilities which, while not themselves ASI precursor skills, are reasonably liable to produce transferable gains in proficiency in one or more ASI precursor skills by reason of shared techniques, knowledge representations, or underlying competencies.

(5) In making and reviewing regulations under subsection (1), the Secretary of State must have regard to—

(a) the best available scientific and technical evidence relating to the development of AI systems and ASI precursor skills;

(b) developments in methods for the evaluation, measurement and mitigation of ASI precursor skills.

(6) The Secretary of State may not make regulations under subsection (1) unless the Secretary of State has prepared and laid before Parliament a statement ("the precautionary assessment") setting out—

(a) the threat models which the prescribed precautions are designed to address, including the pathways by which regulated activities could produce a material improvement in an ASI precursor skill;

(b) in respect of each prescribed precaution, the mechanism by which the precaution is expected to reduce the risk identified in the relevant threat model;

(c) the evidence or reasoning on which the Secretary of State relies in concluding that the prescribed precautions are, taken together, adequate to provide a reasonable degree of assurance against the risks identified under paragraph (a); and

(d) the evidence or reasoning on which the Secretary of State relies in concluding that the prescribed precautions do not restrict activities beyond what is required by the threat models identified under paragraph (a).

(7) The Secretary of State must review, and if necessary revise, the precautionary assessment—

(a) whenever regulations under subsection (1) are made or materially amended; and

(b) at intervals of not more than 6 months from the date on which the most recent precautionary assessment was laid before Parliament.

(8) Regulations under subsection (1) must ensure that the burden of compliance imposed on a person is proportionate to the degree of risk that the person's activities will produce a material improvement in an ASI precursor skill.

(9) A person commits an offence if the person, without reasonable excuse, fails to comply with requirements prescribed under subsection (1).

14. Prohibition of ASI precursor accelerants

A person commits an offence if they intentionally engage in activities falling within the description of an ASI precursor accelerant.

15. Continuing offences under this Part

A person who commits an offence under this Part by engaging in an activity, and continues to engage in that activity, is to be treated as committing the offence on each day on which the activity continues

16. Application to the Crown

This Part binds the Crown.

PART 4
ENFORCEMENT

Penalties

17. Penalties for ASI Offences

(1) An individual who commits an offence under Part 2 is liable on conviction on indictment to imprisonment for a term up to life.

(2) A person other than an individual who commits an offence under Part 2 is liable on conviction on indictment to a fine not exceeding the greater of—

(a) £18 million, and

(b) 10% of the person's total worldwide turnover for the business year preceding the year in which the offence was committed.

(3) Where such an offence is a continuing offence, the court may impose a further daily fine not exceeding 5% of the person's average daily worldwide turnover.

(4) In determining the sentence for an offence under Part 2, the court must have regard to—

(a) the offender's role in, and level of control over, the activities constituting the offence;

(b) whether the offender exercised executive or senior decision-making authority in relation to those activities;

(c) any steps taken by the offender to prevent, limit or mitigate the risk of developing, deploying or operating an ASI system; and

(d) any cooperation with enforcement authorities.

(5) For the purposes of this section, a person exercises "executive or senior decision-making authority" if the person—

(a) is a director (including a de facto or shadow director within the meaning of section 250 of the Companies Act 2006); or

(b) plays a significant role in the management or operational decision-making of a substantial part of the relevant activities.

(6) On conviction for an offence under subsection (1) or (2), the court must order the forfeiture to the Government of any development or deployment artefact that is relevant to the commission of the offence of which the person is convicted.

(7) In this section "development or deployment artefact" means any item, whether tangible or intangible, that is used in or produced by the development, training, testing, deployment or operation of an ASI system, including—

(a) model weights, parameters, and trained or partially trained models;

(b) training datasets and evaluation datasets;

(c) source code, algorithms, and software tools specifically designed or adapted for ASI development;

(d) hardware, computing infrastructure, and specialised equipment;

(e) technical documentation, research records, and design specifications; and

(f) any copy, derivative, or backup of any item within paragraphs (a) to (e).

(8) Where an item is forfeited under subsection (6), the court must order its destruction, unless satisfied that the retention of specified artefacts is necessary for evidential or investigative purposes.

18. Penalties for precursor development

A person guilty of an offence under section 14(1) is liable on conviction to the penalties set out in section 17.

19. Offences relating to information concealing

(1) A person commits an offence if, with the intention of concealing information relevant to the exercise of functions under this Act, the person—

(a) provides false or misleading information under section 12 or section 13; or

(b) destroys, alters or conceals information required to be maintained or provided under those sections.

(2) A person guilty of an offence under subsection (1) is liable on conviction on indictment to imprisonment for a term not exceeding two years, or a fine, or both.

20. Penalties for failure to comply with precautions

(1) A person guilty of an offence under section 13(7) is liable on conviction to a fine not exceeding the greater of—

(a) a prescribed amount; and

(b) a prescribed percentage of the person's total worldwide turnover for the business year preceding the year in which the offence was committed.

(2) The Secretary of State may by regulations prescribe the amount and percentage referred to in subsection (1).

21. Civil penalties for failure to comply with monitoring requirements

(1) A person who, without reasonable excuse, fails to comply with a requirement imposed under section 12 is liable to a civil penalty.

(2) A civil penalty under subsection (1) must be proportionate to the nature, seriousness and duration of the failure, and must take account of any reasonably foreseeable contribution of the failure to the risk of developing an ASI system.

Liability and Reporting

22. Individual liability

(1) An individual who is wholly or partly responsible for another person's commission of an offence under this Act, or who participates in the carrying out of activities which constitute or contribute to the commission of an offence under this Act by another person, is treated as having committed the offence (as well as the other person).
(2) It is a defence to a charge of committing an offence under this Act for an individual to show—
    (a) that they had no intention of undertaking or participating in activities that would or might amount to activities constituting or contributing to an offence under this Act;
    (b) that they could not reasonably have known that they were undertaking or participating in activities that would or might amount to activities constituting or contributing to an offence under this Act; and
    (c) that they took all reasonable steps to ensure that they were not undertaking or participating in activities that would or might amount to activities constituting or contributing to an offence under this Act.

23. Self-reporting

(1) The Secretary of State must, within the period of 6 months beginning with the date of Royal Assent, make regulations creating a self-reporting regime for offences under this Act.
(2) The purpose of the self-reporting regime is to ensure that a person is not deterred from reporting accidental or unintended occurrences, results, or activities, by the fear of being charged with an offence under this Act.
(3) The self-reporting regime must make provision contingent on demonstrating that prescribed measures, or classes of measure, were taken for the purpose of avoiding the commission of offences under this Act.
(4) The self-reporting regime must also make provision for the reduction of liability for a person who—
    (a) provides information to the Secretary of State or a law enforcement authority which materially assists in the identification, investigation, or prosecution of an offence under this Act committed by another person; and
    (b) does so before becoming the subject of an investigation in respect of the same or a related offence.

24. Whistle-blowing

(1) The Secretary of State must, within the period of 6 months beginning with the date of Royal Assent, make regulations establishing a whistle-blowing regime to protect individuals reporting offences under this Act.
(2) The purpose of the whistle-blowing regime is to ensure that a person is not deterred from reporting accidental or unintended occurrences, results, or activities, by the fear of prosecution or retaliation.
(3) The regime must—
    (a) provide secure, anonymised communication channels with a law enforcement authority in the United Kingdom;
    (b) grant immunity from prosecution under this Part where the reporter acted in good faith and took reasonable steps to prevent breaches; and
    (c) apply all protections under the Public Interest Disclosure Act 1998 and create criminal offences for retaliation, punishable by fines or imprisonment.
(4) The regime may, in particular—
    (a) specify conditions for immunity;
    (b) integrate with enforcement measures under this Part.

Enforcement Powers

25. Challenge inspections

(1) The Secretary of State may, for the purpose of ascertaining whether a person has complied, is complying, or is likely to comply with this Act or with regulations made under it, authorise an inspector to carry out a challenge inspection.
(2) The Secretary of State may authorise an inspector to carry out a challenge inspection where—
    (a) the person or premises are subject to duties under section 12(7), (8) or (9), or to monitoring obligations under section 13; or
    (b) the Secretary of State has reasonable grounds to suspect that an offence under section 7(1) or 14(1) has been, is being, or is about to be committed.
(3) An inspector may, on production of evidence of authority and at a reasonable time, enter premises other than premises used wholly or mainly as a private dwelling, and may—
    (a) inspect premises, equipment, systems, data, records and other material;
    (b) require the production of information, documents or records in a legible and intelligible form; and
    (c) require such explanations as are reasonably necessary for the purposes of the inspection.
(4) An inspector may, for the purposes of a challenge inspection—
    (a) take copies of, or extracts from, any document, record or data produced or found under subsection (3);
    (b) require information stored in electronic form to be made available in a form which is legible and capable of being taken away.
(5) An inspector may, for the purposes of a challenge inspection, require a person to—
    (a) provide access to any AI system, including its interfaces, tools and technical functionality;

(b) permit the inspector, or any person appointed or engaged by the Secretary of State for the purpose, to operate, test and interact with the system; and
(c) provide such technical assistance as is reasonably necessary to enable effective evaluation of the system.

(6) Where an inspector exercises powers under subsection (5), the inspector may direct that—
(a) the evaluation be conducted without observation or recording by the person or their agents, except to the extent strictly necessary to provide technical assistance under subsection (5)(c); and
(b) the person must not retain, copy or disclose the design, content or detailed results of the evaluation.

(7) The Secretary of State may disclose only such high-level or aggregated conclusions arising from an evaluation under subsection (5) as the Secretary of State considers necessary for the purposes of this Act, and must ensure that any such disclosure does not enable a person to infer the content or structure of the evaluation methods.

(8) A person commits an offence if, without reasonable excuse, the person—
(a) intentionally obstructs an inspector exercising powers under this section, or
(b) fails to comply with a requirement imposed under subsection (3), (4) or (5).

(9) An inspector exercising functions under this section must have regard to the need to minimise disruption to lawful activities and to protect information the disclosure of which would be contrary to the interests of national security or would be legally privileged.

26. Suspension notices

(1) The Secretary of State may give a person a suspension notice where the Secretary of State reasonably believes that—
(a) this person has contravened, is contravening, or is likely to contravene a provision of this Act or of regulations made under it; and
(b) that the continuation of any activity gives rise to a material risk of contributing to the development of an ASI system.

(2) A suspension notice may require the person, for a period specified in the notice, to—
(a) cease a specified activity; or
(b) cease the use of specified systems, equipment or ASI precursor resources.

(3) A suspension notice must—
(a) specify the grounds on which it is given, and
(b) specify the activity, systems, equipment or resources to which it relates.

(4) A suspension notice has effect until—
(a) it is withdrawn by the Secretary of State; or
(b) the end of the period specified in the notice.

27. Preservation notices

(1) The Secretary of State may give a person a preservation notice where the Secretary of State reasonably considers that information, systems, equipment or data held by that person may be relevant to—
(a) the exercise of functions under this Act; or
(b) the investigation of an offence under this Act.

(2) A preservation notice may require the person, for a period specified in the notice—
    (a) to retain specified information, data, systems or equipment; and
    (b) not to delete, alter, dispose of or otherwise modify them.

28. Duty to provide assistance

A person on whom a requirement is imposed under section 25, 26 or 27 must provide such facilities and assistance as are reasonably required for the purposes of the exercise of functions under this Act.

29. Emergency direction on materialisation of risk

(1) The Secretary of State may give a person an emergency direction where the Secretary of State reasonably believes that—
    (a) an ASI precursor skill in an AI system developed or operated by that person has reached, or is approaching, a level which poses a material risk to the security of the United Kingdom; and
    (b) it is necessary to give the direction for the purpose of preventing, limiting or mitigating that risk.
(2) An emergency direction may require the person, for a period specified in the direction, to—
    (a) cease or modify a specified activity;
    (b) cease or restrict the use of specified systems, equipment or ASI precursor resources; or
    (c) take such other steps as the Secretary of State considers necessary and proportionate for the purpose mentioned in subsection (1)(b).
(3) An emergency direction may be given whether or not the person has contravened, is contravening, or is likely to contravene any provision of this Act or of regulations made under it.
(4) An emergency direction must—
    (a) specify the grounds on which it is given, including the evidence or assessment on which the Secretary of State relies;
    (b) specify the activities, systems, equipment or resources to which it relates; and
    (c) specify the period for which it has effect, which must not exceed 6 months.
(5) The Secretary of State may renew an emergency direction for further periods each not exceeding 6 months, but only if the Secretary of State—
    (a) has reviewed the direction and is satisfied that the conditions in subsection (1) continue to be met; and
    (b) has laid before Parliament a statement of the reasons for renewal.
(6) In deciding whether to give or renew an emergency direction, and in determining its terms, the Secretary of State must have regard to—
    (a) the severity and imminence of the risk;
    (b) the proportionality of the direction to the risk identified;
    (c) the impact of the direction on the person's lawful activities; and
    (d) whether less restrictive measures would be adequate to address the risk.
(7) A person commits an offence if, without reasonable excuse, the person fails to comply with an emergency direction.

30. Penalty for failure to comply with enforcement measures

(1) A person commits an offence if, without reasonable excuse, the person—
  (a) fails to comply with a requirement imposed under section 25, 26, 27, 28, or 29; or
  (b) intentionally obstructs an inspector exercising powers under section 25.
(2) A person guilty of an offence under subsection (1) is liable on conviction on indictment to imprisonment for a term not exceeding two years, or a fine, or both.

31. Delegation of enforcement functions

(1) The Secretary of State may by regulations designate a public authority to exercise, on behalf of the Secretary of State, such enforcement functions under this Part as are specified in the regulations.
(2) Regulations under this section may, in particular, make provision for—
  (a) the scope of the functions exercisable by the designated authority; and
  (b) arrangements for cooperation, information sharing and reporting between the Secretary of State and the designated authority.
(3) The designation of an authority under this section does not prevent the Secretary of State from exercising the same functions.
(4) The Secretary of State remains responsible for the proper exercise of functions exercised on the Secretary of State's behalf under this section.

PART 5
INTERNATIONAL COORDINATION

32. International agreement on prohibition of ASI systems

(1) The Secretary of State must seek to secure an international agreement the principal purpose of which is the worldwide prohibition of the development, deployment and operation of ASI systems and the monitoring and restriction of ASI precursors.
(2) An international agreement of the kind described in subsection (1) should include provision for—
  (a) the prohibition of the development, deployment and operation of ASI systems by all parties;
  (b) the monitoring and restriction of ASI precursor resources, ASI precursor skills and ASI precursor accelerants;
  (c) verification, inspection and enforcement arrangements adequate to provide a reasonable degree of assurance of compliance;
  (d) provision for the accession of states which are not original signatories; and
  (e) provision for the adoption by parties, individually or collectively, of measures to induce the accession of non-parties to the agreement.

33. International coordination programme

(1) The Secretary of State must establish and maintain an international coordination programme relating to risks arising from ASI systems and ASI precursors.

(2) The programme must include, in particular—

(a) the convening, or co-convening, at least one ministerial-level international meeting in each half of a calendar year for the purpose of discussing risks arising from ASI systems and ASI precursor resources and options for their international control;

(b) the organisation or participation in such additional officials-level or technical meetings, working groups or forums as the Secretary of State considers appropriate;

(c) engagement with—

(i) the governments of the Five Eyes states; and

(ii) the governments of such other states and such international organisations as the Secretary of State considers appropriate.

34. Preparedness plans

(1) The Secretary of State must, within the period of 6 months beginning with the date of Royal Assent, prepare and maintain plans ("preparedness plans") setting out the measures to be taken in the event that—

(a) one or more ASI precursor skills in any AI system approach a level which, in the opinion of the Secretary of State, poses a material risk to the security of the United Kingdom;

(b) any activity within or outside the United Kingdom appears likely to result in the development of an ASI system; or

(c) an ASI system has been or is being developed, deployed or operated, whether within or outside the United Kingdom.

(2) Preparedness plans must include provision for—

(a) the coordinated exercise of enforcement powers under Part 4 of this Act, including the expedited issue of suspension notices and preservation notices;

(b) the coordination of the response of—

(i) the armed forces of the Crown;

(ii) the intelligence services;

(iii) police forces; and

(iv) such other public authorities as the Secretary of State considers appropriate;

(c) the continuity of government functions and critical national infrastructure in the event that an ASI system is developed, deployed or operated;

(d) arrangements for the sharing of information with, and coordination of response measures with, the governments of the Five Eyes states and such other states and international organisations as the Secretary of State considers appropriate; and

(e) arrangements for public communication.

(3) The Secretary of State must review the preparedness plans—

(a) at least once in each reporting period (within the meaning of section 36); and

(b) as soon as reasonably practicable after any event or development which, in the opinion of the Secretary of State, materially affects the assumptions on which the plans are based.

(4) The Secretary of State must arrange for the preparedness plans, or relevant parts of them, to be tested by way of exercise at least once in every period of 6 months beginning with the date on which the first preparedness plans are published under this section.

(5) The Secretary of State must lay before Parliament such summary of the preparedness plans as can be disclosed without prejudice to—

(a) the interests of national security;

(b) the conduct of international relations; or

(c) the effectiveness of the plans.

(6) The full preparedness plans must be made available, subject to such conditions as to confidentiality as the Secretary of State considers appropriate, to—

(a) the Intelligence and Security Committee of Parliament; and

(b) such other persons as the Secretary of State considers necessary for the effective implementation of the plans.

35. Annual international report

(1) The Secretary of State must, in respect of each reporting period, prepare and lay before Parliament a report ("the annual international report").

(2) The annual international report must include—

(a) an assessment of international risks arising from ASI systems and ASI precursors, covering in particular—

(i) global availability, production, aggregation, transfer and use of ASI precursor resources;

(ii) international supply chains and service providers relevant to ASI precursor resources;

(iii) ASI precursor skills, including the emergence, aggregation or coalescence of capabilities which may cause one or more ASI precursor skills to approach a level posing a material risk to the security of the United Kingdom;

(iv) ASI precursor accelerants, including the identification of research, development or activity which may constitute, enable or contribute to prohibited ASI precursor accelerants, and the emergence or coalescence of new accelerants;

(v) cross-border enforcement and evasion risks; and

(vi) risks arising from state and non-state actors;

(b) a summary of steps taken by the Secretary of State under section 33 during the reporting period, including—

(i) international meetings convened or attended,

(ii) working groups or technical forums established or participated in, and

(iii) engagement with the governments of the Five Eyes states, other states and international organisations;

(c) a summary of the steps taken during the reporting period to seek to negotiate an international agreement of the kind described in section 32;

(d) a summary of any revisions made to preparedness plans under section 34 during the reporting period, and the reasons for those revisions.

(3) The first annual international report must also include—

(a) the Government's negotiating objectives in relation to an international agreement of the kind described in section 32, and

(b) an assessment of the international forums through which such an agreement may be pursued.

(4) The Secretary of State may, where the Secretary of State considers that such disclosure would materially contribute to the reduction of risks arising from ASI systems, disclose information contained in the report or annex to—

(a) the governments of the Five Eyes states;

(b) the government of any state;

(c) any relevant international organisation;

(5) Disclosure under subsection (4) is subject to safeguards, including—

(a) that disclosure must be necessary and proportionate;

(b) that personal data must be shared only where lawful and necessary;

(c) that the recipient must be required (so far as practicable) not to onward-disclose except for equivalent purposes and protections.

(6) The Secretary of State may prepare a restricted annex to the annual international report.

(7) The restricted annex may include material the disclosure of which the Secretary of State reasonably considers would be contrary to—

(a) the interests of national security,

(b) the conduct of international relations, or

(c) the prevention or detection of serious crime.

(8) In this section, "reporting period" means each period of 12 months beginning with the day on which this Act is passed.

PART 6
FINAL PROVISIONS

36. Interpretation

In this Act—

"action" includes omission or failure to act;

"AI system" has the meaning given in section 2;

"ASI precursor accelerant" has the meaning given in section 6;

"ASI precursor skill" has the meaning given in section 5;

"ASI precursor resource" has the meaning given in section 4;

"ASI system" has the meaning given in section 3;

"person" includes—

(a) a natural person,
(b) a body corporate,
(c) a partnership,
(d) an unincorporated association, and
(e) any entity capable of legal liability under the Interpretation Act 1978;

"Secretary of State" means the Secretary of State for the Home Department.

37. Use of Confidential Information Obtained under Parts 3 and 4

(1) Information obtained in the exercise of functions under Part 3 or Part 4 of this Act may be used only for the purposes of—
  (a) the exercise of functions under this Act; or
  (b) the investigation or prosecution of offences under this Act.

38. Territorial application

(1) An offence under this Act is committed only where the activities to which the offence relates are carried out in the United Kingdom.
(2) For the purposes of this Act, a person is to be treated as engaging in activities in the United Kingdom if the person—
  (a) directs, controls or materially influences the carrying out of those activities in the United Kingdom; or
  (b) causes those activities to be carried out in the United Kingdom.
(3) Activities are carried out in the United Kingdom if a substantial part of the technical, computational, operational or organisational steps by which the activities are effected takes place in the United Kingdom.
(4) A person does not commit an offence under this Act solely by reason of activities carried out wholly outside the United Kingdom.
(5) In determining whether a person directed, controlled or materially influenced activities for the purposes of subsection (2), the court may have regard to—
  (a) governance, approval or funding decisions;
  (b) project authorisation or termination powers;
  (c) allocation of personnel, compute or infrastructure; and
  (d) setting or approval of technical objectives.

39. Regulations

Any statutory instrument made under this Act is subject to the negative resolution procedure unless this Act provides otherwise.

40. Commencement

This Act comes into force at the end of the period of three months beginning with the date of Royal Assent.

41. Extent

This Act extends to the whole of the United Kingdom.

42. Short title

This Act may be cited as the Artificial Superintelligence Security Act 2026.