Research Article
RUSI Journal

Japan's Information Security and Defence Reforms:

From Inner Circle to National Standardisation

Hirohito Ogi and Christopher W Hughes

Recent reforms have elevated information security as a core pillar of Japanese national security. The authors examine the implications for military operations, defence production, and cyber security. The article highlights the shift from closed, inner-circle practices to broader standardisation. It assesses new legal frameworks, international cooperation and ongoing challenges, concluding that Japan's evolving information security architecture has significant progress to date and is pivotal for strengthening defence capabilities in an increasingly complex environment.

Japan's 2022 National Security Strategy (NSS), National Defense Strategy (NDS) and Defense Buildup Programme (DBP) – the 'three national security documents' – have attracted considerable international attention and analysis.[1] This has centred on headline developments – including the adoption of the previous NATO standard requiring 2% of GDP to be allocated to defence expenditure, and a 'counterstrike' doctrine and investment in 'stand-off' missiles.[2] Notwithstanding these headline-making changes, the NSS, NDS and DBP are further focused on 'fundamentally reinforcing Japan's defence capabilities' by addressing many of the more basic but crucial infrastructural foundations of national security and defence, across multiple military domains and capabilities, with the overall aim of strengthening resilience in the face of potential sources of conflict.

A central facilitator of these Japanese defence reform ambitions is information security – identified by the NSS as an 'element of comprehensive national power'. Yet, this aspect has attracted less analysis thus far. This is perhaps due to its more low-key and less tangible profile compared with military platforms.[3]

1. Editorial note: The US spelling of Defense is used for officially translated Japanese bodies, organisations, laws, acts or documents. Elsewhere, the British spelling is used.
2. Cabinet Office, 'National Security Strategy of Japan', 16 December 2022, <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf>, accessed 13 August 2025; Japan Ministry of Defense, 'National Defense Strategy', 16 December 2022, pp. 12, 13–14, <https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf>, accessed 13 August 2025; Japan Ministry of Defense, 'Defense Buildup Program', 16 December 2022, <https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf>, accessed 13 August 2025. For analysis of the 2022 defence reforms, see Jeffrey W Hornung and Christopher B Johnstone, 'Japan's Strategic Shift is Significant, But Implementation Hurdles Await', *War on the Rocks*, 27 January 2023, <https://warontherocks.com/2023/01/japans-strategic-shift-is-significant-but-implementation-hurdles-await/>, accessed 13 August 2025; Adam P Liff, 'Kishida the Accelerator: Japan's Defense Evolution After Abe', *The Washington Quarterly* (Vol. 46, No. 1, 2023), pp. 63–83; Christopher W Hughes, 'Japan's "Three National Security Documents" and Defense Capabilities: Reinforcing a Radical Military Trajectory', *Journal of Japanese Studies* (Vol. 50, No. 1, 2024), pp. 155–83; Robert Ward, *Evaluating Japan's New Grand Strategy* (New York, NY: Routledge, 2025). Japan's inventory of 'stand-off' missiles is projected to include: Tomahawk Block IV and V land-attack cruise missiles; Joint Air-to-Surface Standoff Missile-Extended Range (JASSM-ER) cruise missiles; Joint Strike Missile (JSM) cruise missiles for anti-ship and land attack; upgraded Type-12 cruise missiles in air-, ground- and ship-launched variants; a submarine-launched guided missile for an anti-ship role; a hypersonic guided missile in air- and ground-launched variants for anti-ship and land-attack roles; a hyper velocity gliding projectile (HVGP) ground-launched for land attack; and a new anti-ship and land-attack cruise missile.
3. Cabinet Office, 'National Security Strategy of Japan'.

Japan's information security has undergone important shifts. Courtesy of morepiixel/Adobe Stock

Japan's policymakers in recent years have taken note of trends in other conflict zones and of developments in the capabilities of its US ally and other emerging international partners. As a result, they have become increasingly aware that national defence reforms can only succeed if accompanied by enhancements in two respects: the secure gathering of information; and, crucially, the processing and use of information flows, whether at the strategic or tactical level. These observations are reflected in the NSS and NDS. Without improved information security, Japan's broader ambitions to upgrade the capabilities of the Japan Self-Defense Forces (JSDF) and to advance cooperation with the US and other international partners may prove illusory.

In light of Japan's growing awareness of the indispensability of information security for overall national security, this article investigates three key areas of the country's current and future defence ambitions – military operations, defence production and cyber security – and gauges the degree of progress made in each area in respect of information security. This is not an exhaustive list of the areas of information security applicable to Japan's defence efforts. However, this analysis enables an evaluation of ongoing achievements as well as priorities for further attention in Japan's defence reforms.

This article is significant as the first of its type to study recent developments in Japan's information security practices that are linked to overall defence and security strategy. It provides new levels of detail and up-to-date knowledge on changes in policies, legal frameworks, and capabilities. The article is also one of the first to incorporate into its analysis Japan's increasingly pressing requirements for enhanced information security for cooperation with its US ally and other emerging international partners. To date, much of the literature on Japan's approach to information security, while excellent, has focused on narrower intelligence and information gathering. This differs from the focus here on the secure handling of information across national security requirements as a whole, and, in turn, its application to crucial and evolving domains of Japan's defence posture, whether involving just Japan's own capabilities or working with international partners.[4]

The article argues that Japan's information security has undergone important shifts. The

4. For example studies of Japanese intelligence gathering, see Desmond Ball and Euan Graham, *Japanese Airborne SIGINT Capabilities*, Working Paper No. 353 (Canberra: Strategic and Defence Studies Centre, 2000); Richard J Samuels, *Special Duty: A History of the Japanese Intelligence Community* (Ithaca, NY: Cornell University Press, 2019); Brad Williams, *Japanese Foreign Intelligence and Grand Strategy: From the Cold War to the Abe Era* (Washington, DC: Georgetown University Press, 2021).

country's information security practices in recent years have, in fact, often been of a higher standard than many critical observers – keen to identify that the country has supposedly fallen short of international benchmarks – have assumed. Nevertheless, the crucial requirement for Japan has been to upgrade and shift its information security practices away from the previous concentration within a closed 'inner circle' of the defence establishment. Instead, Japan's objective has become to upgrade information practices and ensure broader sharing and standardisation in terms of regulatory frameworks, and across the rest of government and wider society.

The shift in Japan's information security practices has become essential. This is due to the increasing security risks and requirements imposed by the growing severity of Japan's international environment, and the related and increasing demands for information and defence cooperation with international partners. Overall, therefore, this article concludes that Japan's steady enhancement of its information security architecture forms a pivotal part of its national defence efforts and, thus, for the internal and external balancing of potential adversaries. Its architecture has reached increasingly impressive levels concomitant with international standards.

Key Case Studies: Military Operations, Defence Production, Cyber Security

Military operations are chosen as the first areas for analysis of Japan's information security evolution. For the JSDF to pursue the NSS and NDS's vision of a joint operational architecture for seamless cross-domain operations, it must develop systems for the secure sharing of tactical information. Further, these systems must operate across the three services of the Ground Self-Defense Force (GSDF), Maritime Self-Defense Force (MSDF) and Air Self-Defense Force (ASDF), and in the space and cyber domains. This information security challenge is only amplified when combined with the need to interconnect JSDF operations with joint US–Japan alliance warfare operations for individual or collective self-defence. Japan is further developing a series of defence relationships with 'quasi allies' such as Australia and the UK, and other US partners such as South Korea and the Philippines. These partnerships include Acquisition and Cross Servicing Agreements, Reciprocal Access Agreements and military exercises. They also include sharing of intelligence, surveillance and reconnaissance (ISR), ballistic missile defence (BMD) and command and control. All of these rely on the secure exchange of information. Hence, the article assesses the progress that Japan has made on improving operational information security, as it has expanded cooperation with international partners and the use of mechanisms such as General Security of Military Information Agreements (GSOMIA), General Security of Information Agreements, and the 2013 Act on the Protection of Specially Designated Secrets (SDS Protection Act) or 'state secrecy law'.

Defence production is the second area for examination. This is crucial given the intent expressed in the NSS and NDS to revitalise Japan's indigenous defence industry as 'virtually defence capability itself' and 'an integral part of defence capability'. Japan's task is to be undertaken in large part through increasing international collaborations for joint R&D and production. Such collaboration requires strong information security sharing arrangements.[5] Japan has embarked on the major project of the Global Combat Air Programme (GCAP), with the UK, Italy and Japan as the lead partners, and potentially incorporating other future partners, in the development and procurement of a sixth-generation fighter aircraft.[6] Japan will continue to work with the US on projects relating to glide-phase hypersonic missile interceptors, Collaborative Combat Aircraft, and AI, and an advanced trainer and tactical aircraft, and may even join AUKUS Pillar II.[7]

5. Japan Ministry of Defense, 'National Defense Strategy', p. 33; Japan Ministry of Defense, 'Defense Buildup Program', p. 34.
6. GCAP has attracted speculation, variously, that Saudi Arabia, Germany, Canada and Australia could join the project in some form as technological development or procurement partners. For analysis of the GCAP programme and its role in Japan's international defence production strategy, see Christopher W Hughes, 'Japan's Defence Industrial Strategy and Fighter Aircraft Production: Striving for Tier-One Status and the GCAP Project', *Defence Studies* (Vol. 25, No. 2, 2025), pp. 279–300.
7. Gregg Rubinstein, 'Cooperative Defence Acquisitions Strengthen U.S.-Japan Alliance', Center for Strategic and International Studies, 30 January 2025, <https://www.csis.org/analysis/cooperative-defense-acquisitions-strengthen-us-japan-alliance>, accessed 13 August 2025; Ministry of Defence, 'AUKUS Partnership to Consult with Other Nations Including Japan on Military Capability Collaboration', 8 April 2024, <https://www.gov.uk/government/news/aukus-partnership-to-consult-with-other-nations-including-japan-on-military-capability-collaboration>, accessed 13 August 2025.

Japan's participation in bilateral and multilateral defence production projects is only set to grow with recent and future relaxations of the Three Principles on Overseas Transfer of Defence Equipment that govern its ability to share sensitive technologies. The fundamental basis for the success of such projects is the ability to securely share classified information on technology and production among partners. As the DBP acknowledges, 'the protection of information from intelligence activities and cyberattacks by foreign countries or other causes, is a prerequisite for defense production and international equipment and technology cooperation'.[8]

In the past, Japan has been seen as an outlier that lacked knowledge and policies for the secure sharing of information on weapons platforms. There have been high-profile incidents that have revealed the lack of even basic security protocols. One of the most notable was the revelation in 2006–07 that an MSDF junior officer copied details of the US Aegis system on to a compact disc and passed this to other MSDF officers, who themselves made copies.[9] These actions caused the US to temporarily halt the shipment of parts of Aegis radar upgrades for the Japanese destroyer Kongō, just as Tokyo was pressing Washington to allow it to procure the highly sensitive F-22 fighter and stealth technologies. This article tackles some of those lingering preconceptions of the past, as well as the current deficiencies of Japan's information security practices.[10] It seeks to evaluate Japan's degree of progress in matching the policies and standards of its partners – such as through the implementation of the 2013 Act on SDS – and thus its recasting as a reliable and leading partner in future international defence production projects.

Cyber security is the third vital area relating to information security. Cyber security is crucial for maintaining the resilience and networking of JSDF command and control, and frontline military operations and platforms. It is also important for Japan's broader national defence and civilian infrastructure.[11] Moreover, cyber has itself become a domain for potential hybrid conflict. Cyber security has again been an area of perceived weakness for Japan's national security. The country's civilian and military infrastructure – including defence producers and the Japan Ministry of Defence (JMoD) – has been subject to hacking by groups believed to be from China, Russia and North Korea. Most notably, former US Director of National Intelligence Dennis Blair, during an April 2022 briefing with senior figures in the governing Liberal Democratic Party's (LDP) Policy Research Council Security Research Committee, reportedly stated that Japan's deficiencies in cyber security were the 'biggest weak point of the Japan–US alliance'.[12] In 2023, the then-chief of the US NSA, Paul Nakasone, reportedly, visited the JMoD to receive briefings on the alleged Chinese hacking of Japan's defence cyber networks.[13]

Nonetheless, as outlined in this article, in recent years, Japan has made important advances in cyber security policies and the pursuit of an active cyber defence (ACD) doctrine, including through the passage of new legislation in May 2025. The Active Cyber Defense Act will enable not only the monitoring of sources of cyber threat, but also the initiation of countermeasures in cyberspace to disrupt the capabilities of such threats and adversaries. Additionally, this article examines, in the context of cyber security, the significance of related legislation in the form of the 2024 Act on the Protection and Utilization of Critical Economic Security Information.

Japan's Information Security Evolution Post-World War Two

Contrary to common misunderstandings and criticisms, Japan has maintained information security regulations since the JSDF's establishment in 1954. Article 59 of the 1954 JSDF Act enacted a provision on information security obligations for JSDF personnel (shō hi or 'JMoD confidential').[14] The Japan Defense Agency

8. Japan Ministry of Defence, 'Defense Buildup Program', p. 35
9. *Taipei Times*, 'Japanese Officer Arrested Over Defense Leak', 14 December 2007, <https://www.taipeitimes.com/News/world/archives/2007/12/14/2003392484>, accessed 13 August 2025.
10. For instance, see Eva Pejsova, 'Inside the "Puzzle Box": Unlocking Domestic Barriers to Japan's Defence Transformation', CSDS Policy Brief 19/2025, Centre for Security, Diplomacy and Strategy, Brussels School of Governance of the Vrije Universiteit Brussel, 15 July 2025, <https://csds.vub.be/publication/inside-the-puzzle-box-unlocking-domestic-barriers-to-japans-defence-transformation/>, accessed 13 August 2025.
11. Japan Ministry of Defence, 'National Defense Strategy', p. 11.
12. *Yomiuri Shimbun*, 'Defense Perspective: Proposals / Cybersecurity Command Post Urgently Needed to Direct Active Cyber Defense', 22 November 2022, <https://japannews.yomiuri.co.jp/politics/political-series/20221122-72394/>, accessed 13 August 2025.
13. *Washington Post*, 'China Hacked Japan's Sensitive Defense Networks, Officials Say', 8 August 2023.
14. 'Jieitaihō' ['The Self-Defense Forces Act'], No. 165 of 1954, <https://laws.e-gov.go.jp/law/329AC0000000165>, accessed 13 August 2025.

(JDA), JMoD's predecessor prior to its creation in 2007, also established in 1954 – under the Act on Protection of Secrets Incidental to the Mutual Defence Assistance Agreement Between Japan and the United States of America (often referred to as the MDA Secrets Protection Act) – a separate category of 'Special Defence Secrets' that covered classified information on weapons transferred by the US.[15] Based on these provisions, and through the directives issued by the JDA Director General in 1958, the JDA institutionalised procedures for personnel security clearance (PCL) and other devices for those persons eligible to handle these categories of classified information.[16]

Despite these provisions, Japan's regulations still lacked more fully institutionalised mechanisms for enhancing the effectiveness of information security. Defence-related classified information was distributed solely among JSDF personnel and traditional defence contractors as an 'inner circle'. It was deemed that there was no urgent need for wider statutory law to provide explicit procedures and requirements for PCL and other security clearance mechanisms. The JDA simply mandated security clearance procedures for JSDF personnel and defence contractors through internal directives and contract clauses. In addition, due to the then limited prevalence of advanced communication technologies, the JDA was not obliged to consider stricter standardised physical and cyber security measures.

JDA practices did not change even after the strengthening of information security through amendments of the JSDF Act in 2001 (then Article 96 bis) and the introduction of a new category termed 'Defence Secrets', the breach of which came with stricter criminal penalties. This amendment was part of the strengthening of preventative measures taken in response to an incident in 2000 involving the compromise of classified information by an MSDF officer who passed documentation to a Russian military attaché.[17] But even though this amendment served as the later basis for the Act on SDS, it did not itself articulate the necessary procedures on security clearance. Instead, the expectation was that the prospect of stricter penalties would function as a deterrent against intentional compromises or gross negligence of JSDF personnel and contractors.

Operational Security

Despite recognition, as flagged in the 2022 defence reforms, of the necessity of information security for military operations, the turning point in the post-war period for Japan's inner defence circle to achieve a semi-tacit understanding of its importance only came in the mid-2000s. This stemmed from plans to upgrade US–Japan operational cooperation, especially for bilateral consultations on the realignment of US forces in Japan. The US–Japan Security Consultative Committee (SCC), or '2+2', meeting of defence and foreign ministers in May 2006 produced the Roadmap for Realignment Implementation. The relocation of the US Marine Corps Futenma Air Station from Ginowan City to Henoko in northern Okinawa inevitably attracted the greatest attention given the political tensions domestically and within the alliance over the need to reduce the burden that local prefectural communities bore in hosting US bases. The Roadmap also contained other critical measures for strengthening bilateral defence cooperation, notably the collocation of ASDF and US Air Force commands at Yokota Air Base near Tokyo and the collocation of the new GSDF Central Readiness Force (CRF) Command and the US Army's forward command at Camp Zama in Kanagawa Prefecture.[18] The collocation of these bilateral component commands was expected to increase exchanges between the US and Japan of sensitive operational information, including information for BMD. The SCC further agreed to enhance

15. 'Nichibei Sōgo Bōei Enjo Kyōteitō ni Tomonau Himitsu Hogohō' ['Act on Protection of Secrets Incidental to the "Mutual Defense Assistance Agreement Between Japan and the United States of America"'], No. 166 of 1954, <https://www.japaneselawtranslation.go.jp/en/laws/view/707#:~:text=Act%20on%20Protection%20of%20Secrets,America%22%20%2D%20Japanese%2FEnglish%20%2D>, accessed 13 August 2025. It was previously referred to simply as 'Defense Secrets' before the 2001 amendment when new 'Defense Secrets' were introduced. For an English translation of the JSDF Law, see Robert D Eldridge and Musashi Katsuhiro (eds) *The Japan Self-Defense Forces Law: Translation, History, and Analysis* (Cambridge: Cambridge Scholars Publishing, 2019).
16. Kutsunuki Kazuhito, 'Bōeishō Jieitai ni okeru Himitsu Hozen Seido no Hensen to Kadai' ['The Evolution and Challenges of the Secrecy Protection System in the Self-Defence Forces'], *Rippō to Chōsa* (No. 470, November 2024), pp. 133-145, especially pp. 135–38.
17. Kutsunuki, 'Bōeishō Jieitai ni okeru Himitsu Hozen Seido no Hensen to Kadai' ['The Evolution and Challenges of the Secrecy Protection System in the Self-Defence Forces'], p. 139.
18. United States–Japan Security Consultative Committee, 'United States-Japan Roadmap for Realignment Implementation', 1 May 2006, <https://www.mofa.go.jp/region/n-america/us/security/scc/doc0605.html>, accessed 13 August 2025. The CRF was reorganised in 2018 into the units under the Ground Component Command.

bilateral contingency planning, information sharing and intelligence cooperation.[19]

Such ambitions for enhanced bilateral operational cooperation appeared to drive US demands that Japan adhere to international standards for information security architectures, especially on PCL.[20] Consequently, in 2007, the US and Japan concluded a GSOMIA, with Article 7 on PCL detailing eligibility provisions for the handling of classified information based on the principle of mutual provision of 'substantially equivalent' protection.[21] The language used in the GSOMIA of 'substantially equivalent' was a flexible concept. The US did not demand that Japan construct a symmetrical domestic security architecture. Instead, Japan was obliged to protect classified information provided by counterpart states in a manner substantially equivalent to that of its counterparts through a combination of statutory laws, internal directives, contracting clauses, or other security practices. At the same time, the bilateral agreement indicated for the Japanese side that developing a well-operationalised security clearance system was long overdue.

The conclusion of the US–Japan GSOMIA catalysed a Japanese government-wide standard for information security, termed in 2007 the 'Basic Policy on Strengthening Counterintelligence Capabilities'.[22] A new category of government-wide classified information termed 'Specially Controlled Secrets' was established based on this policy, and, in turn, standard procedures for PCL and related background investigations that required compliance from each government agency as articulated by a memorandum of understanding. Even though these procedures held no legally binding effect, they served – in addition to 'defence secrets' designated in the JSDF Act – to provide another foundation for the later SDS Act. Moreover, in 2010, the US and Japan established the Bilateral Information Security Committee to discuss means to improve bilateral – and, most pointedly, Japan's – government-wide information security.[23]

In line with these developments, in January 2011, the Kan Naoto government of the Democratic Party of Japan formed an advisory committee on information security legislation. After extensive proceedings, the committee submitted a report to the government in August of the same year. It recommended the establishment of stricter, government-wide, and more effective information security legislation.[24] This recommendation led to the SDS Protection Act in 2013, passed under the LDP's Abe Shinzō administration and its Kōmeitō coalition partner, that stipulated a clear PCL procedure with institutionalised background investigations.

Japan's seven-year effort to strengthen its information security, with a particular focus on operational cooperation with the US, thus finally resulted in the promulgation of standardised security clearance requirements in statutory law. This new architecture was of further utility as it could be applied to cooperation with other international partners. Between 2011 and 2021, Japan concluded GSOMIAs or information sharing agreements with France, Australia, the UK, India, Italy, South Korea, and Germany. Although it is not the case that all of these states as yet have the intent to engage with Japan in joint operations, and thus the immediate need to share sensitive operational and tactical information.

The Japan–South Korea GSOMIA was certainly, at least, though, driven by the strong need for bilateral information sharing on North Korean military activities and provocations, especially ballistic missile launches. Moreover, if certain European partners and Australia were to play a supporting role in the Indo-Pacific theatre in a conflict, operational information sharing and information security would provide an indispensable and robust basis for enhancing

19. United States–Japan Security Consultative Committee, 'Joint Statement', 1 May 2006, <https://www.mofa.go.jp/region/n-america/us/security/scc/joint0605.html>, accessed 13 August 2025.
20. Indeed, the 2005 US–Japan 2+2 Joint Statement states that to facilitate information exchanges, 'both sides will take additional necessary measures to protect shared classified information so that broader information sharing is promoted among pertinent authorities'. United States–Japan Security Consultative Committee, 'Joint Statement', 29 October 2005, <https://www.mofa.go.jp/region/n-america/us/security/scc/doc0510.html>, accessed 13 August 2025.
21. Ministry of Foreign Affairs of Japan, 'Agreement Between the Government of Japan and the Government of the United States of America Concerning Security Measures for the Protection of Classified Military Information', 10 August 2007, <https://www.mofa.go.jp/region/n-america/us/security/agree0708.html>, accessed 13 August 2025.
22. Government of Japan, 'Kauntāinterijensu Kinō no Kyōka ni Kansuru Kihon Hōshin' ['Basic Policy on Strengthening Counterintelligence Capabilities'], August 2007, <https://taroyamada.jp/wp-content/uploads/2013/11/d2b9378a83853e7c036d3da9435d29bc.pdf>, accessed 10 July 2025.
23. Answer by Minister for Foreign Affairs Fumio Kishida, Committee on Foreign Affairs, House of Representatives, 185th Diet Session, Minutes No. 3, 6 November 2013.
24. Himitsu Anzen no Tame no Hōsei no Arikata ni Kansuru Yūshikisha Kaigi [The Advisory Committee on Information Security Legislation], 'Himitsu Hozen no tame no Hōsei no Arikata ni Tsuite' ['Report on the Legal Framework for the Protection of Classified Information'], August 2011, <https://www.ombudsman.jp/data/141203-1.pdf>, accessed 10 July 2025.

such cooperation. In fact, in 2024, Australia declared its intention to despatch personnel to the US–Japan Bilateral Information Analysis Cell (BIAC) at Yokota Air Base that jointly analyses operational information gathered by respective ISR activities.[25] Again, BIAC's dealing with sensitive information means that security clearance procedures are a prerequisite, not just for bilateral cooperation, but also for enhancing trilateral cooperation.

Defence Production

Aside from operational security, the main significance of the SDS Protection Act has been to signal to international partners the increasing reliability of Japan's information security practices in a range of areas, including defence production. Access to most operational information and intelligence from international partners is already limited to JSDF personnel and other relevant government officials. These people must possess Japanese citizenship and are substantially vetted for their personal profile at the time of recruitment. Hence, there should be many opportunities for scrutiny of personnel before they handle any classified operational information. Industrial information security, and the ready ability to scrutinise its handling, however, is different from operational security in several regards, and thus strongly applicable to the new strictures of the SDS Protection Act.

Defence R&D and production involve employees of defence contractors. The JMoD naturally does not have the opportunity to vet such employees at the point of recruitment. Moreover, the development and production of weapons systems require complex processes and supply chains. As such, many personnel from outside government might handle sensitive information. In this sense, PCL procedures are arguably even more critical for industrial security than operational security. For these reasons, together with the operational security considerations examined above, the US has seemingly maintained a strong interest in modernising Japan's PCL procedures and pushed for the conclusion of the US–Japan GSOMIA amid increasing bilateral government and industrial cooperation on the co-development of BMD systems.

Of course, the SDS Protection Act includes provisions on security clearance for defence contractors. However, its addition alongside the other extant frameworks created a patchwork of legal structures. These lacked systematisation and faced various difficulties in implementation. In particular, while the SDS Protection Act stipulates the specifics on PCL requirements, the MDA Secrets Act of 1954 does not provide such requirements in detail, even though it is the main device to protect classified information on US weapon technologies. US government and industry counterparts may understandably have been puzzled by such seemingly opaque provisions. This might then have been the source of the confusion and widespread view that Japan's information security remained deficient even after the enactment of the SDS Protection Act.

To address this problem, the JMoD devised a stopgap measure. In December 2014, it announced the Guidelines for Protecting Classified Information Related to Defense Procurement. These Guidelines provide clear designations for those employees of defence contractors who are allowed to handle classified information, including MDA Secrets. The defence contractors are required to obtain the consent of the JMoD to such designations.[26] As the Guidelines form an integral part of defence contracts that have binding force, the PCL procedures are guaranteed, both for SDSs as well as other classified information and MDA Secrets.[27]

On the back of these measures, Japanese defence companies are enabled to participate in the manufacture of F-35 fighter aircraft in the final assembly and checkout phase, as well as in the international maintenance, repair, overhaul and upgrade partnership. The US strictly controls technology related to F-35s, and, so far, no

25. Japan Ministry of Foreign Affairs, 'Eleventh Australia-Japan 2+2 Foreign and Defence Ministerial Consultations', 5 September 2024, <https://www.mofa.go.jp/files/100720472.pdf>, accessed 13 August 2025.
26. Bōeishō [Japan Ministry of Defence], 'Sōbi Hintō no Chōtatsu ni Kakaru Himitsu Hozen TaisakuGuidelines' ['Guidelines for Protecting Classified Information Related to Defence Procurement'], 24 December 2014, <https://www.mod.go.jp/atla/industrialsecurity/files/himitsu_guide_bokeiso19072_r060313.pdf>, accessed 9 November 2025.
27. This was inherited by, and incorporated into, the 'Contract Clauses for Defense Business-Qualified Contractors' introduced in July 2025 as part of the JMoD's effort to establish simplified procedures for contractors. 'Bōei Jigyō Tekigō Jigyōsha Keiyaku Jōkō' ['Contract Clauses for Defense Business-Qualified Contractors'], July 2025, <https://www.mod.go.jp/atla/industrialsecurity/files_tekigo/terms/0301_jigyosha_keiyaku_r0707.pdf>, accessed 9 November 2025.

Table 1: Japan's Classified Information Categories

Classification	Specially Designated Secrets	Special Defence Secrets (MDA Secrets)	JMoD Confidential/ Defence Equipment Confidential	Critical Economic Security Information
Level	Top secrets, secrets	Top secrets, secrets, confidential	Confidential	Confidential
Year of establishment	2013	1954	1954/2023	2024
Legal basis	SDS Protection Act	MDA Secrets Protection Act	JSDF Act/Act on Enhancing Defence Production and Technology Bases	Act on the Protection and Utilization of Critical Economic Security Information
Type	Defence, diplomatic, prevention of specified harmful activities and terrorism	US-made weapons	Defence	Economic security
Personnel security clearance	Explicit in the law	Explicit in directives and contracting clauses	Explicit in directives and contracting clauses	Explicit in the law
Penalty for violations	Imprisonment (up to 10 years) or a fine	Imprisonment (up to 10 years) or a fine	Imprisonment (up to one year) or a fine	Imprisonment (up to five years) or a fine
Note	*Incorporated Defence secrets of the JSDF Law (Article 96) in 2001 and Specially Controlled Secrets in 2007*		*JMoD Confidential for JSDF personnel and Defence Equipment Confidential for contractors*	

Source: Authors' collation from sources cited in the article.

compromise of classified information related to these aircraft has been reported from Japan.[28] In addition, in 2022, the JMoD released a Special Clause for Cybersecurity on Defense Contracts that incorporates the cyber security requirements for handling controlled unclassified information (CUI) within defence contractors as provided for in the US NIST SP 800-171. In 2023, the JMoD further released a Defense Industrial Security Manual similar to that of the US's National Industrial Security Program Operating Manual.[29] These documents assist current and future contractors to comprehend the requirements for meeting the strict standards of defence contracts.

Furthermore, in 2023, Japan's parliament, the National Diet, passed the Act on Enhancing Defense Production and Technology Bases. This established a new classification termed 'Defense Equipment Confidential'.[30] The intention is to extend the reach of the law beyond JSDF personnel and to impose criminal penalties on private citizens employed by defence contractors that violate the obligations relating to 'JMoD confidential' issues. Formerly, such persons could not be prosecuted.[31] Finally, the government can criminally penalise contractors in violation of obligations in all categories of classification: SDSs (top secrets/secrets); MDA Secrets (top secrets/secrets/confidential); and Defence Equipment Confidential (confidential) (see Table 1).

28. For instance, see Jonathan D Caverley, 'United States Hegemony and the New Economics of Defense', *Security Studies* (Vol. 16, No. 4, 2007), pp. 598–614, especially, p. 609.
29. Bōeishō [Japan Ministry of Defence], 'Sōbi Hintō oyobi Ekimu no Chōtatsu ni Okeru Jōhō Sekyuriti Kijun' ['Special Clause for Cybersecurity on Defence Contracts'], April 2022, <https://www.mod.go.jp/atla/cybersecurity/01_kijun_0137_att_r05.pdf>, accessed 13 August 2025; Bōeishō [Japan Ministry of Defence], 'Bōei Sangyō Hozen Manyuaru' ['Defence Industrial Security Manual'], July 2023, <https://www.mod.go.jp/atla/industrialsecurity/files/dism2023_jp.pdf>, accessed 13 August 2025.
30. 'Bōeishō ga Chōtatsusuru Sōbihintō no Kaihatsu oyobi Seisan notame no Kiban no Kyōka nikansuru Hōritsu' ['The Act on Enhancing Defence Production and Technology Bases'] (summary), No. 54 of 2023, <https://www.japaneselawtranslation.go.jp/outline/126/905R639.pdf>, accessed 13 August 2025.
31. This situation was the result of the nature of the clauses included in the JSDF Act. As a result, the only consequence for contractors' violations was the imposition of contractual sanctions. Of course, JSDF personnel who violate the obligation are penalised under the JSDF Act.

Last, but possibly most importantly, in 2020 the JMoD established the Equipment Security Management Division within the Acquisition, Technology, and Logistics Agency. The division was further enlarged in 2023, with its mission specifically dedicated to industrial security and the security clearance of defence contractors. Although this might appear as a minor bureaucratic reorganisation, over the long term, the division will play a key role in developing and supplying experienced information security professionals, or a so-called 'security cadre'.[32] This initiative was important because, without implementation by experienced professionals, information security legislation and security clearance protocols only exist on paper.

To fill these skills gaps, defence contractors may have to consider employing foreign labour. In these instances, PCL will function directly as a precaution against any malicious information theft.

These organisational and procedural updates are becoming ever-more important as the JSDF seeks greater industrial capacity to respond to growing defence requirements as well as advanced dual-use technologies. These demands may call for new entrants into the defence sector, especially in the areas of drones, AI, and space. In a defence-industrial ecosystem with new market entrants, the previously implicit understandings over information security between the JMoD and traditional defence contractors may not function effectively. Hence, for Japan, the explicit standardisation of security protocols has now become an imperative. Moreover, labour shortages – especially of highly skilled labour, just as in the US and Europe – are becoming a serious and disruptive issue in Japan's defence industry. To fill these skills gaps, defence contractors may have to consider employing foreign labour. In these instances, PCL will function directly as a precaution against any malicious information theft.

Standardisation is also important for defence-production cooperation with international partners other than the US. Japan has already launched the GCAP with the UK and Italy, and there will be further cooperation with Australia in the joint production of upgraded Mogami-class multi-mission frigates and joint research on the undersea domain. In such cases, Japan's upgraded information security architecture will catalyse smooth implementation of joint projects. That said, these partners will consider Japan as an equal partner, abiding by similar standards. Japanese policymakers will thus need to keep in mind that any particular information security frameworks created under the US–Japan asymmetrical partnership, and any information issues overlooked within those, may not apply to other partners.

In sum, the standardisation of Japan's industrial information security policy was first triggered by increasing cooperation with the US. However, more recent developments are the result of internal national rationales to improve transparency of procedures for the business community as well as for other international partners.

Cyber Security

Cyber is the last, but certainly not least, of developments in Japan's information security. As noted earlier, the US has long expressed concerns over Japan's cyber security, offering assistance for Tokyo to investigate breaches of its cyber network. Japan has responded by enhancing its cyber capbabilites through increasing budgets and personnel.[33] In 2023, the JMoD established the Joint Cyber Defense Command (JCDC) by restructuring the forerunner Cyber Defense Group that was originally established in 2013. The JCDC is tasked with integrating the cyber defences of the three JSDF services, and with training and coordinating the growth of cyber personnel. The 2022 DBP seeks to increase cyber-trained JSDF personnel to 4,000 by the 2027 fiscal year, and to expand the number of personnel in cyber-related units to 20,000.[34]

32. Jeffrey Bloom, 'The Industrial Security Dilemma: Quest for Substantive Equivalency', International Security Industry Council of Japan, 26 July 2022, <https://isic-japan.org/wp-content/uploads/2021/07/Final-Bloom-Presentation-JP2.pptx.pdf>, accessed 13 August 2025.
33. Paul Kallender and Christopher W Hughes, 'Japan's Emerging Trajectory as a "Cyber-power": From Securitization to Militarization of Cyberspace', *Journal of Strategic Studies* (Vol. 40, No. 1–2, 2017), pp. 118–45.
34. Japan Ministry of Defense, 'Defense Buildup Program', pp. 11–12.

The JSDF has, therefore, been improving its cyber capabilities, at first, incrementally, but now on an accelerating trajectory. Nevertheless, Japan's efforts have certainly not resolved all issues on cyber security. The cyber defence of private networks – especially those of critical infrastructure operators, defence contractors and public R&D agencies – are further major issues that are long overdue for policy attention.

Recent years have witnessed cyberattack incidents on defence-related private organisations. In 2020, Mitsubishi Electric's network was reported as having been compromised by cyber-attacks, with leakages of CUI relating to JMoD's development of hypersonic glide vehicles.[35] In 2023, Japan Aerospace Exploration Agency's cyber infrastructure was breached and some information compromised.[36] Both sets of incidents were reportedly attributed to Chinese hackers. Airlines and financial institutions were also subject to high-profile cyberattacks in 2023 and 2024. These cases demonstrate that even though the JMoD and JSDF have been able to improve their own cyber defences, they have struggled to improve the security of private cyber networks often handling defence-related information.

The JMoD's and JSDF's lack of authority and effective ability to assist organisations outside its immediate networks was due to the absence of any legal basis to conduct offensive cyber operations to neutralise cyberattacks that might necessitate intrusion into private cyber systems and networks. Policymakers had long been reluctant to introduce such measures due to consideration of Article 21 of Japan's Constitution that guarantees the right to the privacy of communications. They were also mindful of statutory regulations that complicate government manipulation of networks to counter hacking.[37] Japan's vulnerabilities and apparent lack of capacity to respond proactively to incidents thus became the source of international doubts over its capacity to protect sensitive information transmitted via cyberspace.[38]

Nonetheless, confronted with an increasing number of cyberattacks, in February 2025 the Japanese government finally submitted a package bill to the National Diet designed to enable the monitoring of suspicious private internet communication and to neutralise cyberattacks on private cyber networks.[39] The Active Cyber Defense Act was approved in May 2025 and is now awaiting enactment. The ACD Act, and related amendments of existing laws, enables the new National Cybersecurity Office (NCO, formerly the National Center of Incident Readiness and Strategy for Cybersecurity) to monitor suspicious activities in private cyber infrastructures, and then for National Police Agency (NPA) and the JSDF to conduct ACD measures to neutralise cyberattacks.

Moreover, for improving threat detection and preparedness for cyber contingencies, Japan still requires closer coordination and communications between the government and private sector. In this respect, the enactment in 2024 of the Act on the Protection and Utilization of Critical Economic Security Information – that seeks to expand the coverage of information security measures to include information on dual-use technologies – should serve as a basis for promoting secure information sharing.[40] This initiative was originally founded on the expectation that creating a security clearance system in this area would increase the opportunities for Japanese companies' participation in international collaborations.

Although the number of international collaborations requiring security clearance beyond defence-related projects may remain relatively limited, the Act undoubtedly contributes to sensitive information sharing on cyber threats between the government and private sector. The Act will further augment Japan's overall cyber security capabilities as it enables greater learning and understanding of ongoing trends in cyberattacks and, thereby, assists preparation for potential future incidents.

35. *Nikkei Shimbun*, 'Shingata Misairu Seinō Rōei ka Mitsubishidenki, Saibā- Kōgeki' ['Possible Leak of New Missile Capabilities – Mitsubishi Electric Targeted in Cyberattack'], 20 May 2020, <https://www.nikkei.com/article/DGXMZO59341910Q0A520C2CR8000/>, accessed 13 August 2025.
36. JAXA, 'JAXA ni Oite Hasseishita Fusei Akusesu ni Yoru Jōhō Rōsetsu ni Tsuite' ['Data Breach Involving Unauthorized Access at JAXA'], 5 July 2024, <https://www.jaxa.jp/press/2024/07/20240705-2_j.html>, accessed 13 August 2025. JAXA is a government-affiliated independent administrative agency focusing on scientific research on space technology often with defence applications.
37. Tomohiko Satake, 'Japan-Australia Security Cooperation: Domestic Barriers to Deeper Ties', Stimson Center, 1 February 2023, <https://www.stimson.org/2023/japan-australia-security-cooperation-domestic-barriers-to-deeper-ties/>, accessed 13 August 2025.
38. William A Stoltz, 'Japan, AUKUS and Cyberwarfare', *The Strategist*, Australian Strategic Policy Institute, 13 May 2024, <https://www.aspistrategist.org.au/japan-aukus-and-cyberwarfare/>, accessed 13 August 2025.
39. Naikaku Kanbō [Cabinet Secretariat], 'Saibā Anzen Hoshō ni Kansuru Torikumi' ['Efforts on Cybersecurity'], <https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html>, accessed 13 August 2025.
40. 'Summary of the Act on the Protection and Utilization of Critical Economic Security Information', 2024, <https://www.japaneselawtranslation.go.jp/outline/127/905R626.pdf>, accessed 13 August 2025.

Conclusion: Future Work for Japan in Information Security

Recent developments in Japan's information security across all three areas outlined indicate a significant shift. There has been a move away from practices within a closed inner circle in the defence community towards a greater government-wide and society-wide standardisation of regulations and a concomitant enhanced level of routinisation and predictability of practices. Japan's shifting practices have been demand-driven in large part by external influences. Closer operational and industrial collaboration with the US and other international partners require Japan to improve the reliability of its security clearance protocols. Further, the need to promote new entrants into the defence-industrial sector requires the Japanese government to enhance the transparency and predictability of its information security policy. In addition, the risk of malicious foreign penetration of information networks has obliged Japan to reinforce its background investigation capabilities. These are necessary for devising security clearance and cyber-defence capabilities. In these respects, the evolution of Japan's information security is a manifestation of its response to the evolving international security environment, and forms a key part of its broader 2022 reforms to strengthen national defence capabilities.

Notwithstanding all these significant shifts and advancements in Japan's information security practices, multiple challenges remain. For instance, while the JMoD is developing information security professionals vested in the Equipment Security Management Division, this resource is not available for other government agencies. This situation has arisen primarily due to Article 12 of the SDS Protection Act. This mandates that each agency is responsible for the background investigation necessary for the security clearance of its own officials and contractors. The US is believed to regard the introduction of a nation-wide background information programme as one of the major areas in which Japan can improve information security practices.[41]

Japan has looked to resolve the problem, in part, through the Act on the Protection and Utilization of Critical Economic Security Information. This Act enables the Cabinet Office to conduct government-wide and centralised background investigations. But as the SDS Protection Act has not yet been amended, individual ministries continue to conduct background investigations for security clearances for handling SDSs. Even though amendments to the SDS Protection Act may be politically sensitive, the Japanese government could still substantially resolve this problem by at least sharing the know-how of JMoD security professionals with other ministries and agencies.

Another issue for resolution is security clearance for politically appointed Cabinet ministers. Currently, ministers and other politically appointed executives can access classified information without obtaining security clearance. This exception risks creating a loophole for information leakage, given that the government has strict security clearance protocols for other employees and contractors. Since these exceptions are explicitly stipulated in laws, the National Diet must consider remedying this potential loophole through amendments to the SDS Protection Act and other statutory acts.

Notwithstanding all these significant shifts and advancements in Japan's information security practices, multiple challenges remain.

41. 'Tokutei Himitsu no Hogo nikansuru Hōritsu' ['Act on the Protection of Specially Designated Secrets'], No. 108 of 2013, <https://www.japaneselawtranslation.go.jp/ja/laws/view/2543#je_ch5at>, accessed 13 August 2025; Bloom, 'The Industrial Security Dilemma'.

Finally, the new ACD Act contains two problems of bureaucratic stove-piping. First, while the NCO is responsible for monitoring private internet communications, the NPA and the JSDF are responsible for neutralising cyberattacks. This division between monitoring and neutralising authorities raises questions over the feasibility of swift responses to cyber incidents. Consequently, the NCO, the NPA and the JSDF must enhance readiness for such incidents through seamless information sharing across government.

Second, the NPA is designated as the primary actor for operations to neutralise cyber-attacks on private cyber systems. The JSDF, in line with the new Article 81 of the JSDF Act, can only join such operations following requests from the NPA and orders from the prime minister. This strict division might mean failing to promptly exploit the JSDF's resources in cyber-defence. Hence, the Japanese government, as a stopgap measure, may consider issuing pre-designated authority to the JSDF to undertake ACD measures against cyberattacks on defence-related private cyber infrastructure, such as that of defence contractors.

Japan's information security architecture and practices, since their initial creation in the immediate post-war period, have a long history and were often refashioned to address issues resulting from changing security environments. As a result, established and newer information security architectures co-exist in a patchwork form. These represent Japan's flexible and pragmatic responses given the often-challenging domestic political constraints on launching more wholesale changes. But at the same time, Japan's information security practices still require constant review and future updates to better deal with newly arising security challenges. ■

Hirohito Ogi is Senior Research Fellow at the Institute of Geoeconomics, International House of Japan. His recent works include 'The Origins of Japan's Arms Export Prohibition', Asia Policy (Vol. 20, No.1, January 2025), pp. 135–155.

Christopher W Hughes is Professor of International Politics and Japanese Studies, University of Warwick. His latest book is Japan as a Global Miltary Power: New Capabiliteis, Alliance Integration, Bilateralism-Plus (Cambridge University Press, 2022).