LAW LIBRARY
LIBRARY OF CONGRESS

Legal Framework for Nuclear Technology and Information

Australia • United Kingdom

February 2022

LL File No. 2022-020966
LRA-D-PUB-002573

The Law Library of Congress, Global Legal Research Directorate
(202) 707-5080 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

Contents

Australia

Kelly Buchanan
Chief, Foreign, Comparative, and
International Law Division II

SUMMARY In September 2021, Australia, together with the United States and the United Kingdom, announced the new AUKUS security partnership. The first initiative under this arrangement is for Australia to acquire nuclear-powered submarine technology, with an 18-month work program commencing to examine the requirements underpinning the delivery of such submarines. In Australia, this process is being led by a new Nuclear-Powered Submarine Taskforce within the Department of Defence. Following this announcement, the three countries signed an agreement regarding the exchange of nuclear propulsion information, which includes information classed as "Restricted Data" under the U.S. Atomic Energy Act.

Australia is a non-nuclear weapon state and the use of nuclear energy for electricity generation is prohibited by federal laws. It possesses around a third of the world's uranium reserves, which is mined in accordance with federal and state/territory legislation and exported to countries with which Australia has a bilateral nuclear cooperation agreement, requiring that such material only be used for peaceful purposes. It is also party to a number of international agreements related to nuclear security, safety, and the non-proliferation of nuclear weapons, and has signed a comprehensive safeguards agreement and additional protocol with the International Atomic Energy Agency.

Australia's legal framework related to atomic energy includes several statutes that implement international agreements; establish the relevant government agencies and their roles; establish a permit system for the control of nuclear material and associated items; control the importation and exportation of nuclear and radioactive material; seek to protect the health and safety of people, and protect the environment, from the harmful effects of radiation; provide for and govern the operations of a nuclear waste management facility; and apply environmental approval processes to nuclear actions.

The head of the Nuclear-Powered Submarine Taskforce told an Australian Senate committee in October and November 2021 that the Taskforce would be examining what amendments are needed to existing legislation in relation to the acquisition of nuclear propelled submarines, working from a first principles basis to identify the regulatory system needed. This would include consideration of the current U.S. regulatory system for nuclear-powered submarines.

While the permit system related to nuclear material and associated technology under Australia's safeguards legislation includes the ability to place restrictions and conditions on the communication of certain information, there is no equivalent information category under Australia's laws to Restricted Data under the U.S. Atomic Energy Act. There is also no specific reference to nuclear information in the Australian government's Protective Security Policy Framework (PSPF). The PSPF includes policies

that set out how government information is to be classified, the additional caveats that can be added to information, and the handling of information received from foreign governments under international information sharing agreements. Offenses under the Criminal Code Act 1995 (Cth) apply with respect to breaches of information secrecy.

Under the AUKUS nuclear propulsion information sharing agreement, there is reference to a potential "Australian equivalent" to Restricted Data and other classes of nuclear information that exist under the laws of the other two countries, which would be "mutually determined by the Parties." More broadly, it states that "[m]utually determined classification policies shall be maintained with respect to all classified information communicated or exchanged under this Agreement. The Parties shall consult with each other on the classification policies." An Australian government official stated that no legislative changes were needed to implement the agreement. However, a subsequent implementation agreement may provide further details on the requirements for Australia to protect information received under the agreement.

I. Introduction

The Commonwealth of Australia is a federation of six states. In addition, two mainland self-governing territories also have their own parliaments and laws. Under the Australian Constitution, the federal government's areas of exclusive legislative power include foreign affairs and the naval and military defense of the Commonwealth and the states.[1] It also has concurrent powers with state and territory parliaments in various areas, including the environment and overseas trade,[2] and has the power to make laws for the territories.[3] State parliaments can also refer matters that would otherwise be a state responsibility to the federal Parliament, with any subsequent federal law on the issue applying to the referring states or to those that decide to adopt the law.[4]

Australia is a non-nuclear weapon state and "is committed to the goal of a world free of nuclear weapons."[5] It also has no nuclear power stations, and the use of nuclear energy for electricity production is in fact prohibited by federal laws. Australia operates one multi-purpose nuclear reactor, the Open Pool Australian Lightwater (OPAL) reactor, "a state-of-the-art 20-megawatt multi-purpose reactor that uses low enriched uranium (LEU) fuel to achieve a range of activities to benefit human health, enable research to support a more sustainable environment and provide innovative solutions for industry."[6]

[1] Commonwealth of Australia Constitution Act (Cth) (Constitution) s 51(vi) & (xxix), https://perma.cc/WQ3R-KZ6C. See *Three Levels of Government – Governing Australia*, Parliamentary Education Office (PEO), https://perma.cc/423L-MR82.

[2] PEO, supra note 1.

[3] Constitution s 122.

[4] Id. s 51(xxxvii); PEO, supra note 1.

[5] *Nuclear Issues*, Department of Foreign Affairs and Trade (DFAT), https://perma.cc/B2SY-Q2KU.

[6] *OPAL Multi-Purpose Reactor*, Australian Nuclear Science and Technology Organisation (ANSTO), https://perma.cc/2CML-N78X.

Australia "has around one third of the world's uranium resources, and is the world's third ranking producer, accounting for approximately 10 per cent of annual global production."[7] Under Australian government policy, uranium can only be exported for peaceful purposes, with treaty-level assurances and minimum requirements applying in furtherance of this policy.[8]

In September 2021, Australia, the United Kingdom, and the United States announced the creation of a trilateral security partnership, AUKUS. The Australian government announced that the first initiative under AUKUS "is for Australia to acquire nuclear-powered submarine technology, leveraging decades of experience from the US and UK."[9] In order to identify "an optimal pathway to deliver this capability," the three countries agreed to undertake work over an 18 month period to "examine the full suite of requirements that underpin nuclear stewardship, with a specific focus on safety, design, construction, operation, maintenance, disposal, regulation, training, environmental protection, installations and infrastructure, basing, workforce and force structure."[10] Australia established the multi-agency Nuclear-Powered Submarine Taskforce within the Department of Defence to undertake this work.[11]

In November 2021, the three AUKUS partners signed the Exchange of Naval Nuclear Propulsion Information Agreement (ENNPIA),[12] which "will further advance consultations by permitting the United Kingdom and the United States to exchange sensitive and classified naval nuclear propulsion information with a third country for the first time."[13] The ENNPIA includes articles specifically related to Restricted Data, which is a distinct class of U.S. nuclear information under the Atomic Energy Act of 1954.[14] This term is defined in that act as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142."[15]

---

[7] Australian Safeguards and Non-Proliferation Office (ASNO), *Annual Report 2018-19, Section 2: Australia's Uranium Production and Exports* (2019), https://perma.cc/Z475-RZGC. See also Geoscience Australia, *Australia's Identified Mineral Resources 2020*, at 19 & 78 (2021), https://perma.cc/5YKB-7UTE.

[8] *Australia's Uranium Export Policy*, DFAT, https://perma.cc/Z888-8EE9; ASNO, supra note 7.

[9] Press Release, Scott Morrison et al., Australia to Pursue Nuclear-Powered Submarines Through New Trilateral Enhanced Security Partnership (Sept. 16, 2021), https://perma.cc/VV8Q-W54X. See also Transcript, Press Conference by Scott Morrison (Canberra, Sept. 16, 2021), https://perma.cc/722S-Z2C4.

[10] *Nuclear-Powered Submarine Taskforce*, Department of Defence, https://perma.cc/8UA2-XE2Z.

[11] *The Taskforce*, Department of Defence, https://perma.cc/3J5F-CKUK.

[12] Agreement between the Government of Australia, the Government of the United Kingdom of Great Britain and Northern Ireland, and the Government of the United States of America for the Exchange of Naval Nuclear Propulsion Information (ENNPIA) (as presented to the Australian Parliament, Joint Standing Committee on Treaties, Nov. 22, 2021), https://perma.cc/GHH9-MAJ7.

[13] Press Release, Peter Dutton, Australia Signs Exchange of Naval Nuclear Propulsion Information Sharing Agreement (Nov. 22, 2021), https://perma.cc/SDV9-N32K.

[14] Atomic Energy Act of 1954 §§ 11(y) & 141-149, 42 U.S.C. §§ 2014(y) & 2161-2169 (2018).

[15] Atomic Energy Act of 1954 § 11y. The term "special nuclear material" means "(1) plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which the Commission, pursuant to

This report provides an overview of Australia's current legal framework related to atomic energy, including international agreements and domestic legislation.[16] It also outlines Australia's existing policies and laws applicable to nuclear information classification and protection, including domestic information and information received from foreign countries under international agreements.

II. Legal Framework Related to Atomic Energy

A. Ban on Nuclear Power Installations

The existing ban on nuclear power plants in Australia is contained in two federal laws. Section 140A of the Environment Protection and Biodiversity Conservation Act 1999 (Cth) (EPBC Act) prohibits the relevant minister from approving certain nuclear installations:

> The Minister must not approve an action consisting of or involving the construction or operation of any of the following nuclear installations:
> (a) a nuclear fuel fabrication plant;
> (b) a nuclear power plant;
> (c) an enrichment plant;
> (d) a reprocessing facility.[17]

Similarly, section 10 of the Australian Radiation Protection and Nuclear Safety Act 1998 (Cth) (ARPANS Act) also prohibits certain nuclear installations, although it is applicable only to Commonwealth entities:

> (1) Nothing in this Act is to be taken to authorise the construction or operation of any of the following nuclear installations:
> (a) a nuclear fuel fabrication plant;
> (b) a nuclear power plant;
> (c) an enrichment plant;
> (d) a reprocessing facility.
> (2) The CEO [of the Australian Radiation Protection and Nuclear Safety Agency, ARPANSA] must not issue a licence under section 32 in respect of any of the facilities mentioned in subsection (1).[18]

In addition, several Australian jurisdictions have legislation that prohibits the building of nuclear power stations.[19]

---

the provisions of section 51, determines to be special nuclear material, but does not include source material; or (2) any material artificially enriched by any of the foregoing, but does not include source material." Id. § 11aa.

[16] See Parliament of Victoria, Legislative Council Environment and Planning Committee, *Inquiry into Nuclear Prohibition* 5–11 (Nov. 2020), https://perma.cc/WR8A-EWE7.

[17] Environment Protection and Biodiversity Conservation Act 1999 (Cth) (EPBC Act) s 140A, https://perma.cc/8T8H-W3J8.

[18] Australian Radiation Protection and Nuclear Safety Act 1998 (Cth) (ARPANS Act) s 10, https://perma.cc/MY2P-S2JU.

[19] Uranium Mining and Nuclear Facilities (Prohibitions) Act 1986 (NSW), https://perma.cc/B9ET-FKS2; Nuclear Facilities Prohibition Act 2007 (Qld), https://perma.cc/J3A7-4E8L; Nuclear Activities (Prohibitions)

Although Australia has no current plans for a domestic nuclear power industry, there have been several formal discussions[20] on this topic at the state level. These include an inquiry by the South Australian Nuclear Fuel Cycle Royal Commission in 2015 and 2016;[21] consideration of a proposed New South Wales Uranium Mining and Nuclear Facilities (Prohibitions) Repeal Bill 2019 (NSW);[22] and the Victoria Parliament's Inquiry into Nuclear Prohibition in 2020.[23] In addition, at the federal level, a parliamentary committee held an Inquiry into the Prerequisites for Nuclear Energy in Australia in 2019.[24]

B. International Agreements

Australia "is involved in numerous bilateral, plurilateral and multilateral treaties and arrangements which seek to reduce or eliminate certain categories of nuclear weapons and to prevent the proliferation of such weapons and their delivery vehicles."[25]

1. Multilateral and Plurilateral Agreements

Australia is a party to the following treaties:

- Treaty on the Non-Proliferation of Nuclear Weapons (NPT)[26]
- Comprehensive Nuclear Test Ban Treaty (CTBT)[27]
- South Pacific Nuclear Free Zone Treaty (Treaty of Rarotonga)[28]
- Convention on Nuclear Safety[29]

Act 1983 (Vic); Nuclear Activities Regulation Act 1978 (WA), https://perma.cc/92B3-YM4D; Nuclear Waste Storage and Transportation (Prohibition) Act 1999 (WA), https://perma.cc/4SRU-EL4W.

[20] See Geoscience Australia, supra note 7, at 80; Ian Cronshaw, *Australian Electricity Options: Nuclear* (Australian Parliamentary Library, July 20, 2020), https://perma.cc/3AG6-ACE8.

[21] Homepage, *Nuclear Fuel Cycle Royal Commission*, https://perma.cc/4EJ3-TDXG.

[22] New South Wales Parliament, Legislative Council Standing Committee on State Development, *Uranium Mining and Nuclear Facilities (Prohibitions) Repeal Bill 2019* (Report 46, Mar. 2020), https://perma.cc/XD23-3AL5.

[23] Parliament of Victoria, Legislative Council Environment and Planning Committee, supra note 16.

[24] Australian Parliament, House of Representatives Standing Committee on the Environment and Energy, *Not Without Your Approval: A Way Forward for Nuclear Technology in Australia – Report of the Inquiry into the Prerequisites for Nuclear Energy in Australia* (Dec. 2019), https://perma.cc/7JHB-AQ8G.

[25] *Nuclear Issues*, supra note 5.

[26] Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, [1973] ATS 3, https://perma.cc/CN2K-NU9T.

[27] See *Comprehensive Nuclear Test Ban Treaty*, DFAT, https://perma.cc/EY8R-78PK; *Comprehensive Nuclear-Test-Ban Treaty*, ARPANSA, https://perma.cc/RD6S-KVWF.

[28] South Pacific Nuclear Free Zone Treaty, Aug. 6, 1985, [1986] ATS 32, https://perma.cc/KQ87-PBNT.

[29] Convention on Nuclear Safety, Sept. 20, 1994, [1997] ATS 5, https://perma.cc/XXL3-HJ5Y. See *Convention on Nuclear Safety*, ARPANSA, https://perma.cc/WX63-EGRQ.

- Convention on the Physical Protection of Nuclear Material (Physical Protection Convention)[30]
- International Convention for the Suppression of Acts of Nuclear Terrorism[31]
- Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management[32]

In addition, it is part of the Non-Proliferation and Disarmament Initiative (NPDI), a cross-regional group of 12 countries with a mandate to implement the 2010 NPT 64-point Action Plan,[33] and the Proliferation Security Initiative (PSI),[34] as well as other initiatives related to nuclear security.[35] It has also participated in discussions related to a potential Fissile Material Cut-Off Treaty and has been an "active contributor" to the International Partnership for Nuclear Disarmament Verification. However, it does not support the Treaty on the Prohibition of Nuclear Weapons that entered into force in January 2021.[36]

2. Safeguards Agreement and Additional Protocol with the IAEA

Australia signed a comprehensive safeguards agreement with the International Atomic Energy Agency (IAEA) in 1974,[37] and an additional protocol in 1997.[38] Under the agreement, Australia undertakes

> to accept safeguards, in accordance with the terms of this Agreement, on all source or special fissionable material in all peaceful nuclear activities within its territory, under its jurisdiction or carried out under its control anywhere, for the exclusive purpose of verifying that such material is not diverted to nuclear weapons or other nuclear explosive devices.[39]

---

[30] Convention on the Physical Protection of Nuclear Material, Mar. 3, 1980, [1987] ATS 16, https://perma.cc/Z8K5-4SMF; Amendment to the Convention on the Physical Protection of Nuclear Material, July 8, 2005, [2016] ATS 22, https://perma.cc/KTV5-URLE.

[31] International Convention for the Suppression of Acts of Nuclear Terrorism, Apr. 13, 2005, [2012] ATS 13, https://perma.cc/5PAG-8RDZ.

[32] Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management, Sept. 5, 1997, [2003] ATS 21, https://perma.cc/53DE-RMQV.

[33] *Nuclear Issues: Treaties and Initiatives*, DFAT, https://perma.cc/X4MZ-R9RM.

[34] *Proliferation Security Initiative (PSI)*, DFAT, https://perma.cc/WJ8K-JLH9.

[35] *Australian Nuclear Security Profile*, ASNO, DFAT, https://perma.cc/BRB4-BTEL.

[36] *Nuclear Issues: Treaties and Initiatives*, supra note 33.

[37] Agreement between Australia and the International Atomic Energy Agency for the Application of Safeguards in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons of 1 July 1968, July 10, 1974, [1974] ATS 16 (IAEA Agreement), https://perma.cc/BA4Y-9X6C.

[38] Protocol Additional to the Agreement between Australia and the International Atomic Energy Agency for the Application of Safeguards in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, Sept. 23, 1997, [1997] ATS 28 (IAEA Additional Protocol), https://perma.cc/KEG8-RJH2.

[39] IAEA Agreement art. 1.

The IAEA is entitled to independently verify that Australia is complying with this obligation.[40] It is required to "take every precaution to protect commercial and industrial secrets and other confidential information coming to its knowledge in the implementation of this Agreement."[41] Under the additional protocol, the IAEA can request access to and information about nuclear fuel cycle-related research and development activities that do not involve nuclear material.[42] It is required to "maintain a stringent regime to ensure effective protection against disclosure of commercial, technological and industrial secrets and other confidential information coming to its knowledge, including such information coming to the Agency's knowledge in the implementation of this Protocol."[43]

Article 14 of the agreement requires that Australia inform the IAEA if it "intends to exercise its discretion to use nuclear material which is required to be safeguarded under this Agreement in a nuclear activity which does not require the application of safeguards under this Agreement."[44] Furthermore, an arrangement must be made between the parties so that

> only while the nuclear material is in such an activity, the safeguards provided for in this Agreement will not be applied. The arrangement shall identify, to the extent possible, the period or circumstances during which safeguards will not be applied. In any event, the safeguards provided for in this Agreement shall apply again as soon as the nuclear material is reintroduced into a peaceful nuclear activity. The Agency shall be kept informed of the total quantity and composition of such unsafeguarded nuclear material in Australia and of any export of such nuclear material[.][45]

An agreement on an arrangement must be "given as promptly as possible and shall relate only to such matters as, *inter alia*, temporal and procedural provisions and reporting arrangements, and shall not involve any approval or classified knowledge of the military activity or relate to the use of the nuclear material therein."[46]

3. Bilateral Agreements

Australia "currently has 25 bilateral nuclear cooperation Agreements in force covering 43 countries" (including all European Union member states).[47] The Department of Foreign Affairs and Trade (DFAT) explains that

> [a]ll of Australia's uranium is exported for exclusively peaceful purposes, and only to countries and parties with which Australia has a bilateral nuclear cooperation (safeguards)

[40] Id. art. 2.

[41] Id. art. 5(a).

[42] IAEA Additional Protocol art. 2.

[43] Id. art. 15(a).

[44] IAEA Agreement art. 14(a).

[45] Id. art. 14(b).

[46] Id. art. 14(c).

[47] *Australia's Network of Nuclear Cooperation Agreements*, DFAT, https://perma.cc/L4KY-ER7F.

> agreement. These agreements ensure that Australia's nuclear exports are handled in a manner consistent with Australia's uranium export policy.
>
> Australia's network of bilateral nuclear cooperation agreements complements and builds upon the IAEA's safeguards regime. They establish treaty-level conditions on the use of all nuclear material exported from Australia.[48]

The bilateral agreements currently in force include a recent bilateral Australia-United Kingdom Nuclear Cooperation Agreement, which was signed in 2018 and came into force on January 1, 2021,[49] and three agreements with the United States: one covering cooperation on Separation of Isotopes of Uranium by Laser Excitation (SILEX) technology (entry into force 2000),[50] one covering supply to Taiwan (entry into force 2002),[51] and one on peaceful uses of nuclear energy (entry into force 2010).[52] The latter agreement includes a provision on the transfer of information, specifying that "[r]estricted data shall not be transferred under this Agreement."[53] The information protection requirements in the SILEX Agreement are outlined in Section III.D., below.

DFAT notes that each bilateral nuclear cooperation agreement is supplemented by its own "Administrative Arrangement," "a confidential document of less than treaty status between Australia and the other country which establishes procedures to ensure the smooth implementation of the provisions of the bilateral nuclear cooperation agreement."[54]

4. Status of the AUKUS Agreement on Exchange of Naval Nuclear Propulsion Information in Australia

The ENNPIA was tabled in (i.e., presented to) the Australian Parliament on November 22, 2021. It was referred to the Joint Treaties Committee,[55] which received submissions and held two

[48] Id.

[49] Agreement between the Government of Australia and the Government of the United Kingdom of Great Britain and Northern Ireland on Cooperation in the Peaceful Uses of Nuclear Energy, Aug. 21, 2018, [2021] ATS 1, https://perma.cc/2F8U-G3UT. See *Australia – United Kingdom Nuclear Cooperation Agreement*, DFAT, https://perma.cc/TLP9-VGNH.

[50] Agreement for Cooperation between the Government of Australia and the Government of the United States of America concerning Technology for the Separation of Isotopes of Uranium by Laser Excitation [SILEX Agreement], Agreed Minute and Exchange of Notes, Oct. 28, 1999, [2000] ATS 19, https://perma.cc/9MBG-CMP9.

[51] Exchange of Notes Constituting an Agreement between Australia and the United States of America Concerning Cooperation on the Application of Non Proliferation Assurances on Retransfer to Taiwan, July 21, 2001, [2002] ATS 9, https://perma.cc/X5GX-LS6T.

[52] Agreement between the Government of Australia and the Government of the United States of America concerning Peaceful Uses of Nuclear Energy, May 4, 2010, [2010] ATS 25, https://perma.cc/9KC9-XTLL.

[53] Id. art. 3 para. 3.

[54] *Australia's Network of Nuclear Cooperation Agreements*, supra note 47.

[55] Press Release, Parliament of Australia, Treaties Committee to Review AUKUS Nuclear Submarine Information Exchange Agreement (Nov. 23, 2021), https://perma.cc/UD2A-J3M5.

hearings before presenting its report on December 17, 2021.[56] The committee supported the agreement and recommended that binding treaty action be taken.[57]

The information protection requirements in the ENNPIA are outlined in Section III.D., below.

C. Legislation

The Commonwealth legislative framework related to nuclear activities includes separate statutes covering environmental impacts, health and safety, uranium mining, export controls for nuclear materials, nuclear weapon non-proliferation safeguards, and radioactive waste. State and territory laws, which are not discussed in this report, also have provisions related to nuclear facilities, mining,[58] and waste.

1. Atomic Energy Act 1953 (Cth)

The Atomic Energy Act 1953 (Cth) requires that the relevant Commonwealth government minister be notified upon the discovery of a prescribed substance, namely uranium or thorium.[59] It also provides that the Commonwealth owns the uranium located in the Northern Territory,[60] and gives the Commonwealth the power to authorize uranium exploration and mining projects in the Ranger Mining Area.[61] Under these provisions, Energy Resource of Australia (ERA) has been authorized to conduct rehabilitation activities at the mine; ERA ceased mining and processing uranium at Ranger on January 8, 2021.[62] The Northern Territory Mining Management Act 2001 (NT) also applies to activities at the Ranger mine, and the Northern Territory government regulates day-to-day activities.[63] The federal act is administered by the Department of Industry, Science, Energy and Resources (DISER).

[56] Parliament of Australia, Joint Standing Committee on Treaties, *Agreement for the Exchange of Naval Nuclear Propulsion Information* (Report 199, Dec. 2021), https://perma.cc/DKD7-6RDU.

[57] Press Release, Parliament of Australia, Treaties Committee Supports First AUKUS Agreement (Dec. 17, 2021), https://perma.cc/WQV5-CLB2.

[58] See *Onshore Legislation – Uranium*, Geoscience Australia, https://perma.cc/3CQ7-X2WY.

[59] Atomic Energy Act 1953 (Cth) ss 36 & 5 (definition of prescribed substance), https://perma.cc/S36M-QP8Y.

[60] Id. s 35.

[61] Id. s 41.

[62] *Regulating the Ranger Uranium Mine*, Department of Industry, Science, Energy and Resources (DISER), https://perma.cc/C5B9-5YXJ.

[63] Id.

2. Nuclear Non-Proliferation (Safeguards) Act 1987 (Cth)

The Nuclear Non-Proliferation (Safeguards) Act 1987 (Cth)[64] gives effect to Australia's obligations under

- the NPT
- Australia's Comprehensive Safeguards Agreement and Additional Protocol with the IAEA
- agreements between Australia and various countries (and Euratom) concerning transfers of nuclear items and cooperation in peaceful uses of nuclear energy
- the Amended Convention on the Physical Protection of Nuclear Material (CPPNM) and
- the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT).[65]

The act "also establishes a system for control over nuclear material and associated items in Australia through requirements for permits for their possession and transport. Communication of information contained in sensitive nuclear technology is also controlled through the grant of authorities."[66]

Section 13 of the act provides that the minister may grant a person a permit to possess nuclear material or an associated item, subject to such restrictions and conditions as the minister specifies in the permit.[67] These restrictions and conditions may relate to, for example, the locations for which the permit is to have effect, measures to ensure physical security, the persons (or class of persons) who are allowed access, the uses to which the material may be put, and "if the permit is a permit to possess associated technology—the communication of the information contained in, or that may be obtained or deduced from, the associated technology."[68] Associated technology is defined as any document that contains information

> (a) that is applicable primarily to the design, production, operation, testing or use of:
> (i) equipment or plant for:
> (A) the enrichment of nuclear material;
> (B) the reprocessing of irradiated nuclear material; or
> (C) the production of heavy water; or
> (ii) nuclear weapons or other nuclear explosive devices; or
> (b) to which a prescribed international agreement applies and that is of a kind declared by the Minister, in writing, to be information to which this definition applies;
> and includes any photograph, model or other thing from which such information may be obtained or deduced.[69]

[64] Nuclear Non-Proliferation (Safeguards) Act 1987 (Cth), https://perma.cc/25J9-ZD9J.

[65] ASNO, supra note 7.

[66] Id.

[67] Nuclear Non-Proliferation (Safeguards) Act 1987 (Cth) s 13(1) & (2).

[68] Id. s 13(3)

[69] Id. s 4(1).

Additional permits that may be granted under the act include special transport permits, permits to establish a facility, and permits to decommission a facility. In addition, the minister may authorize a person to communicate to another person information of the kind referred to in the definition of associated technology.[70] Such authority may be subject to restrictions and conditions, including in respect of the information (or class of information) in relation to which the authority is to have effect, the persons (or class of persons) to whom information may be communicated, the period for which the authority is to have effect, and "conditions as to the giving of notice of, and obtaining consents for, the communication of information."[71]

Various offenses are contained in the act in relation to, for example, possessing nuclear material without a permit, breaching conditions on a permit or authority, breaching a duty to ensure the security of associated technology, unauthorized communication of information, and communicating information knowing that this could prejudice the physical security of nuclear material.[72] Additional offenses apply that relate to the Physical Protection Convention[73] and to nuclear terrorism.[74]

The act is administered by the Australian Safeguards and Non-Proliferation Office (ASNO), which is a division of DFAT and combined the previous Australian Safeguards Office, Chemical Weapons Convention Office, and Australian Comprehensive Test Ban Office.[75] Part IV of the act sets out the functions and powers of both ASNO and the Director of Safeguards. Part V includes a proviso that the exercise of any power, discretion, duty, or function under the act is authorized "only to the extent that the exercise or performance is not inconsistent with Australia's obligations under the relevant international agreements."[76] Such agreements include the NPT, Australia's agreements with the IAEA, the Physical Protection Convention, and bilateral and plurilateral agreements prescribed in regulations.[77]

3. Other Legislation Related to Treaty Implementation

The following statutes give effect to Australia's obligations as a party to specific international agreements:

[70] Id. s 18(1).

[71] Id. s 18(4).

[72] Id. pt III div 1.

[73] Id. pt III div 2.

[74] Id. pt III div 2A.

[75] *Australian Safeguards and Non-proliferation Office (ASNO)*, ASNO, DFAT, https://perma.cc/84WB-8MSR; *About the Australian Safeguards and Non-Proliferation Office*, ASNO, DFAT, https://perma.cc/5T9V-SVT9.

[76] Nuclear Non-Proliferation (Safeguards) Act 1987 (Cth) s 70(1).

[77] Id. s 70(4) & (5); Nuclear Non-Proliferation (Safeguards) Regulations 1987 (Cth) reg 2A & sch 1, https://perma.cc/Y7GA-DDJ8.

- Comprehensive Nuclear-Test-Ban Treaty Act 1998 (Cth):[78] this act prohibits nuclear weapon test explosion or any other nuclear test explosion, establishes inspection processes, and provides for the establishment and operation of monitoring facilities.
- South Pacific Nuclear Free Zone Treaty Act 1986 (Cth):[79] this act contains various prohibitions related to nuclear explosive devices, and provides for inspection and search processes.

4. Customs Legislation

The Customs (Prohibited Exports) Regulations 1958 (Cth), made under the Customs Act 1901 (Cth), prohibit the exportation of nuclear material listed in schedule 7 of the regulations, unless permission has been granted by the relevant minister.[80] This includes source material, special fissionable material, and other fissionable material, as specified in the schedule. The relevant minister under the regulations is the minister administering the National Radioactive Waste Management Act 2012 (Cth).

The regulations also prohibit the exportation of "high activity radioactive sources," as specified in schedule 7A, unless permission is granted by the minister administering the ARPANS Act.[81] In deciding whether to grant permission, the minister must take into account Australia's international obligations and relations with other countries.[82]

The Customs (Prohibited Imports) Regulations 1956 (Cth) prohibit the importation of any radioactive material or substance, unless permission has been granted by the minister.[83] The relevant minister under the regulations is the minister administering the ARPANS Act.

5. Weapons of Mass Destruction (Prevention of Proliferation) Act 1995 (Cth)

This act covers exports of goods or services not controlled under the customs legislation (i.e. "non-regulated goods") "in circumstances where the goods will or may be used in, or the services will or may assist, the development, production, acquisition or stockpiling of weapons that are capable of causing mass destruction or missiles that are capable of delivering such weapons."[84] It is administered by the Department of Defence.

[78] Comprehensive Nuclear-Test-Ban Treaty Act 1998 (Cth), https://perma.cc/CJ99-UXYF.

[79] South Pacific Nuclear Free Zone Treaty Act 1986 (Cth), https://perma.cc/37QD-K2Z2.

[80] Customs (Prohibited Exports) Regulations 1958 (Cth) reg 9 & sch 7, https://perma.cc/8CFC-XPTZ. See Applying to Export Uranium and Controlled Ores, DISER, https://perma.cc/WZT3-3BKV.

[81] Customs (Prohibited Exports) Regulations 1958 (Cth) reg 9AD & sch 7A.

[82] Id. r 9AD(3).

[83] Customs (Prohibited Imports) Regulations 1956 (Cth) reg 4R, https://perma.cc/73C4-J4MF.

[84] Weapons of Mass Destruction (Prevention of Proliferation) Act 1995 (Cth) s 6(1), https://perma.cc/H4C2-7YG6.

6. Australian Radiation Protection and Nuclear Safety Act 1998 (Cth)

In addition to containing the prohibition on nuclear energy facilities set out above, the ARPANS Act, and its associated regulations,[85] aims to "protect the health and safety of people, and to protect the environment, from the harmful effects of radiation."[86] It applies in conjunction with the safeguards legislation, meaning that, for example, a "controlled person" under the act may be required to hold a license with respect to "controlled material," as well as to hold a permit under the safeguards legislation for the same material, and must satisfy the requirements of both statutes "in so far as they are capable of being satisfied concurrently."[87]

Controlled persons under the ARPANS Act are Commonwealth entities, Commonwealth contractors and their employees, and persons in a prescribed Commonwealth place.[88] In addition, the act applies to "permitted persons," being those who are permitted, under an arrangement with the license holder, to do any of the things for which the license holder is authorized.[89] Controlled material means "any natural or artificial material, whether in solid or liquid form, or in the form of a gas or vapour, which emits ionizing radiation spontaneously."[90] The act also applies to controlled facilities (nuclear installations, prescribed radiation facilities, and prescribed legacy sites) and controlled apparatus (apparatus that produce ionizing radiation and apparatus prescribed by regulations that produce harmful non-ionizing radiation when energized).[91]

The act establishes the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), which is "responsible for licensing Commonwealth entities using radiation and for ongoing compliance monitoring of these entities with the requirements" of the act, regulations, and specific license conditions.[92] ARPANSA states that it "regulates a broad range of sources and facilities from baggage X-ray units in airports to the OPAL research reactor at Lucas Heights," and also regulates "the use of hazardous non-ionising radiation which includes high powered lasers and powerful sources of ultraviolet radiation."[93]

[85] Australian Radiation Protection and Nuclear Safety Regulations 2018 (Cth), https://perma.cc/8XN4-WYDK.

[86] ARPANS Act s 3.

[87] Id. s 9 (example).

[88] Id. s 13 (definition of controlled person).

[89] Id. s 11A.

[90] Id. s 13 (definition of controlled material).

[91] Id. (definitions of controlled apparatus and controlled facility).

[92] *Who We Regulate*, ARPANSA, https://perma.cc/WM87-L6QZ.

[93] Id.

7. Australian Nuclear Science and Technology Organisation Act 1987 (Cth)

This act establishes the Australian Nuclear Science and Technology Organisation (ANSTO).[94] The functions of ANSTO include undertaking research and development in relation to nuclear science and nuclear technology, the application and use of such science and technology, and "the production and use of radioisotopes, and the use of isotopic techniques and nuclear radiation, for medicine, science, industry, commerce and agriculture."[95] Other functions relate to, for example, the conditioning, managing, and storing of radioactive materials and radioactive waste; the provision of advice on aspects of nuclear science and nuclear technology and its application or use; and making grants in aid of research into matters related to its activities.[96] ANSTO is specifically prohibited from undertaking research or development "into the design or production of nuclear weapons or other nuclear explosive devices."[97]

Currently, ANSTO operates "OPAL; a comprehensive suite of neutron beam instruments at the Australian Centre for Neutron Scattering; the Australian Synchrotron; the National Imaging Facility Research Cyclotron; and the Centre for Accelerator Science."[98]

8. National Radioactive Waste Management Act 2012 (Cth)

This act, which is administered by DISER, of which the Australian Radioactive Waste Agency is part, makes provision for the selection of a site for a radioactive waste management facility on land in Australia, and for the establishment and operation of such a facility on the selected site.[99] Following amendments to the act passed in June 2021,[100] in November 2021 the government "declared part of the land at Napandee near Kimba in South Australia as the site for the National Radioactive Waste Management Facility (NRWMF)."[101] According to the Minister for Resources and Water, the site selection process came after a "more than 40-year search to deliver a storage facility for waste largely associated with nuclear medicine production."[102]

---

[94] Australian Nuclear Science and Technology Organisation Act 1987 (Cth) (ANTSO Act) s 4(1), https://perma.cc/DWY7-M83W.

[95] Id. s 5(1)(a).

[96] Id. s 5(1)(b)–(m). See also *Governance*, ANTSO, https://perma.cc/2AMX-LP8T.

[97] ANTSO Act s 5(2).

[98] *What We Do*, ANTSO, https://perma.cc/SNB8-TWY6.

[99] National Radioactive Waste Management Act 2012 (Cth) s 3(1), https://perma.cc/4TBC-H38W.

[100] See *Legislation Confirms Future of Australia's Nuclear Industry*, DISER (June 23, 2021), https://perma.cc/5GTU-MA5D.

[101] *Australian Radioactive Waste Agency*, DISER, https://perma.cc/6ZCP-2FF7. See also *Minister Declares Napandee as the Site for the National Radioactive Waste Management Facility*, DISER (Nov. 29, 2021), https://perma.cc/SQ49-PEHW.

[102] Press Release, Keith Pitt, Bipartisan Support for Establishing Australia's National Radioactive Waste Management Facility (June 22, 2021), https://perma.cc/9FKK-UYAN.

9. Environment Protection and Biodiversity Conservation Act 1999 (Cth)

In addition to the ban on nuclear facilities stated above, the EPBC Act "recognises the protection of the environment from nuclear actions as a matter of national environmental significance."[103] If a nuclear action has, will have, or is likely to have a significant impact on the environment, approval will be needed under the act, involving referral to the relevant minister and undergoing an environmental assessment and approval process.[104] Nuclear actions covered by the act are the following:

a. establishing or significantly modifying a nuclear installation
b. transporting spent nuclear fuel or radioactive waste products arising from reprocessing establishing or significantly modifying a facility for storing radioactive waste products arising from reprocessing
c. mining or milling uranium ores
d. establishing or significantly modifying a large-scale disposal facility for radioactive waste
e. decommissioning or rehabilitating any facility or area in which an activity described in paragraphs (a) to (e) above has been undertaken
f. any other type of action set out in the EPBC Regulations.[105]

The act is administered by the Department of Agriculture, Water and the Environment.

D. Consideration of Regulatory Changes Related to the AUKUS Submarine Initiative

During hearings conducted by the Australian Senate Economic References Committee in October and November 2021 as part of its inquiry into naval shipbuilding,[106] the CEO of ARPANSA and the head of the new Nuclear-Powered Submarine Taskforce were questioned separately about the potential need for regulatory changes in order for Australia to acquire, build, and operate nuclear-propelled submarines. The officials explained that this matter will be examined as part of the 18-month process being led by the Taskforce.

For example, the CEO of ARPANSA, Dr. Larsson, stated that aspects of the ARPANS Act, and possibly the EPBC Act, may need to be clarified, such as with respect to the definitions of nuclear power propulsion. He did not wish to "speculate about the facilities that are going to be needed in the future or the regulatory arrangements around those facilities," and stated that "there is a fair amount of work that needs to be done over the next 18 months in order to clarify further."[107]

[103] *Nuclear Actions*, Department of Agriculture, Water and the Environment, https://perma.cc/5MQ5-DHBU.

[104] Id.; EPBC Act s 21.

[105] *Nuclear Actions*, supra note 103; EPBC Act s 22.

[106] *Australia's Sovereign Naval Shipbuilding Capability*, Parliament of Australia, Senate Economic References Committee, https://perma.cc/29VE-UMGE.

[107] Evidence to Senate Economic References Committee, Parliament of Australia, Canberra, Oct. 15, 2021, 2 (Dr. Carl-Magnus Larsson, CEO, ARPANSA), https://perma.cc/PD58-KSNR.

The head of the Taskforce, Vice Admiral Mead, said that the Taskforce is developing an initial scoping list of legislation that may need amendment.[108] This includes the ARPANS Act, EPBC Act, Nuclear Non-Proliferation (Safeguards) Act, and the Australian Nuclear Science and Technology Organisation Act, as well as relevant state and territory legislation. In a subsequent hearing he said that the Taskforce needs to work with the U.S. "to understand the regulatory system that exists with their submarines and whether we adopt part or all of that regulatory system."[109] He indicated that the Taskforce would work on "first principles and identify the regulatory system we need to put in place," which would then trigger the type of domestic legislation that needs to be changed or introduced.[110] This would also involve working with the IAEA.[111]

III. Classification and Protection of Nuclear Information

While the safeguards legislation enables conditions and restrictions to be placed on the communication of information by those authorized to possess nuclear material and associated technology, it does not establish a special class of information. The Australian government's overarching framework for classifying and protecting official information may also apply, as well as federal criminal offenses related to information secrecy (in addition to offenses under the safeguards legislation). The framework also contains policies regarding the handling of foreign information that is subject to international agreements.

A. Protective Security Policy Framework

The Australian government established a new Protective Security Policy Framework (PSPF) in 2018. The framework consists of a series of 16 protective security policies relating to security governance, information security, personnel security, and physical security.[112] There are two overarching principles, established outcomes for each area, and specific core requirements. The core requirements are "supplemented by supporting requirements intended to facilitate a standardised approach to security implementation across government."[113]

Under the area of governance, for example, a core requirement with respect to "security governance for information sharing" is that "[e]ach entity must adhere to any provisions concerning the security of people, information and assets contained in international agreements

[108] Id. at 52 (Vice Admiral Jonathan Mead, Chief, Nuclear-Powered Submarine Taskforce, Department of Defence).

[109] Evidence to Senate Economic References Committee, Parliament of Australia, Canberra, Nov. 17, 2021, 12 (Vice Admiral Jonathan Mead, Chief, Nuclear-Powered Submarine Taskforce, Department of Defence), https://perma.cc/FX93-VNPN.

[110] Id. at 12.

[111] Id. at 13.

[112] See Attorney-General's Department, *Protective Security Policy Framework – Securing Government Business: Protective Security Guidance for Executives* 4–5 (2018), https://perma.cc/GP9B-SY58.

[113] Id. at 4.

and arrangements to which Australia is a party."[114] In the area of information security, with respect to "sensitive and classified information," the core requirements are that each entity must

> a) identify information holdings
> b) assess the sensitivity and security classification of information holdings, and
> c) implement operational controls for these information holdings proportional to their value, importance and sensitivity.[115]

The policies outlined below do not include specific reference to nuclear information.

1. Security Classification of Information

PSPF Policy 8: Sensitive and Classified Information "details how to correctly assess the sensitivity or security classification of information. It also details marking, handling, storage and disposal arrangements to guard against information compromise."[116] It sets out requirements and guidance for the use of the Australian government's three security classifications: PROTECTED, SECRET, and TOP SECRET. A CONFIDENTIAL classification was retired on October 1, 2020.

The policy explains that the relevant security classification "is based on the likely damage resulting from compromise of the information's confidentiality."[117] For example, in order to be classified as TOP SECRET, an entity would need to assess that there would be a "catastrophic business impact" if confidentiality of the information was compromised, and such compromise would be expected to cause "exceptionally grave damage to the national interest, organisations or individuals."[118] Exceptionally grave damage to the national interest includes, with respect to international relations, "directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries."[119] With respect to crime prevention, defense, or intelligence operations, a compromise in confidentiality would significantly affect "the operational effectiveness, security or intelligence operations of Australian or allied forces."[120] Annex A to the policy sets out the minimum protections and handling requirements for TOP SECRET information,[121] with subsequent annexes setting out the requirements with respect to the other security classifications.

[114] Id.

[115] Id. at 5.

[116] *Policy 8: Sensitive and Classified Information*, Protective Security Policy Framework (PSPF), Attorney-General's Department (last updated Nov. 15, 2021), https://perma.cc/WLE2-PDQD.

[117] Attorney-General's Department, *PSPF 8: Sensitive and Classified Information* 4 (v2018.5), https://perma.cc/YE4A-WCAR.

[118] Id. at 2 & 6.

[119] Id. at 7.

[120] Id.

[121] Id. at 29–30.

The policy also explains the use of caveats in labelling information. These are warnings "that the information has special protections in addition to those indicated by the security classification."[122] The four categories of caveats used are codewords (used primarily within the national security community); foreign government markings (applied to information created by Australian government agencies from foreign source information); special handling instructions indicating particular precautions for information handling; and releasability caveats limiting access to information based on citizenship.[123] The foreign government markings caveat imposes special handling instructions, explained as follows:

> PSPF policy 7: Security governance for international sharing requires that, where an international agreement or international arrangement is in place, entities must safeguard sensitive or security classified foreign entity information or assets in accordance with the provisions set out in the agreement or arrangement.
>
> Foreign government marking caveats require protection at least equivalent to that required by the foreign government providing the source information.[124]

2. Protection of Information Received from Foreign Governments

As indicated above, the relevant PSPF policy applicable to information received from foreign governments is PSPF Policy 7: Security Governance for International Sharing. An overview of the policy states that

> Australia has in place international treaty-level agreements, or less-than-treaty-status arrangements, that provide for equivalent international protection of Australian Government sensitive and security-classified resources. Entities must adhere to the provisions contained in these.
>
> Where appropriate Australia takes a whole-of-government approach to international information sharing agreements.
>
> When entities establish new agreements and arrangements they should contact the Attorney-General's Department to discuss their information sharing requirements. This helps to ensure consistent protections for sensitive and security classified information.
>
> The PSPF prevents sensitive and security classified Australian Government resources from being shared with a foreign entity unless there are explicit legislative provisions, international agreements or arrangements to protect these resources.[125]

The policy includes a brief table setting out the Australian classifications and their equivalencies in four other jurisdictions, including the U.S. It shows that the two highest classifications (TOP

[122] Id. at 10.

[123] Id. at 10–12.

[124] Id. at 10–11.

[125] *Policy 7: Security Governance for International Sharing*, PSPF, Attorney-General's Department (last updated Dec. 9, 2021), https://perma.cc/T6F4-HNQH.

SECRET and SECRET) are the equivalent to those same classifications in the U.S. The now-retired CONFIDENTIAL classification was also equivalent to the same classification in the U.S.[126]

In addition to the security classification, the policy states that the Attorney-General's Department "recommends marking foreign entity information and assets with the caveat RELEASABLE TO. This identifies the source of information or asset and restricts release to certain nationalities."[127] The policy further states that the Department "recommends entities review the relevant international agreement or arrangement to identify additional obligations or protections that may differ from the PSPF core requirements."[128]

B. Secrecy Offenses

Part 5.6 of the Criminal Code Act 1995 (Cth) contains offenses related to the secrecy of information.[129] These include, broadly, "Communication and other dealings with inherently harmful information by current and former Commonwealth officers etc."[130] and "Conduct by current and former Commonwealth officers etc. causing harm to Australia's interests."[131] An aggravated offense may apply if particular circumstances exist with respect to one of these two offenses.[132] Further offenses in the criminal code are "Unauthorised disclosure of information by current and former Commonwealth officers etc."[133] and "Communicating and dealing with information by non-Commonwealth officers etc."[134] The code also contains a list of defenses specific to the secrecy offenses.[135]

"Cause harm to Australia's interests" is defined as specifically including to

> harm or prejudice Australia's international relations in relation to information that was communicated in confidence:
> (i) by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and
> (ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth[.][136]

[126] Attorney-General's Department, *PSPF 7: Security Governance for International Sharing* 4 (v2020.1), https://perma.cc/7ZTK-FS93.

[127] Id. at 5.

[128] Id.

[129] Criminal Code Act 1995 (Cth) sch 1 (Criminal Code) pt 5.6 (Secrecy of information), https://perma.cc/5UUU-D5WR.

[130] Criminal Code s 122.1.

[131] Id. s 122.2.

[132] Id. s 122.3.

[133] Id. s 122.4.

[134] Id. s 122.4A.

[135] Id. s 122.5.

[136] Id. s 121.1(1)(c).

In addition, it includes to "harm or prejudice the security or defence of Australia."[137]

"Inherently harmful information" is defined as including any security classified information. "Information" is broadly defined in section 90.1, while "security classification" is defined in section 90.5(1):

> (a) a classification of secret or top secret that is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes that include the purpose) of identifying information:
> (i) for a classification of secret—that, if disclosed in an unauthorised manner, could be expected to cause serious damage to the national interest, organisations or individuals; or
> (ii) for a classification of top secret—that, if disclosed in an unauthorised manner, could be expected to cause exceptionally grave damage to the national interest; or
> (b) any equivalent classification or marking prescribed by the regulations.[138]

In relation to such information, strict liability applies to an element of an offense that

> (a) a classification is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes that include the purpose) of identifying the information mentioned in subparagraph 90.5(1)(a)(i) or (ii); or
> (b) a classification or marking is prescribed by the regulations as mentioned in paragraph 90.5(1)(b).[139]

C. Agreement with the US on Security Measures for the Protection of Classified Information

In 2002, Australia and the U.S. entered into an agreement "concerning security measures for the protection of classified information."[140] This agreement requires that each party protect classified information received directly or indirectly from the other party according to the terms of the agreement and in accordance with its laws and regulations.[141] However, article 21 of the agreement specifies that the agreement "shall not apply to information for which special arrangements or agreements may be required, such as atomic energy information that the United States designates as 'Restricted Data'."[142]

---

[137] Id. s 121.1(1)(g).

[138] Id. s 90.5(1).

[139] Id. s 90.5(1A).

[140] Agreement between the Government of Australia and the Government of the United States of America Concerning Security Measures for the Protection of Classified Information, June 25, 2002, [2002] ATS 25, https://perma.cc/C7DQ-HFMN.

[141] Id. art. 1.

[142] Id. art. 21(4).

D. Information Security Requirements under Nuclear Agreements with the US

1. SILEX Agreement

The US-Australia SILEX agreement provides that "[s]ensitive nuclear technology and Restricted Data related to SILEX technology may be transferred for peaceful purposes."[143] The agreement requires the following:

> 1. Restricted Data and sensitive nuclear technology transferred pursuant to this Agreement shall be protected in accordance with applicable national legislation and regulations of the Parties and applicable security arrangements between the Parties.
> 2. Restricted Data and sensitive nuclear technology transferred pursuant to this Agreement shall be accorded at least the same level of protection by the recipient Party as that accorded to such information by the transferring Party or its authorized person. The Parties shall consult regarding the appropriate protection of such information.
> 3. Restricted Data and sensitive nuclear technology transferred pursuant to this Agreement shall be made available through channels designated by the Parties for the transfer of such information.
> 4. The transferring Party may:
> (A) stipulate the degree to which any Restricted Data and sensitive nuclear technology that it transfers pursuant to this Agreement, and any sensitive nuclear facilities and major critical components subject to this Agreement, may be disseminated or distributed by the other Party;
> (B) specify the categories of persons under the jurisdiction of the recipient Party who may have access to such Restricted Data and sensitive nuclear technology, and to such sensitive nuclear facilities and major critical components; and
> (C) impose such other restrictions on the dissemination or distribution of such Restricted Data and sensitive nuclear technology and of such sensitive nuclear facilities or major critical components as it deems necessary.
> The receiving Party shall comply with any requirements of the transferring Party pursuant to sub-paragraphs A, B or C of this paragraph.
> 5. Restricted Data, sensitive nuclear technology, major critical components and sensitive nuclear facilities transferred pursuant to this Agreement shall be subject to the provisions of Annex A, which is an integral part of this Agreement.[144]

2. AUKUS Naval Nuclear Propulsion Information Sharing Agreement

The ENNPIA requires that the parties "accord full security protection to classified information communicated or exchanged pursuant to this Agreement in accordance with the Annexes to this Agreement, and in accordance with applicable national law and regulations of the Parties."[145] Furthermore, "[m]utually determined classification policies shall be maintained with respect to all classified information communicated or exchanged under this Agreement. The Parties shall consult with each other on the classification policies."[146] "Classified information" is defined as

[143] SILEX Agreement art. 3(1).

[144] Id. art. 11.

[145] ENNPIA art. V para. A.

[146] Id. art. VII.

> information, data, materials, services or any other matter with the security designation of United States Confidential or higher, United Kingdom OFFICIAL-SENSITIVE or higher, and Australia Protected or higher applied under the laws, regulations and government-wide policies of the Parties respectively. Classified information also includes information designated by the Government of the United States as "Restricted Data," or "National Security Information"; that designated by the Government of the United Kingdom as "Atomic" and "Naval Nuclear Propulsion Program Information (NNPPI)"; and for the Government of Australia, the Australian equivalent as mutually determined by the Parties.[147]

The agreement states that the parties may enter into implementing arrangements to implement the provisions of the agreement.[148]

The agreement includes a technical annex and a security annex that contain additional provisions regarding the communication and protection of information, including in relation to the granting and recording of security clearances for relevant personnel; physical and cyber security of information; the application of document and information control programs with respect to classified information; and requirements for inter- and intra-party transmission processes, among others.

During a hearing of the Joint Standing Committee on Treaties as part of its consideration of the ENNPIA, the former first assistant secretary, international policy and agreements, at the Department of Defence, Scott Dewar, stated that the obligations in the agreement are similar to those under Five Eyes agreements and arrangements, and "[n]o new domestic legislation or amendments to existing legislation are required to implement the agreement."[149] He further commented that "[t]he implementing arrangements envisaged under this would only be about implementing information sharing as per this agreement. The annex, in various elements, talks about equivalency of security classifications as mutually agreed by the parties. It's those sorts of things for which we would have an implementing arrangement."[150]

No official statements were located regarding possible changes to the PSPF pursuant to this agreement, or regarding the development of an Australian equivalent to Restricted Data. However, as indicated by Mr. Dewar, it is possible that the implementation agreement may provide further details on the requirements for the protection of such information by Australia.

---

[147] Id. art. IX para. A.

[148] Id. art. X para. D.

[149] Evidence to the Joint Standing Committee on Treaties, Parliament of Australia, Canberra, Nov. 29, 2021, 2 (Scott Dewar, Former First Assistant Secretary, International Policy and Agreements, Department of Defence), https://perma.cc/H5Q3-99LA.

[150] Id. at 11.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

SUMMARY Atomic energy is governed in the United Kingdom (UK) by a number of Acts of Parliament, some of which give effect to obligations created by international agreements. The UK nuclear program has both civil and defense elements. While the UK is a significant proponent against the testing of nuclear weapons, it has developed its own nuclear weapons and maintains a stockpile for deterrent purposes.

The UK is a close ally to the United States and is a signatory to a number of bilateral treaties that are of significant importance to its policy of nuclear deterrence. One of the most significant bilateral treaties is the Agreement for Cooperation in the Uses of Atomic Energy for Mutual Defence Purposes, which has been described as the cornerstone of the nuclear relationship between the US and UK.

The UK has a number of regulators that serve to ensure standards are met and that safety is ensured for nuclear facilities and those who handle sensitive nuclear information.

The information classification system in the UK has three tiers: official, secret, and top secret. Classification is based upon the impact that would result from the compromise, loss or misuse of the information. In addition to these markings, a legislative framework protects sensitive nuclear information. The UK also has legislation that makes it an offense to disclose information if it would damage to the UK in a number of specified areas.

The UK protects classified information provided to it from international partners in accordance with agreements with the country sharing the information. In cases where there is no agreement, the UK classifies information or assets received as official, although it considers each case on its merits and may provide a higher classification if needed.

I. Introduction

The United Kingdom was the third country in the world to develop nuclear weapons. It tested its first nuclear explosive device in October 1952.[1]

The nuclear program in the UK has both defense and civil elements. There are currently eight nuclear power plants in operation able to supply around 21% of electricity in the UK; some of

[1] House of Commons Library, *Briefing Paper No. 9077, Nuclear Weapons at a Glance: United Kingdom* 5 (Mar. 22, 2021), https://perma.cc/6NG7-ZFGJ.

these are soon to be decommissioned due to age. Six new sites are in the development process to replace the plants approaching the end of their operational life.[2]

The UK has a stockpile of nuclear weapons it uses as a deterrent. The government has stated that the fundamental purpose of its nuclear weapons is "to preserve peace, prevent coercion and deter aggression."[3] It currently has four submarines that can be armed with nuclear weapons, and it maintains a constant presence at sea of at least one submarine at all times. The nuclear deterrent is operationally independent and only the Prime Minister can authorize the use of these weapons.[4]

For defense purposes, the UK previously had pledged to reduce its stockpile to no more than 180 nuclear warheads by the mid-2020s. However, in the government's 2021 Integrated Review of Security, Defense, Development and Foreign Policy, it changed its policy, noting that "in recognition of the evolving security environment, including the developing range of technological and doctrinal threats, this is no longer possible,"[5] and it increased its stockpile cap to no more than 260. In the same policy document, the government announced that, due to the same reasons for increasing its stockpile cap, it was extending its policy on deliberate ambiguity and would no longer disclose its stockpile, deployed warhead, or deployed missile numbers.[6] The policy on ambiguity has been in place for a number of years and continues to apply to details regarding the circumstances under which the UK would consider using its nuclear weapons.[7]

II. Domestic Legislation

Atomic energy in both the civil and defense sectors in the United Kingdom is governed by a number of acts and regulations,[8] including but not limited to the following:

- Nuclear Installations Act 1965[9]
- Radioactive Substances Acts[10]

---

[2] House of Commons Library, *Briefing Paper CBP 8176, New Nuclear Power* 4 (Feb. 26, 2021), https://perma.cc/8FKK-6JPF. See also *Nuclear Electricity in the UK*, gov.uk, https://perma.cc/7LTR-8H9P.

[3] HM Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy* 76 (CP 403, 2021), https://perma.cc/HD5D-PRK5. See also HM Government, *The UK's Nuclear Deterrent*, https://perma.cc/9SEF-FNJS.

[4] HM Government, *Global Britain in a Competitive Age*, supra note 3, at 76.

[5] Id.

[6] Id. at 77.

[7] Id.

[8] A summary of the acts and regulations regarding nuclear and radiological safety that apply to the defense industry is available in Defense Safety Authority, *DSA03–DNSR Defence Nuclear Safety Regulations of the Defence Nuclear Enterprise – Guidance* (2021), https://perma.cc/BQ8R-VEZH.

[9] Nuclear Installations Act 1965, c. 57, https://perma.cc/SKY7-R2EC.

[10] Radioactive Substances Act 1948, 11 & 12 Geo. 6, c. 37, https://perma.cc/4JBJ-DCZ6; Radioactive Substances Act 1993, c. 12, https://perma.cc/4VJT-GFD3.

- Energy Acts[11]
- Nuclear Industries Security Regulations 2003[12]
- Atomic Weapons Establishment Act 1991[13]
- Atomic Energy Authority (Weapons Group) Act 1973[14]
- Atomic Energy Acts[15]
- Atomic Energy Authority Acts[16]
- Nuclear Safeguards Acts[17]
- Nuclear Safeguards and Electricity (Finance) Act 1978[18]
- Nuclear Material (Offences) Act 1983[19]
- Health and Safety at Work etc. Act 1974[20]
- Ionising Radiations Regulations 2017[21]
- Justification of Practices Involving Ionising Radiation Regulations 2004[22]
- Radiation (Emergency Preparedness and Public Information) Regulations 2019[23]
- Health and Safety (Enforcing Authority) Regulations 1998[24]

---

[11] Energy Act 1983, c. 25, https://perma.cc/26H8-UG2X; Energy Act 2004, c. 20, https://perma.cc/8PRK-EQ2N; Energy Act 2008, c. 32, https://perma.cc/T5ZD-3T88; Energy Act 2013, c. 32, https://perma.cc/7W8U-63SB.

[12] Nuclear Industries Security Regulations 2003, SI 2003/403, https://perma.cc/L9SH-DNQT.

[13] Atomic Weapons Establishment Act 1991, c. 46, https://perma.cc/4QLV-MPD6.

[14] Atomic Energy Authority (Weapons Group) Act 1973, c. 4, https://perma.cc/9QRE-TUYQ.

[15] Atomic Energy Act 1946, 9 & 10 Geo. 6, c. 80, https://perma.cc/9PSL-N7HU; Atomic Energy Act 1989, c. 7, https://perma.cc/N4ZQ-4678.

[16] Atomic Energy Authority Act 1954, 2 & 3 Eliz. 2, c. 32, https://perma.cc/NUL5-EF7A; Atomic Energy Authority Act 1971, c. 11, https://perma.cc/HA5D-TZZQ; Atomic Energy Authority Act 1995, c. 3, https://perma.cc/K9E5-U5EL.

[17] Nuclear Safeguards Act 2000, c. 5, https://perma.cc/LP5T-CTLU; Nuclear Safeguards Act 2018, c. 15, https://perma.cc/MP8L-RARD.

[18] Nuclear Safeguards and Electricity (Finance) Act 1978, c. 25, https://perma.cc/WJB5-N3HG.

[19] Nuclear Material (Offences) Act 1983, c. 18, https://perma.cc/FD7X-LZVF.

[20] Health and Safety at Work etc. Act 1974, c. 37, https://perma.cc/4WZK-3KHD.

[21] Ionising Radiations Regulations, SI 2017/1075, https://perma.cc/3D3S-MT37.

[22] Justification of Practices Involving Ionising Radiation Regulations 2004, SI 2004/1769, https://perma.cc/66W4-FRYH.

[23] Radiation (Emergency Preparedness and Public Information) Regulations 2019, SI 2019/703, https://perma.cc/Q8RA-8C39.

[24] Health and Safety (Enforcing Authority) Regulations 1998, 1998/494, https://perma.cc/9BD5-DEG8.

- Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009[25]
- Environmental Permitting (England and Wales) Regulations 2016[26]
- Environmental Authorisations (Scotland) Regulations 2018[27]
- Nuclear Reactors (Environmental Impact Assessment for Decommissioning) Regulations 1999[28]
- Visiting Forces Act 1952[29]

III. Regulators

A. Atomic Energy Authority

The United Kingdom Atomic Energy Authority is an executive non-departmental body that manages the UK's nuclear fusion program. It is currently responsible for researching "fusion energy and related technologies, with the aim of positioning the UK as a leader in sustainable nuclear energy."[30]

B. Atomic Weapons Establishment

The Atomic Weapons Establishment (AWE) is a government company wholly owned by the Ministry of Defence[31] that is responsible for manufacturing, maintaining, developing and, when required, disassembling the UK's nuclear warheads.[32] To fulfil these goals it is required to:

> provide a sustainable and capable nuclear weapons research and production facility; carry out science and engineering research and development to understand the performance of nuclear warheads in order to design and assess the safety, security and effectiveness of the stockpile. [33]

[25] Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009, SI 2009/1348, https://perma.cc/8X6S-AVWM.

[26] Environmental Permitting (England and Wales) Regulations 2016, SI 2016/1154, https://perma.cc/CV8J-K4GU.

[27] Environmental Authorisations (Scotland) Regulations 2018, SSI 2018/219, https://perma.cc/V9ZM-SVNB.

[28] Nuclear Reactors (Environmental Impact Assessment for Decommissioning) Regulations 1999, SI 1999/2892, https://perma.cc/PXC7-VDTN.

[29] Visiting Forces Act 1952 15 & 16 Geo. 6 & 1 Eliz. 2, c. 67, https://perma.cc/ZFL7-M4A5.

[30] *About Us*, UK Atomic Energy Authority, https://perma.cc/7H8E-25F7.

[31] Defence Nuclear Organsation, *AWE PLC: Framework Document* 4 (July 2021), https://perma.cc/ES9Y-98JK. See also *Management & Operations Contract*, AWE (Nov. 2, 2020), https://perma.cc/GZ8Y-TK7L.

[32] Defence Nuclear Organsation, *AWE PLC: Framework Document,* supra note 31, at 5.

[33] Id. at 7.

It conducts these activities at two sites in the UK: Aldermaston and Burghfield in Berkshire.[34]

AWE is also the technical authority for the UK's radiological and nuclear portal detection network and in this role supports the government to detect the smuggling of nuclear and radiological weapons.[35] Additionally, the AWE maintains a constant team to respond to, and render safe, any improvised nuclear weapon discovered in the UK.[36] AWE also provides specialist support to the government on the nuclear and radiological threats that face the UK and "expertise on arms control verification, development of monitoring techniques, and the capability to analyse and advise on nuclear tests."[37]

C. Office for Nuclear Regulation

The Office for Nuclear Regulation (ONR), established by the Energy Act 2013, is the independent regulator of safety and security at 37 licensed nuclear sites in the UK, including both the civil and defense sectors.[38] Seven of these sites are part of the Ministry of Defence's Nuclear Programme and are responsible for providing and maintaining warheads that are used for nuclear deterrence and in support of the UK's nuclear powered submarines.[39]

ONR is responsible for establishing requirements for nuclear security outcomes in the civil nuclear sector to help prevent the theft of nuclear or radioactive materials and sensitive nuclear information, with requirements set within the framework of the Nuclear Industries Security Regulations 2003 (NISR 2003).[40] Regulation of the nuclear industry has recently been marked by a shift towards an outcome-focused approach, encapsulated in the Security Assessment Principles, which are high-level principles that require nuclear licensees to justify security measures in relation to assessed threats rather than by meeting set standards.[41] One of the key principles is that licensees must operate nuclear sites to keep risks as low as reasonably practicable, known as the ALARP principle. As such, licensees must consider what measures must be taken to control the risk posed by their activities and must demonstrate to ONR "that they have done everything 'reasonably practicable' to reduce risks."[42] In determining whether duty holders are meeting their obligations, the ONR uses published guidance including its

[34] House of Commons Library, *Nuclear Weapons at a Glance: United Kingdom*, supra note 1. See also *What We Do*, AWE, https://perma.cc/D3TD-R9MJ.

[35] *Protecting Our Borders*, AWE, https://perma.cc/JU6A-QAJS.

[36] *Delivering Emergency Response Capability*, AWE, https://perma.cc/3RTB-HKSV.

[37] *Comprehensive Nuclear Test Ban Treaty Monitoring*, AWE, https://perma.cc/2TVE-MQFG; *Supporting the Government*, AWE, https://perma.cc/L2T9-5CGR.

[38] ONR, *A Guide to Nuclear Regulation in the UK* 3 (2016), https://perma.cc/L8D7-XXDP.

[39] Id. at 10.

[40] Id.

[41] Karl Dewey et al, *Nuclear Security Culture in Practice: A Handbook of UK Case Studies* 15 (2021) https://perma.cc/BEW3-SVTR.

[42] ONR, *A Guide to Nuclear Regulation in the UK*, supra note 38, at 16.

Security Assessment Principles, the Safety Assessment Principles for Nuclear Facilities, Technical Assessment Guides, and Technical Inspection Guides.[43]

ONR has stated the move to a principle-based approach "has been made possible by the significant improvements in security management capability and capacity developed within dutyholder organisations since the establishment of formal regulation under NISR 2003."[44] It notes that the ultimate legal responsibility for ensuring nuclear safety is with the duty holder.[45]

The ONR also "co-operate[s] with international regulators on safety and security issues of common concern, including associated research."[46]

D. Defence Nuclear Safety Regulator

In addition to licensed nuclear sites, some naval sites that conduct nuclear-related activity are exempt from certain aspects of regulation by the ONR because the subject matter falls under the control of the Ministry of Defence. Different aspects of nuclear radiation and safety at these sites are regulated either by the Defence Nuclear Safety Regulator (DNSR)[47] or the ONR. DNSR has set out extensive guidance for the safety of nuclear and radiological materials.[48] ONR is responsible for the conventional safety regulation of these sites under the following:

- Health and Safety at Work etc. Act 1974 (HSWA)[49]
- Ionising Radiations Regulations[50]
- Radiation (Emergency Preparedness and Public Information) Regulations 2019.[51]

[43] Cabinet Office, *HMG Security Policy Framework* (v. 1.1, May 2018), https://perma.cc/G5M7-KVWM; ONR, *Security Assessment Principles for the Civil Nuclear Industry* (2017), https://perma.cc/V7Y8-55AD; ONR, *Safety Assessment Principles For Nuclear Facilities* (2014 ed. rev. 1, Jan. 2020), https://perma.cc/BF7C-H5NV; ONR, *Permissioning Inspection - Technical Assessment Guides*, https://perma.cc/T86Z-ZR4T; ONR, *Compliance Inspection - Technical Inspection Guides*, https://perma.cc/3M9L-F6G7.

[44] ONR, *Security Assessment Principles for the Civil Nuclear Industry,* supra note 43, at 7.

[45] Id.

[46] ONR, *A Guide to Nuclear Regulation in the UK*, supra note 38, at 3.

[47] *Defence Nuclear Safety Regulator (DNSR)*, Gov.uk, https://perma.cc/2M7A-HDT9.

[48] Defence Safety Authority, *DSA02–DNSR Defence Nuclear Safety Regulations of the Defence Nuclear Enterprise* (May 2021), https://perma.cc/X47E-65KQ. See also Defense Safety Authority, *DSA03–DNSR Defence Nuclear Safety Regulations of the Defence Nuclear Enterprise – Guidance*, supra note 8.

[49] Health and Safety at Work etc. Act 1974, c. 37, https://perma.cc/8FLL-YHHK.

[50] Ionising Radiations Regulations 2017, SI 2017/1075, https://perma.cc/U4VZ-34PM.

[51] Radiation (Emergency Preparedness and Public Information) Regulations 2019, SI 2019/703, https://perma.cc/CYL5-MDHQ.

IV. International Agreements

The UK is a party to a number of international agreements that relate to nuclear activities. These include:

- Treaty on the Non-Proliferation of Nuclear Weapons[52]
- Comprehensive Test Ban Treaty[53]
- International Convention for the Suppression of Acts of Nuclear Terrorism[54]
- Convention on the Physical Protection of Nuclear Material[55]
- Convention on Nuclear Safety[56]
- Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management.[57]

The UK is also a party to bilateral treaties with the US on defense and nuclear issues. These include:

- Agreement between the UK and the USA for Cooperation in the Uses of Atomic Energy for Mutual Defence Purposes (Mutual Defence Agreement)[58]
- Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America for Cooperation in Peaceful Uses of Nuclear Energy[59]
- Polaris Sales Agreement.[60]

---

[52] Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 729 U.N.T.S. 168, https://perma.cc/E9SY-V6B9.

[53] Comprehensive Nuclear Test-Ban Treaty, Sept. 10, 1996, 35 I.L.M. 1439 (not yet in force), https://perma.cc/FV3J-3T36.

[54] International Convention for the Suppression of Acts of Nuclear Terrorism, Apr. 13, 2005, 2445 U.N.T.S. 44004, https://perma.cc/BL8C-Z3CG.

[55] Convention on the Physical Protection of Nuclear Material, Oct. 26, 1979, 1456 U.N.T.S. 124, https://perma.cc/4TXY-8EC4.

[56] Convention on Nuclear Safety, Sept. 20, 1994, 1963 U.N.T.S. 293, https://perma.cc/55ZA-V9VY.

[57] Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management, Sept. 5, 1997, 2153 U.N.T.S. 355, https://perma.cc/HN4K-73LT.

[58] Agreement between the UK and the USA for Cooperation in the Uses of Atomic Energy for Mutual Defence Purposes, July 3, 1958, 326 U.N.T.S. 3, https://perma.cc/HTP7-C4E7.

[59] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America for Cooperation in Peaceful Uses of Nuclear Energy, May 14, 2018, T.I.A.S. No. 20-1231, https://perma.cc/9RM5-WZ29.

[60] Polaris Agreement, April 6, 1963, 474 U.N.T.S. 49, https://perma.cc/3WHT-PTBN.

With regard to its bilateral agreements with the United States, the UK government has stated that the US "remain[s] the UK's most important strategic ally and partner"[61] and that

> [n]uclear cooperation remains an important element of the relationship between the United States and the United Kingdom, enhancing transatlantic security. We will continue to work closely with the United States on nuclear matters, including nuclear deterrence policy. The 1958 Mutual Defense Agreement (MDA) has been central to our shared nuclear security goals and we are committed to its renewal in 2024.[62]

The Mutual Defence Agreement has further been described as the cornerstone of the nuclear relationship between the US and UK and is considered to be "fundamental to the UK in maintaining its independent nuclear deterrent."[63]

The UK, the US, and Australia signed the following tripartite agreement in November 2021:

- Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland, the Government of Australia, and the Government of the United States of America for the Exchange of Naval Nuclear Propulsion Information.[64]

V. Classification of Information Concerning Atomic Energy

In 2014, the government replaced its previous six-tier protective marking system with a new security classification system.[65] The UK government currently has three types of classification: OFFICIAL, SECRET, and TOP SECRET. Classification of information reflects the impact that would result from its compromise, loss or misuse, along with the "need to defend against a broad profile of applicable threats."[66]

The government has noted that care must be taken when determining what classification information is marked at, as "[a]pplying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls [while] too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise."[67] When determining the level of classification, the government has stated:

---

[61] HM Government, *Global Britain in a Competitive Age*, supra note 3, at 60.

[62] Id. at 77.

[63] House of Commons Library, *SN/IA/3147, UK-US Mutual Defence Agreement* 3 (Oct. 2014), https://perma.cc/HW3E-HERG.

[64] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland, the Government of Australia, and the Government of the United States of America for the Exchange of Naval Nuclear Propulsion Information, CP 575, Nov. 21, 2021, https://perma.cc/T99M-DFKY.

[65] Department for Business, Innovation & Skills, *Government Security Classifications: Handling Instructions and Guidance for BIS staff* (v. 2.1.1, Feb. 17, 2014), https://perma.cc/E2JG-6LZ6. The six-tier protective markings under the former system were: UNCLASSIFIED, PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET.

[66] Cabinet Office, *Government Security Classifications* ¶ 2 (May 2018), https://perma.cc/9HX2-TK8G.

[67] Id. ¶ 28.

> [the] "consequence of compromise" must be considered, to determine the asset value, and therefore the necessary controls and the protective marking. When assessing the value of an asset it will be necessary to consider the direct and indirect consequences of compromise in relation to a breach or loss of:
>
> - CONFIDENTIALITY: The restriction of information and assets to authorised individuals.
> - INTEGRITY: The maintenance of information systems and physical assets in their complete and proper form.
> - AVAILABILITY: The continuous or timely access to information, systems or physical assets by authorised individuals.[68]

What level information is classified at is the responsibility of the originator of the information, and only the originator may classify information, or change the classification.[69]

The government has noted that, due to the risks posed by the compromise or loss of nuclear information, "enhanced controls to mitigate these risks will be required even if the likelihood seems slight."[70] Certain nuclear information has further protection requirements established by statutes, discussed further below, that must also be met.

The Government Security Classifications policy should be considered alongside various documents describing the government's Security Policy Framework. The framework includes expectations of how the government, organizations, and third parties that handle government information and assets should apply protective security measures to ensure the government can function both effectively and securely.[71]

A. Official Marking

The Official marking is used for the majority of information that is created by the public sector and that could have damaging consequences if the information were lost, stolen, or publicly published. The government compares this category of information to that held by a large private company, and says that it covers "the generality of government business, public service delivery and commercial activity,"[72] It also covers routine international relations and diplomatic activities

[68] Cabinet Office, *Security Policy Framework* 92, https://perma.cc/48T7-JVH3. This document, which is heavily redacted and appears to be superseded, was provided under a Freedom of Information Act request in 2010, and appears on a nonprofit website that publishes FOIA responses. *Security Policy Framework*, What Do They Know, https://perma.cc/KF8K-5BJZ.

[69] Cabinet Office, *Government Security Classifications*, supra note 667, ¶ 28; Cabinet Office, *Security Policy Framework*, supra note 69, at 99.

[70] Cabinet Office, *Government Security Classifications*, supra note 67, ¶ 28.

[71] Cabinet Office, Government Security Profession, & National Security & Intelligence, *Security Policy Framework* (May 2018), https://perma.cc/H7KK-K4JH.

[72] Cabinet Office, *Government Security Classifications*, supra note 67, Annex, Part 1 ¶ 2.

and "many aspects of defence, security and resilience."[73] Under the Security Policy Framework, "OFFICIAL information can be managed with good commercial solutions that mitigate the risks faced by any large corporate organisation."[74]

The Official classification is considered sufficient to protect information from compromise by attackers that have limited capabilities, such as "hactivists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups."[75]

The Government Security Classifications policy describes as "Baseline Security Outcomes" the following:

- **ALL** HMG information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them in line with local business processes.
- Baseline security controls reflect commercial good practice.[76]

There is no requirement that information in this classification be marked. However, in cases where information in this classification is more sensitive, i.e. where it is clear it could have more damaging consequences if it were compromised, but not of such a degree that warrants increasing the classification, it should be marked as "OFFICIAL—SENSITIVE"[77] at the top and bottom of each page.[78]

B. Secret Marking

The Secret classification is applied to "very sensitive information that justifies heightened protective measures to defend against determined and capable threat actors"[79] and that may be the subject of targeted actions.[80] In addition, the Secret classification applies to information for which compromise would likely result in any of the following:

> a. Directly threaten an individual's life, liberty or safety (from highly capable threat actors).
> b. Cause serious damage to the operational effectiveness or security of UK or allied forces such that in the delivery of the Military tasks:
> i. Current or future capability would be rendered unusable;
> ii. Lives would be lost; or,

[73] Id. ¶ 15.

[74] Cabinet Office, *HMG Security Policy Framework,* supra note 43, at 10.

[75] Cabinet Office, *Government Security Classifications*, supra note 67, ¶ 15.

[76] Id. The baseline security controls are contained in the Annex.

[77] Id.

[78] Id. ¶ 28.

[79] Id. ¶ 2.

[80] Id.¶ 15.

iii. Damage would be caused to installations rendering them unusable.
c. Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.
d. Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction.
e. Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests.
f. Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.
g. Cause major impairment to the ability to investigate or prosecute serious organized crime.[81]

Information in this classification must be clearly marked as "SECRET" at the top and bottom of each page.[82]

C. Top Secret Marking

Top Secret is the classification used for the UK's most sensitive information and services that require the highest levels of protection. This classification covers "[e]xceptionally sensitive [UK government] (or partner's), information assets that directly support (or threaten), the national security of the UK or allies AND require extremely high assurance of protection from all threats."[83] Information in this classification is of interest to "advanced state actors that will prioritise compromising this category of information or service, using significant technical, financial and human resources over extended periods of time."[84]

This classification applies to information that, if compromised, would:

a. Lead directly to widespread loss of life.
b. Threaten directly the internal stability of the UK or friendly nations.
c. Raise international tension.
d. Cause exceptionally grave damage to the effectiveness or security of the UK or allied forces, leading to an inability to deliver any of the UK Defence Military Tasks.
e. Cause exceptionally grave damage to relations with friendly nations.
f. Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.
g. Cause long term damage to the UK economy.
h. Cause major, long-term impairment to the ability to investigate or prosecute serious organised crime.[85]

[81] Id. ¶ 17.

[82] Id. ¶ 28.

[83] Id. ¶ 17.

[84] Id. ¶ 15.

[85] Id. ¶ 17.

Information in this classification must be clearly marked as "TOP SECRET" at the top and bottom of each page.[86]

D. Descriptor Markings

The Government Security Classifications policy provides that information that requires more restrictive handling may be subject to additional markings, known as special handling instructions, that consist of descriptors, codewords, prefixes and national caveats, in addition to the original classification mark, e.g.: "TOP SECRET [DESCRIPTOR]."[87] The government has maintained a list of descriptor marks to help provide consistency across all government departments.[88] The marking ATOMIC has been referred to as a codeword.[89] These additional markings can indicate the "nature or source of its content, limit access to designated groups, and / or to signify the need for enhanced handling measures," but should be used sparingly.[90]

The government has noted that care should be taken to avoid confusing descriptor marks. For example, the "OFFICIAL–SENSITIVE caveat" should not be confused with a separate classification; rather "it is tool to denote OFFICIAL information that is of a particular sensitivity but that can be managed on OFFICIAL systems and infrastructure," and should be used only in limited circumstances.[91] Additional security controls used with this type of descriptor are typically procedural, common sense precautions, such as enforcing need-to-know requirements, rather than technical in nature.[92] The government has further stated that in order to avoid confusion, descriptors should not be used on information sent to overseas partners, as they have not been recognized in any international agreements.[93]

National caveats may be used for information that is particularly sensitive to the UK, or where dissemination must be restricted to specified foreign nations. Where the document is marked with a national caveat, it may not be sent to foreign governments, overseas contractors, international organizations, or foreign nationals without the consent of the originator of the assets. Such marks are usually provided in a format such as "TOP SECRET—UK/US EYES ONLY."[94]

---

[86] Id. ¶ 28.

[87] Id. ¶ 18.

[88] Id. ¶ 21.

[89] Defence Science and Technology Laboratory UK, *Defence Research Report Specification: Format Standards for Scientific and Technical Reports for the United Kingdom Ministry of Defence* 5 (2016), https://perma.cc/N2US-JY53.

[90] Cabinet Office, *Government Security Classifications*, supra note 67, ¶¶ 18, 19.

[91] Cabinet Office, *Government Security Classifications FAQ Sheet 2: Managing Information Risk at OFFICIAL* 7 (v. 2.0, Mar. 2014,), https://perma.cc/S36F-5WML.

[92] Cabinet Office, *Security Policy Framework*, supra note 69, at 96.

[93] Cabinet Office, *Government Security Classifications*, supra note 67, ¶ 23.

[94] Id. ¶ 25.

E. Sensitive Nuclear Information

While not a specific government security classification, the Anti-Terrorism, Crime and Security Act 2001 (ATCSA),[95] the Nuclear Industries Security Regulations 2003 (NISR), and the Energy Act 2013 provide a statutory framework for the protection of sensitive nuclear information (SNI).[96] This is defined within the ATCSA as

> (a) information relating to, or capable of use in connection with, the enrichment of uranium; or
> (b) information relating to activities carried out on or in relation to nuclear sites or other nuclear premises which appears to the Secretary of State to be information which needs to be protected in the interests of national security.[97]

The ONR states that SNI may fall within the following classifications: OFFICIAL—SENSITIVE, SECRET, and potentially TOP SECRET.[98] The ONR has provided the following advice to individuals responsible for applying a security classification to information that includes SNI:

- SNI that could have damaging consequences if lost, stolen or disclosed without authorisation should be classified as OFFICIAL-SENSITIVE. This relates to sensitive information concerning arrangements to protect the public from the risks arising from a radiological event caused by the theft or sabotage of Nuclear Material (NM)/Other Radioactive Material (ORM) and supporting systems or through the compromise of SNI. It typically applies to less detailed information concerning Category I – III NM or Vital Areas (VAs) 2 that is only likely to affect a single layer of defence in depth and/or be of minimal consequence to the overall security effect. Most sensitive information concerning Category IV NM, ORM, Baseline Areas or protective measures for SNI will also be OFFICIAL-SENSITIVE.
- SNI where compromise could seriously damage nuclear security should be protectively marked SECRET. This relates to very sensitive information concerning arrangements to protect the public from the risks arising from a radiological event caused by the theft or sabotage of NM/ORM and supporting systems or through the compromise of SNI. It typically applies to highly detailed and exploitable information regarding Category I – III NM and VAs which could facilitate attack planning by affecting several layers of defence in depth and/or jeopardising an effective security response. There may also be instances where details of protective measures for SNI are SECRET.[99]

[95] Anti-terrorism, Crime and Security Act 2001, c. 24, https://perma.cc/KE66-A754.

[96] ONR, *NISR 2003 - Classification Policy for the Civil Nuclear Industry* 4 (Nov. 2021), https://perma.cc/6468-67T6.

[97] ATCSA § 77(7).

[98] ONR, *NISR 2003 - Classification Policy for the Civil Nuclear Industry*, supra note 97, ¶ 7.

[99] Id. ¶ 8.

The ONR has stated that, within the civil nuclear energy sector, SNI "that could have damaging consequences if lost, stolen or disclosed without authorisation should be classified as OFFICIAL – SENSITIVE: SNI."[100]

The Nuclear Industries Security Regulations 2003[101] requires individuals to protect "sensitive nuclear information." It applies to all information that is generated, or held, by the civil nuclear industry, including from Ministry of Defense contracts or the government, that is protectively marked.[102] Civil Nuclear Security, which is part of the ONR, enforces these regulations. The Civil Nuclear Police Authority is also required to comply with directions issued by the ONR relating to these regulations.[103]

Within the civil nuclear industry, the ONR has stated that it expects digital SNI will always be protected by encryption. The following controls are mandatory:

- Electronic information, at rest and in transit, must be adequately protected by a suitably assured solution. The level of assurance gained will depend upon the assessment scope. Such assessments should take account of recognised principles for product design, security functionality, the asset environment, and specifics of implementation, along with through life assurance in line with guidance set out by the National Cyber Security Centre (NCSC), as the National Technical Authority (NTA).
- Removable Media (USB memory sticks, CD, DVD, external-HDD, floppy disc, etc.) used for SNI data transfer should be encrypted using a suitably assured product in line with NCSC guidance.
- SNI must not be transmitted by fax in the UK or overseas unless its use is required as a standby measure and has been justified and agreed with ONR.[104]

In order to ensure that SNI is protected, ONR conducts announced and unannounced inspections at facilities it oversees. These inspections occur once every three years for OFFICIAL-SENSITIVE SNI and once every two years for SECRET SNI, unless circumstances indicate SNI is at risk.[105]

F. Government Policy

The Government Security Classifications policy notes that "as a minimum, all [government] information must be handled with care to comply with legal and regulatory obligations and reduce the risk of loss or inappropriate access. There is no requirement to mark routine OFFICIAL information."[106]

---

[100] *Regulation of Sensitive Nuclear Information (SNI) in the Supply Chain (List N)*, ONR, https://perma.cc/K6HJ-77ZT.

[101] Nuclear Industries Security Regulations 2003, SI 2003/403.

[102] Cabinet Office, *Nuclear Industries Security Regulations 2003*, at 3 (v. 4.1, last reviewed April 2014), https://perma.cc/N8GV-HVEM.

[103] Energy Act 2004 § 52.

[104] ONR, *A Guide to Nuclear Regulation in the UK*, supra note 388, at 10.

[105] *Regulation of Sensitive Nuclear Information (SNI) in the Supply Chain (List N)*, supra note 101.

[106] Cabinet Office, *Government Security Classifications*, supra note 67, ¶ 3.

The policy sets out four key principles that must be followed. Principle one requires that all information produced by the government be provided with an appropriate degree of protection. Principle two provides that everyone who works with the government has a duty of confidentiality and responsibility to safeguard any government information or data they access, regardless of whether it is marked as classified; individuals are responsible for the compromise, loss or misuse of government information, which can, in certain instances, constitute a criminal offense. The policy notes, "[i]ndividuals are personally responsible for protecting any [government] information or other assets in their care, and must be provided with guidance about security requirements and how legislation relates to their role, including potential sanctions."[107]

Principle three provides that sensitive information must only be provided to those who have a genuine "need to know," along with appropriate security control.[108]

Principle four provides that "assets received from or exchanged with external partners[[109]] **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations."[110]

VI. Legislative Framework Providing for the Security of Nuclear Information

There are a number of pieces of legislation that provide a framework relating to the security and unauthorized disclosure of sensitive material. The legislation discussed below covers government information, as well as provisions specially written to safeguard nuclear information.[111]

The protection of nuclear information is primarily regulated by:

- the ATCSA
- Official Secrets Acts[112]
- Nuclear Industries Security Regulations 2003
- Freedom of Information Act[113]

[107] Id.¶ 6.

[108] Id. ¶ 6.

[109] External partners include foreign governments, international organizations, NGOs, and private individuals. Id. ¶ 11.

[110] Id. ¶ 10.

[111] For a broader overview of legislation that the government Security Policy Framework operates within, see Cabinet Office, *Legal Guidance* (v. 7.1, April 2013), https://perma.cc/VB5P-VLTK.

[112] Official Secrets Act 1911, 1 & 2 Geo. 5, c. 28, https://perma.cc/42LE-7DQH; Official Secrets Act 1920, 10 & 11 Geo. 5, c. 75, https://perma.cc/CNW3-4Y7M; Official Secrets Act 1939, 2 & 3 Geo. 6, c. 121, https://perma.cc/SG6Y-22WZ; Official Secrets Act 1989, c. 6, https://perma.cc/D9D6-GEWQ.

[113] Freedom of Information Act 2000, c. 36, https://perma.cc/9MEC-RWLC.

- Public Records Act[114]
- Data Protection Act[115]

A. Official Secrets Acts

The Official Secrets Acts provide that it is an offense to engage in acts that are prejudicial to the safety or interests of the United Kingdom. The Official Secrets Act 1989 (OSA) contains the main legislative framework that aims to prevent the unauthorized disclosure of official information that damages the UK, its citizens, or its allies.

The OSA applies to current and former Crown servants, government contractors, members of the security and intelligence services, and those who have been notified that the OSA applies to them.[116] Disclosing, without lawful authority, any information, document or article relating to security or intelligence that a person has in their possession due to their position that is damaging is an offense. A disclosure is damaging if it causes damage to the work or any part of the security and intelligence services or is likely to cause such damage; damages the capability of the armed forces to carry out their tasks; leads to the loss of life or injury to members of the armed forces or serious damage to the equipment or installations of the armed forces; endangers the interests of the UK abroad or the promotion or protection by the UK of those interests; endangers the safety of British citizens abroad; or would be likely to have any of these effects.[117]

Damaging the UK's international relations and foreign confidences is also covered by the OSA. It is an offense for individuals who are or have been Crown servants or government contractors to disclose any information, document, or article relating to international relations or confidential information, document or other article obtained from another state or an international organization, without lawful authority, if such disclosure is damaging.[118]

In these circumstances, for a disclosure to be considered damaging, it must endanger the interests of the UK abroad, seriously obstruct the promotion or protection by the UK of these interests, endanger the safety of British citizens overseas, or be likely to have any of these effects.[119] The OSA provides that, for the purposes of this provision, a document is considered to be confidential "at any time while the terms on which it was obtained require it to be held in confidence or while the circumstances in which it was obtained make it reasonable for the State or organisation to expect that it would be so held."[120]

---

[114] Public Records Act 1967, c. 44, https://perma.cc/2D7C-YJC7.

[115] Data Protection Act 2018, c. 12, https://perma.cc/B6DQ-ANAQ; Data Protection Act 1998, c. 29, https://perma.cc/SQM4-VTFT.

[116] Official Secrets Act 1989 § 1.

[117] Id. § 2.

[118] Id. § 3.

[119] Id.

[120] Id.

The unauthorized disclosure of official information that results in the commission of an offense or the escape of a person from legal custody, or impedes the prevention or detection of an offense or the prosecution of a suspected offender, is an offense under the OSA.[121]

The government recently conducted a public consultation that sought opinions on the reform of the Official Secrets Acts. It was noted there have been few recent prosecutions and that the legislation "does not sufficiently capture the discernible and very real threat posed by state threats."[122] It believes that

> [r]eform of the Official Secrets Act 1989 is essential to strengthen the UK's ability to tackle hostile activity by states, by ensuring official information (which can significantly harm the nation and its citizens if it falls into the wrong hands) is better protected, by legislation that enables offenders to be prosecuted and punished appropriately.[123]

B. Anti-terrorism, Crime and Security Act 2001

Section 70 of the ATCSA provides it is an offense to disclose information relating to nuclear security that "might prejudice the security of any nuclear site or of any nuclear material."[124] The disclosure of information that might prejudice nuclear security can be either intentional or reckless. The offense is extra-territorial, meaning that it applies to acts conducted within the UK or those outside the UK by UK persons. It is punishable with up to seven years imprisonment and/or a fine.[125]

To help ensure the safety of nuclear premises and information, the ATCSA provides the Secretary of State the power to direct that the person responsible for nuclear premises take certain actions to ensure that both the premises and information held is secure.[126]

C. Atomic Energy Act 1946

The Atomic Energy Act 1946 provides that it is an offense for any person to communicate a document, drawing, photograph, plan, model, or information that describes, represents or illustrates an existing or proposed nuclear plant, its machinery, equipment or appliances; the purpose or method of operation of such a plan; or any process that is used or proposed to be used in any plant without the consent of the Secretary of State.[127]

---

[121] Id. § 4.

[122] Home Office, *Legislation to Counter State Threats (Hostile State Activity) Government Consultation* 15 (2021), https://perma.cc/W7TT-ANVE. See further Law Commission, *Protection of Official Data*, HC 716, Law Com. No. 395 (2020), https://perma.cc/RA3M-P392.

[123] Home Office, *Legislation to Counter State Threats (Hostile State Activity) Government Consultation*, supra note 123, at 15.

[124] ATCSA § 79.

[125] Id.

[126] ATCSA § 77; Nuclear Industries Security Regulations 2003, SI 2003/403, ¶ 11.

[127] Atomic Energy Act 1946, 9 & 10 Geo. 6, c. 80, § 11, https://perma.cc/QR2C-K3WH.

D. Nuclear Industries Security Regulations 2003

The NISR regulates the security of the civil nuclear industry and requires the Secretary of State to approve a security plan for each nuclear premises that details, in writing, the standards, procedures and arrangements that have been or will be adopted to ensure the safety of the premises, any nuclear material, equipment kept or stored on the premises, and sensitive nuclear information kept on the premises.[128] A nuclear premise is defined in the regulation as

> (a) a nuclear site on which nuclear material or other radioactive material is used or stored;
> (b) premises that form part of a nuclear site and are premises on which a person, who is not the holder of the nuclear site licence and is not acting as an officer, employee or contractor of that holder, uses or stores nuclear material or other radioactive material; or
> (c) other nuclear premises on which Category I/II nuclear material or Category III nuclear material is used or stored, but excluding premises that are used solely for the purpose of the temporary storage of such material during the course of or incidental to its transport in any case where the standards, procedures and arrangements in respect of the security of the transport are contained in an approved transport security statement[129].

The NISR contains a number of "events and matters" that effectively constitute security breaches. These incidents must be reported to the Secretary of State within twenty four hours after the person responsible for the nuclear premises becomes aware of the incident. The incidents include the theft, attempted theft, loss, suspected loss, or unauthorized movement of any nuclear material that is used, stored on, or in transit to, the premises. Any unauthorized access, or attempt to access, to sensitive nuclear information kept on the premises; or any theft, attempted theft, loss or unauthorized disclosure, suspected or otherwise, of sensitive nuclear information kept on the premises must also be reported.[130]

Individuals that have sensitive nuclear information and keep it anywhere other than at a nuclear premises that has an approved security plan in place must:

> (a) maintain such security standards, procedures and arrangements as are necessary for the purpose of minimising the risk of loss, theft or unauthorised disclosure of, or unauthorised access to, any sensitive nuclear information within his possession or control,
> (b) comply with any direction given by the Secretary of State requiring him to take such steps as are necessary or as are specified in the direction for that purpose,
> (c) ensure that each of his relevant personnel who—
> (i) is specified in such a direction as a person whose suitability requires investigation and assessment by the Secretary of State, or
> (ii) falls within a description of persons who are so specified, is a person who has been approved by the Secretary of State as being of suitable character and integrity, having regard to the need to ensure the security of any sensitive nuclear information within the possession or control of the person to whom this regulation applies, and
> (d) report to the Secretary of State any event or matter of a kind specified in paragraph (6) that relates to any sensitive nuclear information within his possession or control as soon as practicable and in any event within 24 hours of its becoming known to him, specifying

[128] Nuclear Industries Security Regulations 2003, SI 2003/403, ¶ 4.

[129] Id. ¶ 1.

[130] Id. ¶ 10.

> the nature of the event or matter and, in the case of an event, the date and time it occurred and the apparent reason for it.[131]

The events and matters specified are

> (a) any theft or attempted theft, or any loss or unauthorised disclosure, of sensitive nuclear information, or any suspected such theft, loss or disclosure;
> (b) any unauthorised access to sensitive nuclear information or any attempt to gain such access;
> (c) any other event or matter which might affect the security of any sensitive nuclear information.[132]

E. Data Protection Act

The Data Protection Act sets out principles relating to the protection of data and provides individuals with rights of access to their personal data. While the Data Protection Act 2018 provides a number of exemptions to these rights of access, including relating to national security, some of the data protection principles and the right of access to personal data may apply to information that is considered sensitive. The government notes that all data must be handled in compliance with the provisions of Data Protection legislation, and that "while [the national security exception] is widely drawn, it is only available to the extent that it is required for the purpose of protecting national security."[133] It has stated that a classification marking can be used to indicate that a national security exemption applies, but that it should not be a determining factor when making the determination.[134]

F. Freedom of Information Act

The Freedom of Information Act 2000 (FOIA) provides for a system for citizens to request information from the government. While the government must consider each individual request on its own merits, the government may use classification markings as an aid in assessing whether a FOIA exemption applies.[135]

A Security Policy Framework document notes that classified information received from foreign governments held by UK government departments and agencies can be subject to disclosure under FOIA. While there are exemptions to disclosure of information on grounds such as international relations and national security, the government must consider each request on its own merits, and these exemptions:

> are subject to public interest balancing tests that cannot be prejudged. The possibility therefore exists that the Information Commissioner, Information Tribunal or the Courts

[131] Nuclear Industries Security Regulations 2003, SI 2003/403, ¶ 22.

[132] Id.

[133] Cabinet Office, *Government Security Classifications*, supra note 67, at 15 (emphasis in original).

[134] Id.

[135] Cabinet Office, *Security Policy Framework*, supra note 69, at 107.

> may compel the disclosure of foreign classified information, even without the express consent of the nation concerned.[136]

G. Public Records Act

The Public Records Act 1967 provides the framework for the preservation of records. Certain records may be closed under one of the exemptions contained in the Freedom of Information Act 2000. The government has stated that the decision whether to retain or close records "are driven by perception of residual sensitivities at the time that release is being contemplated."[137]

VII. Handling of RD Classified Information from the United States

As noted above in part IV, the UK, US, and Australia recently signed a treaty the regarding the exchange of naval nuclear propulsion plant information (NNPPI). The term "restricted data," and the atomic and NNPPI classifications referred to in the treaty do not appear to have been specifically discussed in any publicly available documents originating from the UK government. In the House of Lords debate on this treaty, a Peer noted that the information provisions of the agreement are "based on existing information-sharing practices in place between the United Kingdom and the United States."[138] These existing practices thus provide guidance for how NNPPI would be handled under the treaty.

As noted above, principle four of the Government Security Classifications policy provides that "assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations."[139]

The policy further states:

> Where specific reciprocal security agreements / arrangements are in place with foreign governments or international organisations, equivalent protections and markings must be recognised and any information received must be handled with AT LEAST the same degree of protection as if it were UK information of equivalent classification.[140]

Government functional standards are management standards designed to promote consistent ways of working across the UK government. The government functional standard on security provides that "if an organisation shares information with international partners, it shall have

---

[136] Id. ¶ 4.6.1.

[137] Cabinet Office, *Government Security Classifications*, supra note 67, at 15.

[138] 817 Parl. Deb., HL (6th Ser.) (2022) 177GC, https://perma.cc/8S7B-FJDC.

[139] Cabinet Office, *Government Security Classifications*, supra note 67, ¶ 10.

[140] Id. ¶ 12. This paragraph further states that "[d]etailed information about international and bilateral security agreements and the controls for managing foreign-originated information is set out in the 'International Protective Security Policy' supplement to the SPF," but we have been unable to locate this document.

policies and processes in place to securely manage international classified exchanges that are compliant with government policies and standards."[141]

The Government Security Classifications policy says that in cases where no security agreements or arrangements are in place, any information or assets received must be protected to an equivalent standard of OFFICIAL assets. In certain cases, higher classifications may be appropriate, but care must be taken to ensure that the originator is not precluded from accessing their information by virtue of the UK imposing a higher classification than the originator has access to.[142] The policy further notes that "[t]he need to know principle must be strictly enforced for access to international partners' information."[143]

The UK has further stated that it "will only use international classified information for the purpose for which it was provided, unless otherwise authorised by the originator."[144] International classifications marked as international TOP SECRET are handled in the UK and protected as TOP SECRET. Those marked international SECRET and international CONFIDENTIAL are handled and protected in the UK as UK SECRET. Those marked as international RESTRICTED are handled and protected as UK OFFICIAL—SENSITIVE.[145]

The Cabinet Office has issued guidance on the operation of the June 2007 UK/USA Defense Trade Cooperation Treaty[146] that provides the UK must provide an appropriate degree of security protection and access to defense articles received from the other party.[147] The guidance states that the original US marking of defense articles exported under this treaty must be retained and not be re-marked in the UK with the equivalent UK classification. It notes that material marked RESTRICTED USML//REL USA and GBR Treaty Community must be handled as UK OFFICIAL - SENSITIVE; those marked as CONFIDENTIAL USML//REL USA and GBR Treaty Community and SECRET USML//REL USA and GBR Treaty Community must be handled as UK SECRET.[148]

A guidance document on security requirements for companies working on UK government contracts that require them to hold classified information provides that in cases where government contractors require access to "ATOMIC information," an "ATOMIC Liason Officer" must be appointed who is solely responsible for the security of this information. The appointment

[141] HM, *Government Functional Standard* ¶ 6.7 (GovS 007: Security, v. 2.0, Sept. 13, 2021), https://perma.cc/V662-3PR8.

[142] Cabinet Office, *Government Security Classifications*, supra note 67, ¶ 13.

[143] Id. ¶ 14.

[144] Cabinet Office, *International Classified Exchanges* (v. 1.5, Mar. 2020) ¶ 29, https://perma.cc/S7YL-9T75.

[145] Id.

[146] Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation, June 21, 2007, https://perma.cc/7C4G-ZGV5.

[147] Cabinet Office, *United Kingdom / United States of America Defense Trade Cooperation Treaty* (v. 1.2, Mar. 2020), https://perma.cc/M6F9-W8ZM.

[148] Id. at 3.

of this officer must be approved by the ATOMIC Coordination Office in the Ministry of Defence.[149]

In a Security Policy Framework document, the government notes that the UK is party to international agreements that cover how classified information that originates from foreign governments is handled that "commit the parties to apply equivalent, mutually agreed security standards for the protection of information bearing a security classification and to provide assistance for personnel and industrial security checks."[150] Atomic information agreements are among the international agreements addressing this issue. The Security Policy Framework document states that while the government has attempted to provide consistency between the standards for how UK assets are marked and the requirements to protect foreign classified information, some differences remain. It notes that any treaty entered into imposes legal obligations on both parties and specifies that "[c]lassified assets originated by foreign governments should be afforded the same level of protection determined by its equivalent UK protective marking."[151]

The UK is party to a number of agreements that require it to establish a National Security Authority responsible for protecting classified information that has been received as a result of an international exchange.[152] Within the UK, the Government Security Group (GSG) in the Cabinet Office fulfils this role, but it notes that all government departments and agencies are individually responsible for the security of internationally held classified information.[153]

[149] Cabinet Office, *Security Requirements for List X Contractors* ¶ 6.(e) (v. 7.0. April 2014), https://perma.cc/YJ4Y-LE5S.

[150] Cabinet Office, *Security Policy Framework*, supra note 69, at 53.

[151] Id. at 55.

[152] Id. ¶ 4.

[153] Id.