General Enquiries:
info@Britishdemocracy.co.uk
Membership support:
membership@britishdemocracy.co.uk
www.britishdemocracy.co.uk

National Information Security Act 2025

(Draft prepared for consideration by the British Democratic Alliance)

Contents

National Information Security Act 2025

(Draft prepared for consideration by the British Democratic Alliance)

Part I — Preliminary and General Provisions

1 Short title and commencement

1. This Act may be cited as the *National Information Security Act 2025*.

2. It shall come into force six months after the date of Royal Assent, or on such earlier day as the Secretary of State may by regulations appoint.

3. Different days may be appointed for different provisions.

Explanatory note:
Clause 1 sets the title and allows staged commencement–standard practice enabling preparatory regulations and creation of oversight bodies before the offences take effect.

2 Purpose and scope of the Act

1. The purposes of this Act are–
   (a) to protect the United Kingdom from espionage, foreign interference, sabotage and unauthorised disclosure of official information;
   (b) to regulate the possession, handling, communication and protection of information relevant to the national security interest; and
   (c) to ensure that the exercise of powers for those purposes is lawful, proportionate and subject to democratic oversight.

2. This Act applies to–
   (a) conduct occurring within the United Kingdom; and
   (b) conduct occurring outside the United Kingdom by–
      (i) a British citizen;
      (ii) a person ordinarily resident in the United Kingdom; or
      (iii) a body incorporated under the law of any part of the United Kingdom.

Explanatory note:
Establishes both territorial and extra-territorial reach, matching modern practice in counter-espionage statutes.

3 Interpretation
In this Act, unless the context otherwise requires–

- **"Authorised person"** means any person who has received lawful authority under this Act or any other enactment to access, handle or disclose official information.

- **"Classified information"** means information formally designated under a government security classification scheme.

- **"Foreign entity"** means any government, agency, organisation, or person acting directly or indirectly in the interests of a state or political authority other than the United Kingdom. This shall include any and all proscribed organisations.

- **"National security interest"** means the preservation of the sovereignty, territorial integrity, defence capability, democratic institutions, persons or critical infrastructure of the United Kingdom.

- **“Official information ”** means any information, document, data, or material held by or on behalf of the Crown, a government department, or a person acting under Crown authority.
- **“Public interest disclosure ”** has the meaning given in section 17.
- **“Security classification scheme ”** means any scheme approved by the Cabinet Secretary for designating information as protected or classified.
- **“United Kingdom ”** includes the Channel Islands, the Isle of Man, and British Overseas Territories except where otherwise specified.

Explanatory note:
Provides core definitions. The Act deliberately avoids the term “enemy” and replaces it with neutral, functional language suited to peacetime or hybrid-threat contexts.

4 Repeal and supersession of earlier enactments

1. The following enactments are repealed in their entirety–
   (a) the *Official Secrets Act 1911*;
   (b) the *Official Secrets Act 1989*; and
   (c) the *National Security Act 2023*.
2. All references in any other enactment or instrument to those Acts shall be construed as references to this Act or to regulations made under it.
3. Any prosecution, investigation or proceeding commenced under the repealed Acts may continue as if instituted under the corresponding provisions of this Act, unless a court directs otherwise in the interests of justice.

Explanatory note:
Ensures full consolidation and prevents “partial survival” of earlier legislation–closing the loophole that allows lazy cross-reference drafting.

5 Saving and transitional provisions

1. Any security classification, directive, or lawful authorisation in force immediately before commencement shall continue in effect until replaced under this Act.
2. Codes of practice issued under previous legislation remain in force insofar as they are consistent with this Act.
3. Nothing in this Act affects the operation of the *Freedom of Information Act 2000* or the *Data Protection Act 2018* except where inconsistent with the protection of national security interests.

Explanatory note:
Provides continuity of government operations and clarifies interaction with information-access laws.

6 Extent
This Act extends to–
(a) England and Wales;
(b) Scotland;
(c) Northern Ireland; and
(d) the Channel Islands, the Isle of Man, and British Overseas Territories, subject to such exceptions or adaptations as may be specified by Order in Council.

Part II – Espionage and Related Offences

7 Espionage

1. A person commits the offence of espionage if that person–
   (a) obtains, records, possesses, transmits, communicates, or makes available to any foreign entity, any official, any classified information; and
   (b) does so with intent, or having reasonable cause to believe, that the act is prejudicial to the safety or interests of the United Kingdom.
2. For the purposes of this section, it is immaterial whether the information is obtained directly, indirectly, or through electronic or digital means.
3. It is not necessary for the prosecution to prove that the United Kingdom is at war or that the foreign entity is classified as an “enemy”; it shall be sufficient to prove that the act was prejudicial to the national security interest.
4. A person guilty of an offence under this section is liable–
   (a) on conviction on indictment, to imprisonment for life; or
   (b) on summary conviction, to imprisonment for a term not exceeding thirty six months, or to a fine, or both.

Explanatory note:
This clause replaces s 1 of the 1911 Act and Part 1 of the 2023 Act, removing the obsolete “enemy” test and adapting to modern espionage, including cyber or economic intelligence activity.

8 Preparatory and ancillary acts

1. A person commits an offence if that person–
   (a) collects, makes, or possesses any sketch, plan, model, note, digital record, or data capable of being used for espionage purposes; or
   (b) undertakes surveillance, reconnaissance, or other preparatory conduct likely to facilitate an offence under section 7.
2. An offence under this section is an Indictable offence and punishable–
   (a) on conviction on indictment, by imprisonment for a term not exceeding

twenty-five years;

(b) on summary conviction, by imprisonment for a term not exceeding thirty six months, or a fine, or both.

Explanatory note:
Consolidates preparatory-offence language from s 2 of the 1911 Act and Part 1 of the 2023 Act, covering digital and physical intelligence gathering.

9 Aiding, abetting, and conspiracy

1. A person who–

(a) aids, abets, counsels, procures, conspires with, or otherwise assists another to commit an offence under this Part, or

(b) intentionally enables or facilitates such an offence,

commits an offence and is liable to the same penalty as the principal offender.

2. This includes conduct occurring wholly or partly outside the United Kingdom.

3. A person who-

(a) Becomes aware of such an offence and fails to report it commits an indictable offence and is liable, upon conviction, to a sentence of imprisonment not exceeding 10 years.

(b) Suspects have reasonable grounds to believe that an offence has, or will occur, occur and fails to report it commits a summary offence and shall be liable, upon conviction, to a period of imprisonment not exceeding 12 months, a fine, or both.

Explanatory note:
Re-enacts s 4 of the 1911 Act and ensures parity of punishment for conspirators and facilitators, reflecting modern joint-enterprise principles.

10 Sabotage and interference with defence or critical assets

1. A person commits an offence if, for a purpose prejudicial to the safety or interests of the United Kingdom, that person damages, disables, obstructs, or interferes with–

(a) any armed-forces installation, vehicle, aircraft, vessel, or supply;

(b) any communications, transport, energy, or data-infrastructure system designated as critical to national security; or

(c) any apparatus, computer, or network used, or may be used, for national-security, defence, or emergency purposes.

2. A person guilty of an offence under this section is liable on conviction on indictment to imprisonment for life. The minimum term not less than 30 years.

Explanatory note:
Draws from the 2023 Act provisions on sabotage and critical-infrastructure interference, merging them with the older 1911 “prohibited-place” concept.

11 Unlawful communication and retention of protected information

1. A person who, having lawful access to official or classified information–
   (a) communicates it to a person who is not authorised to receive it;
   (b) retains it when no longer authorised to do so; or
   (c) fails to take reasonable steps to secure or return it,
   commits an offence.

2. It shall be a defence to prove that the communication or retention was–
   (a) expressly authorised; or
   (b) necessary and reasonable in the public interest as defined in section 17.

3. Penalty: on conviction on indictment, imprisonment for a term not exceeding fifteen years.

Explanatory note:
Modernises s 2 of the 1911 Act and s 1 of the 1989 Act (“wrongful communication”), incorporating proportional public-interest protection.

12 Receiving protected information unlawfully

1. A person commits an offence if that person knowingly, or having reasonable grounds to believe, receives or obtains official or classified information disclosed in contravention of section 11.

2. Penalty: on conviction on indictment, imprisonment for a term not exceeding ten years.

Explanatory note:
Replaces s 2(2) of the 1911 Act; creates liability for intentional receipt of unlawfully obtained material, including through digital transfer.

13 Harbouring or concealing offenders

1. A person who knowingly harbours, conceals, or assists any person whom they know, or have reasonable grounds to suspect, has committed or intends to commit an offence under this Part commits an offence.

2. Penalty: imprisonment for a term not exceeding fifteen years.

Reasonable Defence

3. A person shall not be guilty of an offence where they can demonstrate they were in reasonable fear for their life and were unable to communicate with the lawful authorities.

Explanatory note:
Retains s 7 of the 1911 Act, expressed in modern language.

14 Defence of lawful authority

It is a defence for a person charged under this Part to prove that–

(a) the act was carried out under lawful authority, warrant, or directive; or

(b) the person reasonably believed that they were acting under such authority.

Explanatory note:
Standard safeguard ensuring that authorised intelligence and defence operations are not inadvertently criminalised.

15 Evidential presumption

Where a person obtains, communicates, or possesses any classified information relating to defence, intelligence, or critical infrastructure, the conduct shall be presumed to have been prejudicial to the national security interest unless the contrary is proved.

Explanatory note:
Carries forward the evidential presumption from s 1(2) of the 1911 Act, adapted for the broader national-security context.

16 Jurisdiction and trial

1. Offences under this Part may be tried in any part of the United Kingdom regardless of where the act occurred.
2. The consent of the Attorney General is required for a prosecution under this Part, save that arrest and remand may occur prior to such consent.

Explanatory note:
Maintains the procedural safeguard from s 8 of the 1911 Act while clarifying UK-wide jurisdiction.

Part III – Protection and Disclosure of Official Information

17 Unauthorised disclosure of official information

1. A person who, without lawful authority–

(a) discloses or makes available official or classified information to another person who is not authorised to receive it; or

(b) publishes, transmits, or otherwise communicates such information to the public,

commits an offence if the disclosure is likely to cause damage to the national security interest or to the safety of any person.

2. For the purposes of this section, “damage” includes endangering life, impairing defence or intelligence capability, compromising operations, or seriously undermining the United Kingdom’s diplomatic or economic interests.

3. A person guilty of an offence under this section is liable–

(a) on conviction on indictment, to imprisonment for a term not exceeding fifteen years; or

(b) on summary conviction, to imprisonment for a term not exceeding twelve months, or to a fine, or both.

Explanatory note: Re-enacts the core of the 1989 Act ss 1-3, replacing vague “damage to interests” tests with a clear, evidence-based definition of harm.

18 Unauthorised retention, copying, or negligent handling

1. A person who–
(a) retains, copies, or stores any official or classified information when not authorised to do so; or
(b) fails to take reasonable steps to protect such information against unauthorised access, loss, or disclosure,
commits an offence.

2. It is a defence to prove that the act or omission was not negligent and that all reasonable measures were taken to safeguard the information.

3. Penalty: on conviction on indictment, imprisonment for a term not exceeding ten years.

Explanatory note: Combines negligent-handling offences with the 1989 Act’s unauthorised-retention clause, extending it to digital data and removable media.

19 Offences by contractors, consultants, and former Crown servants

1. This section applies to any person who–
(a) is or has been a contractor, consultant, or employee engaged by or on behalf of the Crown; or
(b) has previously held office or employment under the Crown.

2. A person to whom this section applies commits an offence if they disclose, retain, or use official information obtained by virtue of that position otherwise than in accordance with lawful authority.

3. Penalty: imprisonment for a term not exceeding fifteen years.

Explanatory note: Ensures parity of duty between civil servants, contractors, and ex-officials, modernising the 1989 Act s 5.

20 Failure to return or account for official information

1. A person commits an offence if, when required by lawful direction, they fail–
(a) to return or destroy any official or classified material; or
(b) to account for its whereabouts to an authorised person.

2. Penalty: on conviction on indictment, imprisonment for a term not exceeding five years.

Explanatory note: Introduces a discrete offence for non-compliance with retrieval orders, closing a gap in prior legislation.

21 Disclosure prejudicial to defence, security, or international relations

1. A person who communicates or publishes information relating to–

(a) the operations or organisation of the armed forces;

(b) the work of the intelligence or security agencies;

(c) nuclear or other strategic defence capabilities; or

(d) the conduct of international relations or confidential communications with foreign governments,

commits an offence if the disclosure is likely to prejudice the effectiveness, security, or trust essential to those functions.

2. Penalty: on conviction on indictment, imprisonment for a term not exceeding twenty years.

Explanatory note: Consolidates OSA 1989 ss 1-3 and NSA 2023 Part 2, defining specific protected domains.

22 Public-interest and whistleblower defence

1. It is a defence for a person charged under sections 17-21 to prove that–

(a) the disclosure was made in good faith and in the reasonable belief that it exposed serious wrongdoing, corruption, or a grave threat to public safety or the environment; and

(b) the disclosure was made to–

(i) an authorised oversight body established under this Act; or

(ii) a Member of Parliament, judge, or other person designated by regulation as a secure recipient of protected disclosures.

2. Where a disclosure is made directly to the media or public, the defence shall only apply if the accused can demonstrate that–

(a) no authorised body could reasonably have been expected to act on the information in time to prevent the harm; and

(b) the disclosure was proportionate to the wrongdoing revealed.

Explanatory note: Provides a codified whistleblower defence, balancing national-security protection with constitutional accountability.

23 Oversight of protected disclosures

1. The National Security Commissioner established under section 30 shall–

(a) receive and investigate disclosures made under section 22;

(b) determine whether such disclosures fall within the public-interest defence; and

(c) report annually to Parliament on the number, category, and outcome of cases.

2. No civil or criminal liability shall attach to a person who makes a protected disclosure in accordance with this section.

Explanatory note: Institutionalises independent handling of whistleblower cases, ensuring accountability without compromising operations.

24 Prohibition on commercial or personal use of official information

1. A person commits an offence if they use or attempt to use official or classified information for commercial advantage, personal gain, or political influence.

2. Penalty: imprisonment for a term not exceeding twenty years.

Explanatory note: Modern anti-profiteering clause to deter “insider” misuse of government information.

25 Extraterritorial application

1. An offence under this Part committed outside the United Kingdom by a person who–
   (a) is a British citizen or subject; or
   (b) is ordinarily resident in the United Kingdom,
   may be tried as if committed within the United Kingdom.

2. Where the offence is committed by a corporate body incorporated in the United Kingdom, that body shall be liable to prosecution and, upon conviction, to an unlimited fine, seizure of assets, including, but not limited to, shares and the dismissal of all c-suite officials who shall be banned from such positions for a period no less than 10 years.

Explanatory note: Confirms global reach of disclosure offences and introduces corporate liability.

Part IV – Foreign Power Threat Activity

26 Definition of foreign power threat activity

1. For the purposes of this Act, “foreign power threat activity” means any act or omission carried out–
   (a) on behalf of, under the direction of, or with financial or other assistance from, a foreign entity; and
   (b) with intent, or having reasonable cause to believe, that the conduct–
   (i) interferes with, influences, subverts, or prejudices the exercise of functions of the United Kingdom Government, Parliament, judiciary, or democratic institutions; or
   (ii) is otherwise prejudicial to the national security interest.

2. “Foreign entity” has the meaning given in section 3.

3. An activity is “directed by” a foreign entity if the person knew or ought reasonably to have known that the foreign entity had instigated, requested, or encouraged the activity.

Explanatory note:
This clause defines the core concept drawn from the 2023 Act’s “foreign power condition”, expressed in modern language and applicable to hybrid threats, cyber operations, and covert influence.

27 Foreign interference

1. A person commits the offence of foreign interference if they engage in foreign power threat activity which–

(a) seeks to influence elections, referendums, or public appointments;

(b) manipulates or suppresses information with the intent to affect public opinion or policy; or

(c) interferes with the functioning, composition, or independence of political parties, trade unions, universities, or media institutions.

2. A person guilty of an offence under this section is liable on conviction on indictment to imprisonment for a term not exceeding twenty-five years.

Explanatory note:
Condenses multiple interference clauses from the 2023 Act into a single, easily prosecutable offence focused on intentional influence or manipulation of democratic processes.

28 Coercion or intimidation of public officials

1. A person commits an offence if, acting for or with a foreign entity, they directly or indirectly coerce, intimidate, or exert improper pressure on–

(a) a Minister, Member of Parliament, devolved-administration member, judge, or senior civil servant;

(b) a member of the armed forces or police service; or

(c) any person exercising public functions on behalf of the Crown.

2. Penalty: on conviction on indictment, imprisonment for a term not exceeding twenty five years.

Explanatory note:
Targets coercive diplomacy, blackmail, and cyber-harassment of officials–acts that fall short of espionage but threaten state integrity.

29 Funding and material support of influence operations

1. A person commits an offence if they–

(a) provide, receive, or conceal money or other benefit in kind from a foreign entity for the purpose of influencing political, governmental, or academic outcomes in the United Kingdom; or

(b) knowingly arrange or facilitate such funding.

2. An offence under this section shall be indictable and punishable on conviction by imprisonment for a term not exceeding twenty five years.

Explanatory note:
Adapts the foreign-donations and covert-funding offences of the 2023 Act into clearer, corruption-style language.

30 Clandestine or deceptive conduct

1. A person commits an Indictable offence if, on behalf of a foreign entity, they–

(a) use false identities, front organisations, or deceptive digital means to conceal

the foreign origin of any communication or campaign; or

(b) fail to declare a foreign relationship where law or regulation requires disclosure.

2. Penalty on conviction of imprisonment for a term not exceeding fifteen years.

Explanatory note:
Creates a catch-all offence covering covert-propaganda networks, cyber-bots, and undisclosed lobbying.

31 Registration of foreign influence arrangements

1. No person shall undertake, arrange, or assist any activity for the political or governmental interests of a foreign entity unless registered under this section.

2. The Secretary of State shall maintain a public register of foreign-influence arrangements, setting out–

(a) the identity of the foreign entity;

(b) the nature and purpose of the arrangement; and

(c) the persons or organisations acting under it.

3. Failure to register, or providing false or misleading particulars, constitutes an offence punishable by imprisonment for a term not exceeding seven years or a fine, or both.

Explanatory note:
Simplifies the “Foreign Influence Registration Scheme” of the 2023 Act into a transparent, administratively light system.

32 Prohibition on foreign-state lobbying without registration

1. A person commits an offence if they, on behalf of a foreign entity, seek to influence Members of Parliament, peers, or government officials regarding legislation, policy, or procurement without a valid registration under section 31.

2. Penalty: imprisonment for a term not exceeding fifteen years.

Explanatory note:
Creates a direct enforcement link between registration and lobbying–closing the practical loophole that undermined prior schemes.

33 Reporting and oversight

1. The National Security Commissioner shall–

(a) oversee the administration of sections 31 and 32;

(b) issue guidance on compliance and exemptions; and

(c) report annually to Parliament on registered entities and enforcement actions.

2. The Commissioner may, by notice, exempt categories of activity deemed low-risk to national security, subject to affirmative resolution by Parliament.

Explanatory note:
Introduces independent oversight of registration and reporting to maintain political neutrality.

34 Penalties and ancillary powers

1. In addition to any term of imprisonment imposed under this Part, a court may order–

(a) confiscation of any benefit or asset proven, or reasonably shown to have been obtained, through the commission of an offence;

(b) disqualification from holding public office or acting as a company director for a period not exceeding ten years; and

(c) deportation of a non-British offender following conviction, subject to human-rights safeguards.

2. The Secretary of State may by regulations prescribe further sanctions, including exclusion from public-procurement contracts, against persons or organisations convicted of offences under this Part.

Explanatory note:
Adds civil-penalty tools and asset-recovery powers to reinforce deterrence.

Part V – Cybersecurity and Information Integrity

35 Unauthorised access to protected systems

1. A person commits an offence if that person–

(a) knowingly or recklessly gains access to, or enables another to access, any computer, network, or data system designated as protected under this Act; and

(b) does so with intent, or having reasonable cause to believe, that the access is prejudicial to the national security interest.

2. It is immaterial whether the access is temporary, partial, or achieved by automated or remote means.

3. Penalty: on conviction on indictment, imprisonment for a term not exceeding twenty-five years.

Explanatory note:
Modernises core hacking provisions to cover all digital intrusion into national-security or critical-infrastructure systems.

36 Cyber-espionage

1. A person commits the offence of cyber-espionage if, for or on behalf of a foreign entity, they–

(a) obtain, copy, or transmit data from a protected system;

(b) intercept electronic communications of the Crown, defence contractors, or critical-infrastructure providers; or

(c) deploy, install, or facilitate malware or spyware for such purposes.

2. Penalty: imprisonment for life.

Explanatory note:
Integrates espionage and cyber-offence provisions to ensure parity between physical and digital intelligence gathering.

37 Interference with data integrity or availability

1. A person commits an offence if, for a purpose prejudicial to the safety or interests of the United Kingdom, that person–

(a) alters, deletes, encrypts, corrupts, or withholds data held in any system critical to national security, defence, emergency response, or essential services; or

(b) impairs the operation of such a system through denial-of-service, overload, or similar means.

2. Penalty: on conviction on indictment, imprisonment for a term not exceeding thirty years.

Explanatory note:
Expands sabotage concepts into the digital sphere, criminalising destructive cyber operations.

38 Manipulation of digital or AI systems

1. A person commits an offence if they intentionally or recklessly interfere with the training data, parameters, or outputs of an artificial-intelligence or automated-decision system used for–

(a) defence, intelligence, law enforcement, or emergency management; or

(b) the administration of public elections or democratic processes,

with intent to cause damage, disruption, or misinformation prejudicial to national security.

2. Penalty: imprisonment for a term not less than twenty years.

Explanatory note:
Introduces explicit protection of AI and automated-decision systems–a forward-looking addition beyond current UK legislation.

39 Duty of cybersecurity cooperation

1. Every government department, contractor, or critical-infrastructure operator shall–

(a) implement and maintain security measures proportionate to the classification of systems under its control;

(b) report significant cyber incidents to the National Cyber Security Centre and the National Security Commissioner within seventy-two hours; and

(c) cooperate with authorised investigators under this Act.

2. Failure without reasonable excuse to comply with subsection (1) constitutes an offence punishable by–

(a) on conviction on indictment, a fine without limit; or

(b) in the case of a responsible officer, imprisonment for a term not exceeding five years.

Explanatory note:
Creates a statutory security-duty framework binding both public and private operators of critical systems.

40 Corporate and individual liability

1. Where an offence under sections 35 to 39 is committed by a body corporate, any director, manager, or officer who consented to or connived in the offence is guilty of the same offence.

2. A court may, in addition to other penalties, order–
   (a) confiscation of any profits or assets derived from the offence;
   (b) temporary or permanent exclusion from government contracts; and
   (c) mandatory cybersecurity audits at the offender's expense.

Explanatory note:
Ensures executive accountability and introduces meaningful corporate sanctions.

41 Disclosure of vulnerabilities

1. A person who, in good faith, discovers and responsibly reports a cybersecurity vulnerability to the relevant authority shall not be guilty of an offence under this Part.

2. The Secretary of State shall by regulation establish a public-interest reporting process for such disclosures.

Explanatory note:
Provides safe-harbour protection for ethical security researchers, balancing enforcement with innovation and public benefit.

42 Jurisdiction and extraterritoriality

1. This Part applies to any act done–
   (a) within the United Kingdom; or
   (b) outside the United Kingdom by a British citizen, UK-incorporated body, or person acting against UK systems.

2. A person may be tried for an offence under this Part in any part of the United Kingdom irrespective of the place of commission.

3. Where the person acts contrary to the interests of the United outside the jurisdiction of the United Kingdom, they may be tried in their absence. An arrest warrant shall be issued as per the Extradition Act 2003 or the Extradition (Provisional Arrest) Act 2020.

4. Where an organisation is not incorporated, or otherwise present, in the UK it shall be tried in its absence and upon conviction, forever banned from operating upon any territory under UK Jurisdiction. Any and all officers of that organisation shall be issued an arrest warrant as per the Extradition Act 2003 or the Extradition (Provisional Arrest) Act 2020.

Explanatory note:
Confirms global jurisdiction to meet the realities of transnational cyber operations.

Part VI – Oversight, Authorisation, and Accountability

43 Establishment of the National Security Commissioner

1. There shall be an independent officer known as the *National Security Commissioner* (“the Commissioner”).

2. The Commissioner shall be appointed by His Majesty on the recommendation of the Defence Select Committee, the Director General of MI5, the Chief of the Secret Intelligence Service and the Chief of the Defence Staff, following an open selection process and subject to confirmation by a two-thirds majority of a Joint Committee of Parliament.

3. The Commissioner shall hold office for a single, non-renewable term of seven years and may be removed only for incapacity or serious misconduct by resolution of both Houses of Parliament.

4. The Commissioner shall be independent of the Government and shall not, in the exercise of their functions, be subject to the direction or control of any Minister of the Crown.

5. The Commissioner should have sufficient knowledge and experience of intelligence matters that they can adequately perform their duties. They should have at least 15 years’ experience in senior management within the Defence Intelligence infrastructure or senior military roles.

Explanatory note:
Creates a constitutionally independent oversight authority with guaranteed parliamentary rather than ministerial accountability.

44 Functions of the Commissioner

1. The functions of the Commissioner are–
(a) to oversee compliance with this Act by all public authorities and persons acting under Crown authority;
(b) to initiate and monitor prosecutions and investigations under this Act and certify that they are not politically motivated;
(c) to receive and investigate public-interest disclosures under section 23;
(d) to audit the use of classified information and cybersecurity duties under Part V; and
(e) to report annually to Parliament on the exercise of these functions.

2. The Commissioner may conduct thematic reviews and issue guidance on the interpretation or application of this Act, subject to approval by a Joint Committee of Parliament.

3. The Commissioner may, where urgent, issue interim directions to suspend or amend any activity suspected of breaching this Act. This may include the removal of the security clearance of any individual, including, and not limited to, any government minister or the Prime Minister.

Explanatory note:
Defines broad investigative and advisory powers, integrating roles formerly split between several commissioners and reviewers.

45 Access to information

1. The Commissioner shall have unrestricted access to–
(a) any document, record, or system held by a government department or intelligence agency relevant to the performance of their functions; and
(b) any person employed or contracted by the Crown, who may be required to give evidence or provide assistance.

2. It shall be an offence to–
(a) knowingly obstruct the Commissioner; or
(b) withhold or falsify information requested under subsection (1).

3. Penalty: imprisonment for a term not exceeding twenty five years.

Explanatory note:
Guarantees investigatory independence and criminalises obstruction, ensuring oversight has real authority.

46 Special and classified reports

1. Where disclosure of material in a report would prejudice ongoing operations or national security, the Commissioner shall prepare–
(a) a full classified report for the Prime Minister and the Intelligence and Security Committee of Parliament; and
(b) a redacted public version for general publication.

2. The Prime Minister shall lay the public report before Parliament within thirty sitting days of receipt.

Explanatory note:
Balances transparency with operational security through a dual-reporting mechanism.

47 Judicial review of prosecutorial decisions

1. Any decision by the Director of Public Prosecutions, the Attorney General, or the Advocate General for Scotland to authorise, refuse, or discontinue a prosecution under this Act shall be required to undergo judicial review before the High Court (or Court of Session in Scotland).

2. The court may, if satisfied that the decision was irrational, politically influenced, or otherwise unlawful, quash the decision and/or direct that any prosecution be terminated or reconsidered.

3. Applications under this section shall be heard by a specially designated panel of not less than 5 judges with security clearance for classified material.

Explanatory note:
Provides a statutory mechanism to prevent political suppression or manipulation of national-security prosecutions.

48 Warrants and lawful authorisation

1. Any act that would otherwise constitute an offence under this Act shall be lawful if done under–

(a) a warrant or written authorisation issued by the Secretary of State; and

(b) subsequent review and certification by the Commissioner within fourteen days.

2. The Commissioner shall maintain a secure register of all such authorisations, accessible to the Intelligence and Security Committee.

3. A warrant or authorisation not certified under subsection (1)(b) shall cease to have effect after fourteen days.

Explanatory note:
Creates a dual-key authorisation model ensuring both ministerial and independent approval for covert operations.

49 Protection of intelligence officers and whistleblowers

1. No criminal or civil liability shall attach to any person acting in good faith under a certified warrant or authorisation issued under this Act.

2. A person who makes a protected disclosure in accordance with sections 22 and 23 shall not be subject to disciplinary action or detriment for doing so.

3. Any person who retaliates against a protected discloser commits an offence punishable by imprisonment for a term not exceeding five years.

Explanatory note:
Codifies immunity for lawful operations and anti-reprisal protections for whistleblowers.

50 Parliamentary oversight

1. The Intelligence and Security Committee of Parliament shall, in addition to its existing functions–

(a) review the operation and effectiveness of this Act at least once every three years;

(b) receive classified reports from the Commissioner; and

(c) make recommendations to Parliament on legislative amendments or improvements.

2. The Committee shall have power to summon witnesses and require documents relevant to its review, subject to national-security safeguards approved by the Commissioner.

Explanatory note:
Formalises parliamentary review and strengthens democratic control over security legislation.

51 Annual transparency report

1. The Secretary of State shall, after consultation with the Commissioner, lay before Parliament an annual report setting out–

(a) the number and category of offences prosecuted under this Act;

(b) the number of warrants or authorisations issued;

(c) statistics on protected disclosures and oversight findings; and

(d) such other information as may be necessary for public confidence, subject to lawful redaction.

2. Failure to publish the report within 28 sitting days of the end of each reporting year shall require an explanatory statement to be made to both Houses of Parliament. In any event, the report must be published no later than 60 days from issue.

Explanatory note:
Ensures continuous public accountability and provides measurable data on the Act's application.

52 Independent review and sunset provision

1. This Act shall be subject to independent statutory review every ten years by a commission appointed jointly by the Prime Minister and the Leader of the Opposition, in consultation with the Commissioner.

2. The commission shall examine–

(a) the continuing necessity and proportionality of each Part of the Act; and

(b) whether any provisions should be repealed, amended, or replaced.

(c) no provisions may be repealed, amended or replaced without Judicial review.

3. Unless renewed by affirmative resolution of both Houses of Parliament, this Act shall expire fifteen years after Royal Assent.

Explanatory note:
Builds in democratic renewal and prevents permanent entrenchment of extraordinary powers.

Part VII – Evidence, Procedure, and Sentencing

53 Admissibility of classified evidence

1. Classified or sensitive material shall be admissible in proceedings under this Act, subject to the safeguards set out in this Part.

2. The court shall ensure that–

(a) disclosure of such material does not compromise ongoing operations, sources, or methods; and

(b) the accused receives a fair trial consistent with Article 6 of the European Convention on Human Rights.

3. Where disclosure would endanger national security, the court may order alternative arrangements including–

(a) summaries or redacted versions of evidence;

(b) agreed statements of fact; or

(c) examination of material in camera by security-cleared special advocates.

Explanatory note: Formalises admissibility of sensitive evidence while embedding fair-trial guarantees, replacing ad-hoc Public Interest Immunity procedures.

54 Closed material proceedings

1. The Attorney General or the Director of Public Prosecutions may apply to the High Court for a declaration that a case under this Act should include closed material proceedings.
2. If such a declaration is granted, the court shall appoint one or more special advocates to represent the interests of the defendant during any closed session.
3. A transcript of all closed proceedings shall be retained under secure seal by order of the presiding judge for not less than thirty years.

Explanatory note: Introduces a permanent statutory framework for handling secret evidence, consistent with modern national-security jurisprudence.

55 Protective orders and witness anonymity

1. Where the court is satisfied that disclosure of a witness's identity would endanger life or national security, it may order that–
   (a) the witness give evidence under a pseudonym or from a secure location;
   (b) identifying details be withheld from publication; and
   (c) proceedings be conducted wholly or partly in camera.
2. Contravention of an anonymity or publication order constitutes contempt of court.

Explanatory note: Protects informants, undercover officers, and intelligence witnesses, while giving courts explicit statutory powers.

56 Interception and surveillance evidence

1. Evidence obtained under a lawful warrant or authorisation issued pursuant to section 48 or any other enactment shall be admissible notwithstanding its origin from interception or surveillance activities.
2. The court shall determine admissibility based on reliability and relevance, not on the manner in which the evidence was lawfully obtained.

Explanatory note: Clarifies that authorised intelligence material may be used in court, aligning evidential rules with security practice.

57 Burden and standard of proof

1. Except where expressly provided otherwise, the prosecution bears the burden of proving each element of an offence under this Act beyond reasonable doubt.
2. Where this Act creates an evidential presumption (including section 15), the defendant bears an evidential, not legal, burden to adduce sufficient evidence to raise reasonable doubt.

Explanatory note: Re-states fundamental criminal-law principles to avoid misinterpretation of reverse-onus provisions.

58 Sentencing principles

1. In determining sentence for an offence under this Act, the court shall have regard to–

(a) the gravity and duration of the conduct;

(b) the extent of actual or potential harm to national security;

(c) any abuse of official position or trust;

(d) cooperation with investigators or voluntary disclosure; and

(e) deterrence and protection of the public interest.

2. A court may impose consecutive sentences for separate offences arising from distinct acts or transactions.

3. Life imprisonment shall be reserved for offences involving espionage, sabotage, or cyber-espionage causing or intended to cause severe damage to the United Kingdom's security or vital interests.

Explanatory note: Establishes statutory sentencing guidance consistent across all offences within the Act.

59 Forfeiture and confiscation of assets

1. Where a person is convicted of an offence under this Act, the court may order the forfeiture of–

(a) any money, asset, or benefit obtained as a result of the offence; and

(b) any equipment, data, or document used in its commission.

2. Forfeited assets shall vest in the Crown and may be applied to the Victims and Security Assistance Fund established by regulation.

Explanatory note: Unifies proceeds-of-crime provisions for espionage and cyber-offences, funding victim and resilience programmes.

60 Restitution and compensation

1. Where an offence under this Act has caused loss or damage to a public authority, corporate body, or individual, the court may order the offender to pay compensation in addition to any other penalty.

2. Compensation orders may be enforced as civil judgments.

Explanatory note: Ensures restitution for material harm caused by national-security breaches.

61 Deportation and exclusion orders

1. Where a person who is not a British citizen is convicted under this Act, the Secretary of State may, after considering any human-rights obligations, order that person's deportation or exclusion from the United Kingdom.

2. Such an order may include permanent exclusion from re-entry unless revoked by the Secretary of State with the concurrence of the Commissioner.

Explanatory note: Provides a statutory basis for removal of hostile-state actors following conviction, subject to due-process safeguards.

62 Civil proceedings and injunctions

1. Where it appears to the Attorney General or the Commissioner that any conduct constitutes, or is likely to constitute, an offence under this Act, they may apply to the High Court for an injunction restraining such conduct.
2. The court may grant interim or permanent relief notwithstanding the absence of criminal proceedings.

Explanatory note: Allows preventive civil remedies against imminent security breaches.

63 Appeals

1. A person convicted under this Act may appeal–
   (a) against conviction, to the Court of Appeal; or
   (b) against sentence, on the ground that it is excessive or wrong in law.
2. Appeals involving classified material shall be heard in closed session insofar as necessary to protect national security, under procedures approved by the Lord Chief Justice.

Explanatory note: Maintains standard appellate rights while preserving secrecy where required.

64 Procedural rules

1. The Lord Chief Justice, with the concurrence of the Commissioner, may make rules of court for the procedure and practice to be followed in proceedings under this Act.
2. Rules made under this section shall be laid before Parliament and subject to the affirmative resolution procedure.

Explanatory note: Empowers judiciary and oversight to co-author binding procedural regulations, ensuring flexibility and accountability.

Part VIII – Miscellaneous and Supplementary

65 Power to make regulations

1. The Secretary of State may make such regulations as appear necessary or expedient for the purpose of carrying this Act into effect.
2. Regulations under this Act may, in particular–
   (a) prescribe procedures for the classification and declassification of official information;
   (b) establish the Victims and Security Assistance Fund referred to in section 59(2);
   (c) specify categories of foreign-influence arrangements exempt from registration under section 33(2);
   (d) set technical standards for cybersecurity compliance under section 39; and
   (e) make provision for the secure storage, transmission, and destruction of classified material.
3. Regulations under this section–
   (a) shall be made by statutory instrument; and

(b) shall not come into force until approved by resolution of both Houses of Parliament.

Explanatory note:
Creates flexible delegated powers for secondary legislation but restricts them to affirmative parliamentary scrutiny to prevent abuse.

66 Codes of practice

1. The Commissioner may, after consultation with the Secretary of State and the Intelligence and Security Committee of Parliament, prepare and issue codes of practice for the purpose of–
(a) guidance on the handling of official information and classified data;
(b) the conduct of investigations and prosecutions under this Act;
(c) procedures for receiving protected disclosures; and
(d) interaction between public authorities and private contractors in matters of national security.
2. Codes of practice issued under this section–
(a) shall be laid before Parliament; and
(b) shall come into effect on such date as the Commissioner may specify by order.
3. Failure to comply with a code of practice shall not of itself render a person liable to criminal or civil proceedings, but any such code shall be admissible in evidence and may be taken into account by any court or tribunal.

Explanatory note:
Allows the Commissioner to issue detailed professional guidance, ensuring consistent standards across departments and industries.

67 Protection of personal data and privacy

1. Nothing in this Act shall be construed as authorising any conduct contrary to the *Data Protection Act 2018* or the *Human Rights Act 1998*, except where expressly provided by warrant or authorisation under section 48.
2. All processing of information under this Act shall comply with the principles of necessity and proportionality.

Explanatory note:
Affirms compatibility with existing privacy and data-protection frameworks, preventing misuse of national-security powers.

68 Interaction with other enactments

1. In the event of inconsistency between this Act and any other enactment relating to official information, espionage, or national security, the provisions of this Act shall prevail.
2. References in any enactment, instrument, or contract to–
(a) the *Official Secrets Act 1911*;
(b) the *Official Secrets Act 1989*; or
(c) the *National Security Act 2023*,
shall be construed as references to this Act.

Explanatory note:
Legally establishes NISA as the primary, overriding statute in the field of national security and official information.

69 Power to amend consequential provisions

1. The Secretary of State may by regulations make such consequential, incidental, or transitional provision as appears necessary in consequence of this Act.
2. Regulations made under this section may amend, repeal, or revoke any enactment (including this Act), but only for the purpose of maintaining consistency with its provisions.
3. Regulations under this section are subject to the affirmative resolution procedure.

Explanatory note:
Provides a limited Henry VIII power to align existing legislation with this Act while keeping parliamentary oversight intact.

70 Crown application

1. This Act binds the Crown.
2. Nothing in this Act renders the Crown criminally liable, but the High Court may, on the application of the Commissioner or the Attorney General, declare unlawful any act of a Crown servant contrary to its provisions.

Explanatory note:
Ensures the Crown and its servants are legally bound by the Act, while maintaining constitutional limits on criminal liability of the sovereign.

71 Expenses

Any expenditure incurred by a Minister of the Crown in consequence of this Act, and any increase attributable to this Act in sums payable out of money provided by Parliament, shall be paid out of such money.

Explanatory note:
Standard financial authority clause enabling Treasury allocation for enforcement, oversight, and operational costs.

72 Transitional and saving provisions

1. All security clearances, protective markings, and lawful authorisations in force immediately before the commencement of this Act shall continue as if made under this Act until replaced, revoked, or expired.
2. Any investigation, prosecution, or proceeding commenced under the repealed Acts may continue as if instituted under the corresponding provisions of this Act.

Explanatory note:
Ensures legal continuity across repeal of the 1911, 1989, and 2023 Acts.

73 Review and reporting obligations

1. Within three years of this Act's commencement, the Commissioner shall conduct a review of its operation and report to Parliament with recommendations for improvement.
2. Subsequent reviews shall occur at ten-year intervals in accordance with section 52.

Explanatory note:
Establishes an early-stage operational review to identify implementation challenges before the decennial statutory review.

74 Repeals and consequential amendments

1. The enactments specified in Schedule 1 are repealed to the extent stated.
2. The enactments specified in Schedule 2 are amended as set out therein.
3. Schedules 1 and 2 shall have effect from the commencement of this Act.

Explanatory note:
Formal repeal and amendment clause referencing attached schedules.

75 Extent

This Act extends to–

(a) England and Wales;

(b) Scotland;

(c) Northern Ireland; and

(d) the Channel Islands, the Isle of Man, and British Overseas Territories, subject to such exceptions or modifications as may be made by Order in Council.

Explanatory note:
Ensures comprehensive territorial coverage with flexibility for local adaptation.

76 Commencement

1. This Act shall come into force six months after Royal Assent, or on such earlier day as may be appointed by the Secretary of State by regulations.
2. Different days may be appointed for different provisions.

Explanatory note:
Allows staged implementation to accommodate organisational and technical preparations.

77 Short title

This Act may be cited as the *National Information Security Act 2025*.

Explanatory note:
Concluding clause confirming the official short title for all legal and parliamentary references.

Part IX – Local Government and Public Authorities

78 Application to local government and devolved authorities

1. This Act applies to–
   (a) all principal councils and combined authorities in England;
   (b) the Welsh Government and local authorities in Wales;
   (c) the Scottish Government, Scottish local authorities, and public bodies established under the *Local Government etc. (Scotland) Act 1994*; and
   (d) Northern Ireland departments, district councils, and public bodies established under the *Local Government Act (Northern Ireland) 2014*.

2. For the purposes of this Part, "local authority" includes any body corporate exercising public administrative, regulatory, or service-delivery functions funded wholly or partly by public money.

Explanatory note:
Explicitly extends the Act's coverage beyond central government to the devolved administrations and local authorities.

79 Security obligations of local authorities

1. Each local authority shall–
   (a) implement and maintain appropriate physical, procedural, and digital safeguards to protect official information and computer systems under its control;
   (b) appoint a *Designated Information Security Officer* responsible for compliance with this Act;
   (c) report all breaches of security, loss of data, or cyber-incidents affecting official information to the National Cyber Security Centre and the Commissioner within seventy-two hours; and
   (d) ensure that employees and contractors receive training on their obligations under this Act.

2. Failure to comply with subsection (1) constitutes an offence punishable–
   (a) on conviction on indictment, by a fine without limit; or
   (b) on summary conviction, by a fine not exceeding level 5 on the standard scale.

Explanatory note:
Creates a statutory security framework for local government, mirroring the duties imposed on central government under Part V.

80 Application to employees and contractors of local authorities

1. Any employee, contractor, or elected member of a local authority who has access to official or classified information shall be subject to the same duties, restrictions, and penalties as a Crown servant under this Act.
2. Where a local authority engages a contractor for information-technology or administrative services, the contract shall expressly incorporate obligations consistent with this Act.

Explanatory note:
Eliminates ambiguity over the liability of local-government employees and contractors handling sensitive data.

81 Oversight and coordination

1. The Commissioner shall maintain a register of compliance audits for all local authorities and may issue directions or recommendations to remedy deficiencies.
2. The Secretary of State, after consultation with the devolved administrations, may issue a Code of Practice on local-authority information security, subject to parliamentary approval.

Explanatory note:
Ensures uniform national oversight and coordination while respecting devolved-government competence.

Part X – Declared National Emergencies and Times of War

82 Declaration of national emergency or war

1. Where–
   (a) a state of war exists involving the United Kingdom; or
   (b) His Majesty, on the advice of the Prime Minister, declares by Order in Council that a *national emergency* exists which threatens the life of the nation or the integrity of its defence or civil-protection systems,
   the provisions of this Part shall apply for the duration of that declaration.

2. Any such Order in Council–
   (a) shall specify the reasons for the declaration;
   (b) shall be laid before Parliament forthwith; and
   (c) shall lapse after sixty days unless renewed by affirmative resolution of both Houses of Parliament.

Explanatory note:
Creates a lawful and time-limited mechanism for invoking emergency powers, ensuring parliamentary control.

83 Modified powers during emergencies

1. During a declared national emergency or time of war, the following modifications shall apply–
   (a) the requirement for prior judicial or Commissioner certification under section 48 may be suspended for up to fourteen days, provided that retrospective certification is obtained thereafter;
   (b) authorised persons may intercept communications, access data, or seize material where immediate action is necessary to prevent serious damage to national security or the lives of UK citizens; and
   (c) the Secretary of State may issue interim directives to safeguard critical national infrastructure or communication systems without prior parliamentary approval, subject to review under section 84.

2. All actions taken under this section shall be recorded in writing and reported to the Commissioner within seventy-two hours.

3. Any and all sentences upon conviction for any offence in this act committed at a time of declared national emergency or declared war shall be doubled where it can be reasonably demonstrated they harmed the national interests of the United Kingdom, an ally state or the lives of citizens of the United Kingdom or an ally.

Explanatory note:
Allows temporary operational flexibility under oversight and time limits to ensure rapid response while retaining accountability.

84 Oversight and post-event review

1. The Commissioner shall conduct a special review within six months of the termination of any declaration made under section 82, examining–
(a) all warrants, directives, and authorisations issued under emergency powers;
(b) compliance with statutory safeguards; and
(c) any instances of misuse or disproportionate action.
2. The Commissioner shall submit a report of the review to the Intelligence and Security Committee and lay a redacted version before Parliament.

Explanatory note:
Mandates retrospective scrutiny of all emergency actions to prevent abuse and ensure democratic transparency.

85 Protection of operational information in conflict zones

1. It shall be an offence, during a time of war or declared national emergency, to disclose without lawful authority any information relating to–
(a) the disposition, movement, or readiness of UK or allied forces;
(b) the identity of operational personnel; or
(c) military, intelligence, or humanitarian operations conducted abroad,
where such disclosure could reasonably be expected to cause significant damage to the United Kingdom's civil or military interests.

2. Penalty: imprisonment for life or for such lesser term as the court may determine.

Explanatory note:
Extends protection to sensitive operational information from foreign theatres, replacing outdated "enemy" concepts with modern security language.

86 Expiry of emergency powers

1. All powers conferred by this Part shall cease–
(a) upon revocation or expiry of the declaration made under section 82; or
(b) automatically twelve months after the declaration unless renewed by Act of Parliament.
2. No renewal may extend such powers beyond three consecutive years without fresh primary legislation.

Explanatory note:
Builds in automatic expiry and renewal safeguards to prevent indefinite emergency powers.

Schedule 1 – Repeals

Would formally list every section, subsection, and schedule of the **Official Secrets Acts 1911 and 1989** and the **National Security Act 2023** that are repealed, for example:

Enactment	**Extent of Repeal**
Official Secrets Act 1911 (1 & 2 Geo. 5 c. 28)	The whole Act
Official Secrets Act 1989 (c. 6)	The whole Act
National Security Act 2023 (c. 29)	The whole Act
Any subordinate legislation made under those Acts	To the extent inconsistent with this Act

Schedule 2 – Consequential Amendments

Would set out the technical edits to other laws that still reference the repealed Acts, e.g.:

- In the *Armed Forces Act 2006*, substitute “National Information Security Act 2025” for “Official Secrets Act 1911”.
- In the *Freedom of Information Act 2000*, amend section 23(3) accordingly.
- Update cross-references in the *Investigatory Powers Act 2016* and any regulations referring to the *National Security Act 2023*.