Hudson Institute

Closing the Defense Industrial Security Gap with Japan

防衛産業のセキュリティー・ギャップへの対応

Dr. Arthur Herman
Senior Fellow

July 2018
Conference Report

Hudson Institute

Closing the Defense Industrial Security Gap with Japan

防衛産業のセキュリティー・ギャップへの対応

Dr. Arthur Herman
Senior Fellow

For more information about obtaining additional copies of this or other Hudson Institute publications, please visit Hudson's website, www.hudson.org

Hudson Institute would like to thank Northrop Grumman Corporation, Lockheed Martin Corporation, White & Case LLC, The Boeing Company, and the Japanese External Trade Organization for their generous support.

ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit **www.hudson.org** for more information.

Hudson Institute
1201 Pennsylvania Avenue,
N.W. Suite 400
Washington, D.C. 20004

P: 202.974.2400
info@hudson.org
www.hudson.org

Table of Contents

Executive Summary and Overview

The Hudson Institute organized a series of workshops, one in Washington DC on March 23, and two in Tokyo May 21-2, under the title "Closing the Defense Industrial Security Gap with Japan."

The conversations that arose from those workshops brought good news for Japan on the industrial security front, and for the U.S.-Japan alliance: that what has been a sometime contentious issue in the recent past, may be able to move forward to a resolution that satisfies both countries.

These workshops (which included more than fifty industrial security professionals, industry executives, and senior government officials from both Japan and the United States) offered an unprecedented forum for discussing two key issues:

> 1.) How the government of Japan can continue to close the perceived gap in industrial security (IS) between Japan and the U.S. and its allies.
>
> 2.) How the U.S. can help to incentivize Japan to improve its industrial security through efforts that will strengthen the alliance and benefit the U.S. defense security in future—even making the alliance stronger than it has been in more than seventy years.

Indeed, it is possible that rapid and significant progress on this issue could open the way for a major milestone in the US-Japan alliance: Japan's admission into the exclusive "Five Eyes" club for permanent intelligence-sharing.

The Five Eyes is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. All are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence dating back to World War II. [1]

While the Five Eyes alliance has had no new members for more than seventy years, many feel Japan would be the leading candidate for a Sixth Eye—especially if Japan's IS standards were raised to the level of other Five Eye members.

For now, it is widely recognized that unlike other Five Eye countries, and many NATO countries, the government of Japan still lacks a comprehensive defense industrial security program that applies and enforces universal security standards to Japanese government and Japanese industry. Although Japan has made great strides in this area, especially since 2007 when it signed a landmark General Security of Military Information Agreement (GSOMIA) with the U.S., there remains a significant industrial security gap between Japan and its most important allies.[2]

---

[1] Cox, James "Canada and the Five Eyes Intelligence Community" (PDF). Canadian Defence and Foreign Affairs Institute. (December 2012).

[2] Col. Hiroaki Uchikura, "U.S.-Japan Interoperability" (statement, Defense Challenges and Future

The good news is that although there is still work to be done, Japan is on the road to making interoperability, advanced technology transfers, and defense industrial cooperation with the U.S a reality—which will make the alliance stronger now and in the future.

For example, the government of Japan has adopted a standard for protecting classified information under its Secrets Protection Act. It is also currently adopting the information security protocols developed by the Ministry of Economy, Technology, and Industry (METI) in 2017 as a government-wide standard; while METI, Japanese Ministry of Defense (JMOD), ATLA, and other agencies are working together to implement both of those standards in their areas of jurisdiction.

Overall, Japan is achieving what can be called the "silver standard" in IS in all areas. Participants in the Hudson conferences agreed that it must now strive to reach the "gold standard" as defined by the Defense Technology Security Administration's (DTSA) International Security Directorate, which carries out the responsibilities of the Secretary of Defense for U. S. national policy governing the disclosure of classified military information (CMI) and material to foreign governments and international organizations under the National Disclosure Policy (NDP-1), and which is responsible for the development and negotiation of security arrangements with allied and other friendly governments. Those standards are in turn those which U.S. companies must meet under the National Industrial Security Program as defined by the National Industrial Security Program Operating Manual (NISPOM).

Meeting this standard is necessary because for U.S.-Japan defense industrial cooperation to continue forward, the U.S. will require a "secure landing zone" for sharing technology and sharing classified information. Right now with U.S. help, Japan is successfully protecting U.S. technology in joint programs such as the F-35 Joint Strike Fighter and the SM3 Block IIA anti-ballistic missile. The gold standard will be where Japan is able to implement a rigorous IS regime on its own as a matter of law and practice; the "equivalence" standard other U.S. allies currently have to meet (see Section III).

For example, for protecting indigenous technology, Japan's existing system (or rather, systems) for implementing IS still have a long way to go. This becomes a problem for the U.S., as well, since if Japanese technology is vulnerable to theft or espionage, then so is any U.S. technology that incorporates that Japanese technology.

In addition, there is the issue of personnel security (see Section V). Nearly all Japanese participants in the Hudson conferences acknowledged that Japan still has a long road ahead to create a systematic and consistent system of screening current and potential employees of companies handling defense and defense-related technologies, articles, and information, including classified information (not that the US system is perfect, as cases such as Edward Snowden and Chelsea Manning demonstrate). Further, the government of Japan's efforts to create effective national standards for cybersecurity—an essential

Opportunities event at Brookings, Washington, D.C., March 26, 2010).

ingredient in today's IS regimes—still lag behind those of allies such as the U.S. The cybertheft raid in January of this year, when hackers stole almost $500 million in cryptocurrencies from Coincheck, a Tokyo-based cryptocurrency exchange, strongly indicates that there is much to improve in the private as well as public sector.

Yet overall, it is abundantly clear today that the Japanese government understands what is at stake, and is working to close the remaining gaps. It is true that Japanese industry still needs help addressing key IS issues, although most Japanese companies have effective systems for protecting their intellectual property rights (IPR) and proprietary information. On the other hand, Japanese industry may hold the key to unlock the issues regarding personnel screening, and may have an important opportunity to establish a "best practices model" for personnel security that the government can embrace (see Section V).

What are the next steps for Japan in order to achieve that IS "gold standard"? Such a standard will not only give Japan the same access to the U.S.'s most advanced defense technologies like allies such as Great Britain, Australia, and Canada, but also make possible the new level of interoperability both countries have pledged to achieve in their 2015 Security Guidelines.

Four issues stand out:

> **First**, addressing the personnel security issue by developing uniform standard for screening personnel and handling classified information that will apply to both government and industry.
>
> **Second**, creating a single authority to oversee the government of Japan's IS rules and protocols in both government and industry, that answers directly to the Office of the Prime Minister, the National Security Council, and the Cabinet.
>
> **Third,** establishing a Japanese version of the U.S. Defense Security Service (DSS) with a trained professional IS cadre to implement and enforce the same IS rules and protocols (for details, see Section V).
>
> **Fourth**, raising cybersecurity standards in both government and industry through a rigorous interagency consultation progress, that includes the Ministry of Defense (JMOD), METI, National Center of Incident Readiness and Strategy for Cybersecurity(NISC), and other agencies in order to develop information security procedures that will support a modern IS regime.

There are important ways the U.S. can help, as well.

The first is to encourage the government of Japan to consider joint efforts in IS such as the Bilateral Information Security Conversations (BISC—see Section II) and the F-35 Joint Strike Fighter program between Lockheed Martin and Mitsubishi Heavy Industry, as stepping stones to developing an indigenous system for complex 'made in Japan" defense equipment such as the Future Fighter Program—a system that achieves "equivalence" without the need for U.S. help or oversight.

The second would be to progressively ease export controls for Japan under the International Traffic in Arms Regulations (ITAR) in response to demonstrative improvements in Japan's IS regime.

The third, and most important, would be to incentivize a Japanese surge in IS improvement by offering U.S. help to add Japan as a full member in the Five Eyes intelligence-sharing alliance, along with the UK, Australia, Canada, and New Zealand. Achieving status as "the Sixth Eye" would not only be a landmark for Japan; but for the U.S.-Japan alliance and the special relationship.

As Section VI of this report explains, a major step in achieving this Sixth Eye status would be incorporating Japan as part of the National Technology and Industrial Base (NTIB), alongside other Five Eye members UK, Australia, and Canada. Japan would swiftly become a major factor in the Pentagon's goal to build a global supply chain to undergird the U.S.'s defense industrial base; while becoming part of NTIB would also open the way for Japan to begin direct investment in the U.S. defense sector.

Becoming part of NTIB would, however, entail major advances in Japan's IS efforts—advances that match the equivalence standards of UK, Canada, and the other Five Eyes. Those advances could also clear the way for formal consideration for Sixth Eye status: an accomplishment that any Japanese prime minister would consider a major legacy.

In the final analysis, then, closing the IS gap offers powerful opportunities for Japan, and not only in the defense sector. As Section VII will reveal, Japan could take the lead in creating new ways to conduct IS by incorporating advanced technologies such as big data analytics, artificial intelligence, and robotics.

Japan could extend its global competitiveness and become the "best practices model" for the rest of Asia, including South Korea and India, in how to achieve an effective IS regime.

At the same time, there are important risks in failing to achieve the "gold standard" that is already within Japan's reach, and only requires increased focus and consistent leadership to acquire.

Japan would be losing out on full access to future technological cooperation with the U.S., e.g. the E2D Hawkeye early warning radar aircraft Global Hawk unmanned aerial vehicle, and ballistic missile defense systems at a time when the Pentagon is looking to boost exports to allies. Other ramifications include delaying reaching interoperability standards essential for strengthening security in a rapidly evolving security environment and vulnerability of Japan's own indigenous advanced systems, like the Future Fighter program.

Meanwhile, as numerous workshop participants noted, South Korea has rapidly made impressive strides to improve its IS ecosystem and is waiting in the wings to be the U.S.'s leading Asian partner in developing and producing advanced systems.

In industrial security reform, as in most of politics, timing and leadership is primary, particularly leadership from the top. But in IS, perception is also reality. No matter how

much progress Japan is actually making toward closing the defense industry security gap, as long as it is *perceived* as not taking important and serious steps toward IS reform, the U.S. and other allies will be reluctant to share their classified and most sensitive data and technology with an otherwise valued and trusted ally.

Therefore, this report concludes by suggesting five concrete steps the government of Japan can take to change perceptions and light the way toward lasting IS reform.

- Designate industrial security reform as an integral part of Japan's national strategy in the 5-year Mid-Term Defense Program, and the 10-year National Defense Program Guidelines.

- Establish funding in the FY2019 defense budget for a feasibility study on creation of a Japanese defense security service, including training, staffing, and integrating information and personnel security practices and procedures for protecting advanced technology.

- Establish funding for and creation of an interagency industrial security working group, to examine the steps needed to create a unified industrial security program that can regulate and oversee both government and industry.

- Require Japan's defense industry to establish an Information Sharing and Analysis Center (ISAC) for sharing data regarding cyberattacks and hacks, which will also be shared with agencies responsible for industrial security.

- Continue and extend cooperation with the U.S. in key areas of industrial security including the Bilateral Information Security Cooperation discussions (BISC), and the F-35 joint strike fighter program under Foreign Military Sales (FMS), as pathways to formulating the general rules and regulations for Japan's future government-led industrial security program.

There are also two important steps the United States can take today to encourage Japan along this path.

- Suggest extending and expanding the BISC meetings on a more frequent basis and at a higher official level, e.g. at a Cabinet level, so that both countries will see these consultations as constructive steps toward a permanent "made in Japan" IS regime.

- Begin consultations on the steps necessary to make Japan one of the countries included in the Pentagon's NTIB, so that Japan's IS reform effort leads toward a systematic expansion of Japanese industry's role as part of the U.S. global supply chain for defense and defense-related articles and technologies.

Introduction

"What is the state of your industrial security program?"

That is the question being posed more and more during informed discussions about defense trade, particularly given today's global marketplace of defense articles and defense-related technologies.

What is the state of your industrial security? How do we, as an ally, know trusted people are safely handling information sensitive to our national security? How do we know industrial facilities and research laboratories are secure from hostile interests or vindictive employees? How can we be sure intellectual property is protected—not only ours but your own? How robust and resilient are the cybersecurity programs of your defense-related companies large and small, and of your government—and are they aware of each other's efforts and standards? And if security leaks, can we be sure you will inform us on a timely basis and correct the problem?

These are the questions that haunt today's defense market place—and they have become increasingly acute for the government of Japan. It is widely recognized that Japan lacks a strong comprehensive IS program both in government and in industry.

Fortunately, the problem is far from insoluble. Today there are multiple efforts by multiple Japanese government agencies, including the Ministry of Defense's Acquisition Technology and Logistics Agency (ATLA), the National Center of Incident Readiness and Strategy for Cybersecurity NCIRSC), METI, and the Cabinet Intelligence Research Office (CRIO). JMOD's defense contractors already must comply with the provisions of the Special Designated Secrets Act, and the Japanese government has created an interagency uniform secret classification system in accordance to the same act. In addition, an effort is now underway to use the 2017 METI guidelines as a template for development of a future Japanese version of NISPOM—the document that oversees US's own industrial security procedures.

Nor from an historical point of view is Japan the only example of a country that has had to rapidly make up ground on the IS front. In the early 1980s, the U.S. faced enormous challenges when its NATO allies lost technology to the Soviets, endangering the future of the alliance (it was the need to monitor and deter critical technology transfers to the Soviets that led to the creation of DTSA itself). A decade later, thanks to U.S. encouragement and cooperation, the situation had changed and an important level of security equivalence had been achieved which has lasted until today— and which has been a foundation of U.S.-NATO defense industrial cooperation ever since.

A similar success story has been South Korea, where with U.S. help and encouragement the Seoul government has been able to transform Korea's IS ecosystem from negative to positive in a relatively short time.

By starting with a strong comprehensive program that covers defense contractors within the purview of JMOD and ATLA, Japan can create IS protocols and mechanisms for application that can be expanded into a broad interagency approach.

Furthermore, it is imperative that the United States help Japan close this gap because the future of the alliance's technology sharing, defense trade, and industrial cooperation hinges on it—as well as the future security of the region.

Japan's Forward Progress

As noted, Japan's progress in creating the bureaucratic foundations for comprehensive IS has been steady and ongoing. For example, steps have been taken since the 1950s which include:

The Treaty of Mutual Cooperation and Security between the United States and Japan, January 1954.

The Mutual Security Assistance Pact initially involved a military aid program that provided for Japan's acquisition of funds, materiel, and services for the nation's essential defense. Although Japan no longer received any aid from the United States by the 1960s, the agreement continued to serve as the basis for purchase and licensing agreements ensuring interoperability of the two nations' weapons and for the release of classified data to Japan, including both international intelligence reports and classified technical information, as well as defense equipment-related secrets provided by the U.S. government.

Signing of General Security of Military Information Act (GSOMIA) between the U.S. and Japan, August 2007.

The GSOMIA is an agreement between both governments to protect classified military information that may be exchanged. It is not an agreement to compel the parties to share information; rather it is an agreement to protect shared classified information in a manner that provides substantially the same degree of security protection as that provided by the originating government.

Basic tenets of the agreement include: establishing a system for handling classified military information (CMI) in the Japanese government that correspond with U.S. classifications (Article 4);[3] defining principles for protecting that information including from third parties (Article 6),[4] decreeing that "access to CMI shall be granted only to those government officials whose official duties require such access and who have been granted a personnel security clearance,"; and granting of that security clearance be implemented "consistent with national security" (Article 7).[5] The agreement also established procedures for securing facilities where CMI is kept and for secure transmission, destruction, reproduction, and transmission of CMI (Articles 10- 15), as well as "appropriate measures" for release of CMI to contractors (Article 16). [6][7]

---

[3] 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, 2007, art. 4, available at http://www.mofa.go.jp/region/n-america/us/security/agree0708.html.
[4] 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, 2007, art. 6.
[5] 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, 2007, art. 7.
[6] 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, 2007, art. 10-15.
[7] Agreement Between the Government of Japan and the Government of the United States of America

Bilateral Information Security Consultations, May 2007.

Created by a U.S.-Japan 2+2 meeting in Tokyo in 2007, the Bilateral Information Security Consultations (BISC) are an ongoing mechanism for sharing and protecting sensitive information between the U.S. and Japan, and is attended by both U.S. and Japanese officials.

BISC meetings feature attendance by officials from a number of agencies led by Defense and State Departments on the American side, and JMOD/ATLA, CIRO, MOFA, METI, and National Police Agency (NPA) officials on the Japanese side. As a bilateral framework, BISC consists of a plenary gathering at the deputy assistant secretary and deputy director general level, with inter-sessional meetings at the office director level which are designed to address and resolve information security challenges.

The ultimate BISC goal is for the U.S. and Japanese governments to share information security best practices in key areas of physical security, personnel security, counterintelligence, cyber security, industrial security, and establishment of whole-of-government security policies, practices and procedures.

In successive bilateral engagements such as the Security Consultative Committee (2+2) and POTUS-Prime Ministerial summits, the U.S. and Japan have committed to BISC goals as the foundation of future alliance cooperation in consideration of sharing advanced defense systems and technologies as well as classified information, intelligence, and capabilities.

The Secrets Protection Act, October 2013.

As passed by the Japanese Diet, the Secrets Protection Act allows the Japanese government to designate non-military defense and other sensitive information as "specially designated secrets" protected from public disclosure (these are information and/or data requiring secrecy due to the risk of causing severe damage to Japan's national security if disclosed without authorization). The Act also made the Japanese government responsible for classifying national security-related information, and establishing a security clearance process— both major steps toward closing the IS gap.

The Act decrees that access to "specially designated secrets" (SDS) shall be limited to government personnel; employees of contractors with the Government of Japan; and those prefectural police officers who, following the security clearance process, are identified as not liable to engage in unauthorized disclosure of SDS.[8]

In addition, the Secrets Protection Act decreed that unauthorized disclosure of SDS by those authorized to handle SDS, whether by accident or by intention, be subject to legal punishment. In the case of intentional disclosure, the punishment is to be not more than 10 years' imprisonment;[9] in the case of negligence, imprisonment is to be for not more

Concerning Security Measures for the Protection of Classified Military Information, 2007, art. 16.
[8] Act on the Protection of Jointly Designated Secrets, Act No. 108 of December 13, 2013, art. 5, para. 1-6.
[9] Act on the Protection of Jointly Designated Secrets, Act No. 108 of December 13, 2013, art. 23, para. 1.

than 2 years or a fine of not more than 500,000 yen.[10]

As for those knowingly receiving SDS from an authorized person, the punishment is imprisonment for not more than 5 years.[11] If that acquisition was done to serve the interest of a foreign country, i.e. as an act of espionage, imprisonment to be not more than 10 years.[12]

Originally proposed by the Prime Minister Abe cabinet, the Secrets Protection Act was approved by the Security Council on October 25, 2013, and then submitted to the National Diet where it was approved and then promulgated on December 13, 2013, coming into force one year later.

Revised U.S.-Japan Security Guidelines, April 2015.

The joint statement of the Security Consultative Committee made up of U.S. and Japanese officials "affirmed the importance of enhanced information security cooperation as reflected by continued progress through the Bilateral Information Security Consultations and by Japan's implementation of the Act on the Protection of Specially Designated Secrets."[13]

In addition, Article VII on Bilateral Enterprise states, "In order to enhance interoperability and to promote efficient acquisition and maintenance, the two governments will:

- cooperate in joint research, development, production, and test and evaluation of equipment and in mutual provision of components of common equipment and services;

- facilitate reciprocal defense procurement to enhance efficient acquisition, interoperability, and defense equipment and technology cooperation; and

- explore opportunities for cooperation with partners on defense equipment and technology."[14]

All these provisions imply a major joint effort on industrial security, as part of the equal partnership status laid out in the 2015 guidelines.

"The Guideline for Safeguarding Technology Information," prepared by METI, April 2017.

This document "provides standardized, concrete instructions for the Japanese manufacturing industry with regards to safeguarding technology information from

[10] Act on the Protection of Jointly Designated Secrets, Act No. 108 of December 13, 2013, art. 23, para. 4.
[11] Act on the Protection of Jointly Designated Secrets, Act No. 108 of December 13, 2013, art. 23, para. 2.
[12] Act on the Protection of Jointly Designated Secrets, Act No. 108 of December 13, 2013, art. 24, para. 1.
[13] "Joint Statement of the Security Consultative Committee," Japanese Ministry of Defense, April 27, 2015, http://www.mod.go.jp/e/d_act/anpo/js20150427e.html.
[14] "Joint Statement of the Security Consultative Committee," Japanese Ministry of Defense, April 27, 2015, http://www.mod.go.jp/e/d_act/anpo/js20150427e.html.

unauthorized access or disclosure," including sections on:

- Controlling access to technology information
- Security training of employees
- Reporting system "to grasp signs of information leakage"
- Information management of each process
- Cybersecurity

Joint Statement of the Security Consultative Committee, August 2017.

This statement reaffirmed the commitment from the 2015 Guidelines to "intelligence cooperation and information security," including "deepening consultations in a timely manner on Alliance responses to serious cyber incidents."[15]

Digital Nippon 2017: Special Mission Committee on IT Strategy, Liberal Democratic Party's Policy Research Council, May 2017.[16]

Noting that "Japanese private companies cannot access cyber incident information of other countries due to its lack of a security clearance system," the Special Mission Committee recommended that Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NCIRSC) create security clearance guidelines for certain sensitive government information, and that Japan create a "Japanese FedRAMP" cloud that meets international technological standards of cybersecurity, based on U.S. NIST standards under SP800-53, for USG cloud procurement.

The Committee also noted: "Without a security clearance system in place, Japan is in danger of losing out" to international competitors in the cybersecurity sphere, especially the U.S. and EU.

Amendment of the Industrial Competitiveness Enhancement Act, May 2018.

On May 16, 2018 the Diet added new provisions to the original 2013 act which will set security standards applicable for any businesses based on METI's impending decree on those standards which is expected later this year. By the terms of the measure any company demonstrating conformity with those standards, will be able to apply for government certification by a government-designated certifying body, also created by the terms of the act.

---

[15] "Joint Statement of the Security Consultative Committee," U.S. Department of State, August 17, 2017, https://www.state.gov/r/pa/prs/ps/2017/08/273504.htm.

[16] Special Mission Committee on IT Strategy, Liberal Democratic Party's Policy Research Council. "Digital Nippon 2017." May 23, 2017. https://www.hirataku.com/wp-content/uploads/2017/05/デジタルニッポン20171.pdf.

Nonetheless, four areas of challenges remain.

- Personnel security, where the government of Japan is still working to develop a uniform system for both government and industry;
- Uniform standards of classification of information at the governmental and industry levels;
- Formation of an IS professional cadre;
- Conflicting timelines between the U.S. and Japan, where the U.S. sees closing the IS gap as a more urgent issue given the rising threat from China, whereas Japan's timeline involves less urgency and a more methodical and deliberate pace on IS reform.

For all these reasons, the resulting IS gap is why U.S. government agencies like the Defense Technology Security Administration's (DTSA) International Security Programs Directorate, has had to play an essential role in helping Japan develop the policies, practices, and procedures for effective information and technology security programs for more than a decade; and why an American company, Lockheed Martin, has taken the lead in administering the IS protocols for the F-35 Joint Strike Fighter co-production program (see Section IV, below).

This gap has limited the incentive of U.S. defense companies to work with Japanese counterparts, including commercial companies, since the lack of a reliable industrial security regime makes co-development and co-production with Japan on new defense articles and technologies a formidable challenge. Such gaps will also increasingly act as a brake on U.S. technology sharing and information sharing with Japan, which will severely limit Japan's ability to interoperate in an alliance environment dominated by U.S.-built and U.S.-led technologies.

The key concept for closing the gap is "equivalence," which means that the government of Japan must achieve an agreed standard of protection similar to the U.S. in IS, even if it's achieved by methods different from the ones used by the U.S. and other allies.

Defining Equivalence

The 2007 GSOMIA signed between the U.S. and Japan, Article 6 (b), required Japan to "take appropriate measures to provide to the CMI a degree of protection substantially equivalent to that afforded by the releasing Party," namely the United States.[17]

In terms of defense trade with the U.S., IS equivalence is essential for enabling information and technology-sharing, and not just in the case of Japan.

This issue arose, for example, in the 1980's when the U.S. needed to protect classified information from the Soviets, especially concerning new advanced weapons systems, at a time when defense companies belonging to NATO allies such as Germany and France were extremely vulnerable to Soviet penetration. This made the U.S. deeply reluctant to share the latest defense technologies until it ultimately mobilized the Coordinating Committee for Multilateral Export Controls (CoCoM) to oversee the process.

Formed in 1949, CoCoM was originally a nontreaty organization of the NATO nations (except Iceland and with the addition of Japan) that set rules on exports of strategic goods to Communist countries. In the 1980's, it expanded its reach to include advanced technologies such as GPS. Even today the term "CoCoM Limits" refers to a limit placed on GPS tracking devices that disables tracking when the device calculates that it is moving faster than 1,000 knots (1,900 km/h; 1,200 mph) at an altitude higher than 18,000 m (59,000 ft). This was intended to prevent the use of GPS in intercontinental ballistic missile-like applications.[18]

Supervision by CoCoM proved effective for three reasons. The first was that it was made up of not only NATO members but other countries which had the capability to produce technologies similar to those controlled by NATO. This served to strengthen a dependable supply chain, as well as to provide security for defense articles.

Second, CoCoM began its oversight by showing NATO countries what they were losing thanks to technology being leaked or stolen by the Soviets. This made countries such as France, which already had an active arms export trade, realize that cooperating with the U.S. and CoCoM would not only strengthen the alliance but would also protect the future of France's export markets.

Third, the meetings of CoCoM embraced the concept of equivalence, i.e. arriving at an agreed standard of protection in security terms even if it's achieved by different methods. This allowed individual countries to design their own export control programs, rather than simply copying the U.S. model—and it enabled them to avoid having U.S. officials

---

[17] "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." Section 6, b. General Security of Military Information Agreement (GSOMIA), 2007. https://www.mofa.go.jp/region/n-america/us/security/agree0708.html.

[18] "COCOM GPS Tracking Limits," Ravtrack, accessed May 9, 2018, http://ravtrack.com/GPStracking/cocom-gps- tracking-limits/469/.

supervise the export control process in order to meet U.S. standards.

Both these last two aspects of the CoCoM precedent should have considerable resonance in the Japanese case, where the government can look for ways to pursue an "equivalence" standard that brings the same result through different "made in Japan" methods—for example in ways that bring a proactive, rather than reactive, approach to the entire issue of IS.

For example, America's defense industrial security system rests on a single (albeit hefty) document: the National Industrial Security Program Operating Manual (NISPOM). NISPOM establishes procedures for companies involved in Department of Defense contracts requiring access to classified information. This comprehensive document applies IS protocols to both government and contractor facilities, and is constantly revised and regularly updated (the most recent revision was issued on May 7, 2018).[19]

If there is to be "a NISPOM with 'Japanese characteristics,'" as some are arguing and of the kind that ATLA is working to achieve using the 2017 METI guidelines as a template, a comprehensive IS system that reaches an equivalence "gold standard" must undertake the following tasks:

- create a universally applied security classification system;
- build a security and legal framework that protects the IP of its own companies and those of allies;
- implement an aggressive cybersecurity program of which the current effort to adhere to the standards laid out in NIST 800 171 is only a start;
- establish a security service that regularly inspects facilities and clears new companies and reviews current companies in IS;
- systematically trains IS professionals in both government and industry, from security service officers and cyber security experts to managers and executives who understand security risk management.
- oversees export controls of defense and defense-related technologies, including dual-use technologies, in coordination with the Ministry of Economy, Technology, and Industry (METI), which has formal authority over Japanese exports, as well as the Ministry of Foreign Affairs (MOFA).

At the same time, Japan's IS regime will also have to measure up to today's international security standards, as maintained by the U.S. and its other allies, an issue subsumed under the term "equivalence"—as well as meet or even surpass the standards of tomorrow.

Additionally, creating an "equivalent" system does not mean merely copying the U.S.

[19] U.S. Department of Defense, National Industrial Security Program Operating Manual (Washington, D.C., 2006), https://fas.org/sgp/library/nispom/nispom2006.pdf.

system, let alone the NISPOM—or the industrial security system of any other country. The key will be leveraging the advantages already embedded in Japanese government, industry, and society, to create a system that achieves the same result through its own unique method.

The imperatives for the government of Japan to aggressively undertake this task are three-fold.

First, a strong IS regime will provide robust protection of Japanese IP and technologies generally, and incidentally the data and technologies of allies in the defense realm. Severe external threats to Japan's integrity as a high-tech industrial nation exist today in the commercial and defense realms. Therefore, strong protections in the commercial realm will work very effectively and provide a firm foundation for security in the defense realm.

Second, a robust IS system will encourage future co-development with the U.S. and other allies of advanced systems, in which Japanese companies and technologies are destined to play a key, even a leadership, role.

Third, the future of the U.S.-Japan alliance will find it difficult to break new ground until the IS issue is definitively resolved. Relying on the U.S. to set the standard and implement effective policies is neither efficient nor desirable. The 2015 Security Guidelines have set up an equal partnership for forthcoming advanced capabilities, which will demand a higher level of cooperation than ever, including in industrial security.[20]

At the same time, many participants in the Washington and Tokyo workshops voiced the view that achieving "equivalence" might be setting the bar for Japan too low. If the U.S. encourages Japan merely to emulate the U.S. IS system, Japan might miss opportunities to devise and staff a system that *exceeds* the U.S. industrial security system. More than one participant pointed out that today's U.S. NISPOM embodies protocols stemming from the industrial age while today we find ourselves in the information age, when advanced technology such will not only be the objects of IS regulation, but become powerful tools to build a modern IS system.

Hence, flexible risk management and enhanced due diligence supported by advanced technology becomes a key way to think about how to devise an effective IS regime with Japanese characteristics.

Are there points of entry for Japan already where an effective IS can begin to take shape? And what role can the U.S. play in providing support?

[20] Japan Ministry of Defense and U.S. Department of Defense, Guidelines for Japan-U.S. Defense Cooperation (2015), http://www.mod.go.jp/e/d_act/anpo/shishin_20150427e.html.

What is America's Role?

The Hudson Institute conference consensus was that the U.S. has an important role to play in encouraging Japanese government and companies to taking control of their own IS ecosystem, and to construct a future "made in Japan" system that is of equivalence with U.S. standards and those of allies. The United States is doing this already, both through cooperative programs and by example.

F-35 Joint Strike Fighter Program

For example, an important and highly successful benchmark in U.S.-Japanese cooperation on IS has been the F-35 Joint Strike Fighter program, in which the prime contractor Lockheed Martin partnered with a Japanese subcontractor, Mitsubishi Heavy Industries, for co-production. MHI has provided the facilities, capital, infrastructure, and workforce, while Lockheed Martin provides tooling, equipment, training, and information and industrial security.

On June 5, 2017, MHI was able to roll out its first domestically built F-35A Joint Strike Fighter from its Komaki South F-35 Final Assembly and Check Out (FACO) facility.[21] During the co-production process, Lockheed Martin and MHI worked together to establish "equivalency" rules and procedures for IS that officials and executives from both countries consider an impressive success. The cooperation in the F-35 program, in short, offers a tantalizing possibility of extending those rules and procedures into a set of general principles that Japan can adapt as part of an indigenous IS program.

The Bilateral Information Security Consultations (BISC)

As noted above, since 2007, the Bilateral Information Security Consultations (BISC) between the U.S. and Japanese government feature regular meetings between officials from the U.S. and Japan. The meetings are led by Defense and State Departments on the American side, and JMOD, MOFA, METI, and NPA officials on the Japanese side in order to strengthen and deepen overall alliance security cooperation, information sharing, and advanced defense equipment and technology transfer.

One measure of the effectiveness of the BISC process was Japan's passage of the 2013 Act on the Protection of Specially Designated Secrets as a critical foundational law to safeguard classified national security information in the key areas of defense, diplomacy, counter-intelligence and counter-terrorism. Other examples could follow.

Although limited in its authority and scope, an expanded version of BISC that includes a support staff working fulltime on IS issues could assume many responsibilities for advancing Japan toward equivalence standards in IS via an established interagency, inter-ministerial process.

---

[21] Kyodo Jiji, "Mitsubishi Heavy unveils first F-35 stealth fighter assembled in Japan," Japan Times, June 5, 2017, https://www.japantimes.co.jp/news/2017/06/05/business/mitsubishi-heavy-unveils-first-f-35-stealth-fighter- assembled-japan/#.WvMQwWNgGQ0.

National Industrial Security Program (NISP) and NISPOM

In the case of America's own defense industrial security system, a 1993 executive order (12829) created the National Industrial Security Program (NISP), with the president designating the Secretary of Defense as the program's executive agent, and the National Security Council having overall policy direction.[22] An interagency division of labor underlies the program. So while the Secretary of Energy and Nuclear Regulatory Commission are responsible for administering that part of the program that is covered by the Atomic Energy Act of 1954, and the Director of National Intelligence "is responsible for those portions of the NISPOM that pertain to intelligence sources and methods, ultimately the Secretary of Defense remains "the Executive Agent for inspecting and monitoring contractors, licensees, grantees, and certificate holders," which "applies to almost all Executive Branch Departments and Agencies and to all created contractor facilities within the United States and its territories."[23]

In the Japanese case, it would not be difficult to see a similar executive agent role exercised by the Minister of Defense in coordination with other agencies such as intelligence (the Defense Intelligence Headquarters, Public Security Intelligence Agency (PSIA), and National Police Agency Security Bureau (NPASB)) and export control (METI and MOFA). Additionally, Japan's National Security Council might assume overall policy direction for a Japanese IS program that applies to all government agencies and all contractor facilities, and their licensees and employees.

The Defense Security Service (DSS)

Another important place where Japan can look to the United States for a best practices model is the agency tasked with overseeing and enforcing NISP: the U.S.'s Defense Security Service (DSS).

Today the DSS provides the U.S. military services, defense agencies, non-defense federal agencies and approximately 13,500 cleared contractor facilities, with security support services.[24] Its principal job is serving as the security interface between the government and cleared industry.

DSS also determines the eligibility of industry personnel for interim clearances (and will transition no later than October 1, 2020 to handling the majority of industry clearance investigations and eligibility decisions) and legal entity facilities for access to classified information; adjudicates interim personnel clearances requests for cleared contractors; and provides security assurances on U.S. contractor facilities and individuals to foreign governments. It also validates clearance information for visit authorizations from U.S.

---

[22] "Executive Order 12829 of January 6, 1993, National Industrial Security Program, as amended by Executive Order 12885, December 16, 1993," Code of Federal Regulations, title 3 (1993), https://www.archives.gov/isoo/policy-documents/eo-12829.html.
[23] U.S. Department of Defense, National Industrial Security Program Operating Manual (Washington, D.C., 2006), Chapter 1, section 1, https://fas.org/sgp/library/nispom/nispom2006.pdf.
[24] "About Us," U.S. Department of Defense, Defense Security Service, accessed May 9, 2018, http://www.dss.mil/about_dss/index.html.

contractors in foreign locations.

In addition, DSS personnel oversee U.S. contractor compliance with security provisions of international classified contracts and agreements, and handle foreign ownership, control or influence (FOCI) issues for U.S. cleared companies that become foreign owned and/or controlled.

Finally, DSS has oversight responsibility for plant visits by foreign nationals involving classified information and provides interpretations and guidance on NISPOM, while also overseeing the majority of cleared industry's compliance with the NISPOM.

In clearing companies, DSS requires sponsorship by another cleared company, a U.S. agency, cleared foreign entity, or foreign agency in limited cases. DSS makes sure it's a legitimate sponsorship, then does a risk analysis by asking: Is this company a trustworthy entity?

After examining databases and other informing factors, DSS arrives at a judgement. In order to be deemed trustworthy, DSS conducts an evaluation of the company's facility clearance application and ensures that key management personnel, obtain security clearances at the level of the entity's impending security classification. Upon a successful review, that company then receives a Facility Security Clearance (FCL). However, if DSS finds derogatory information or security issues during periodic reviews, it will tell the government sponsor or the applicable prime contractor sponsor's government customer. The government customer or government sponsor then determines whether to support the sponsorship or withdraw the sponsorship request.[25] Later, DSS also conducts periodic reviews of cleared facilities once the FCL has been obtained.

Today's DSS has over 900 employees.[26] A Japanese counterpart would be considerably smaller. It could, for example, rely on a small core of permanent officers supported by a "reserve" corps made up of trained investigators from the National Police Agency Security Bureau (NPASB) and Japan's financial industry. It is possible that private Japanese security companies could work to clear facilities for contractors to the government, while big data analytics and AI could expedite the clearance process and monitoring.

In any case, the creation and training of a competent and reliable security is the third most crucial part of an effective IS program, after the establishment of its legal statutory basis and the designation of an agency to implement the program. Here again the United States can be, and has been, of assistance to Japan.

The Center for Development of Security Excellence (CDSE)

For example, the DSS's Center for Development of Security Excellence (CDSE) provides security training to Department of Defense (DoD) and other U.S. government personnel,

[25] "Facility Clearance Process FAQs," U.S. Department of Defense, Defense Security Service, accessed May 9, 2018, http://www.dss.mil/isp/fac_clear/per_sec_clear_proc_faqs.html
[26] "A Q&A with the Director," DSS Access 4, no. 4 (2015): 4, http://www.dss.mil/documents/about/ACCESS_4.4.pdf.

employees of U.S. government contractors, as well as employees of foreign governments. In addition, DSCA maintains an IS training facility, as does the Department of Defense.

In all three cases, programs exist that can facilitate the training not only of individual security officers for Japan, which already happens today, but also the education of future Japanese trainers. In this way, Japan's current industrial security program under MOD/ATLA can become the incubator for an indigenous IS service that is equipped with the latest methods and latest tools for IS, and can educate personnel in private companies on how to implement and oversee the same protocols and requirements—the equivalent of Facility Security Officers (FSO's) under NISPOM rules.

Finally, there is another U.S. institution related to defense trade to which Japan could look for partnership on defense industrial cooperation and industrial security: the National Technology and Industrial Base (NTIB).

The National Technology and Industrial Base (NTIB)

Following the collapse of the Soviet Union and the end of the Cold War, U.S. policymakers became concerned about the future of its defense industrial base. In 1992, an act of Congress mandated that the DoD submit an annual report on "steps necessary to foster and safeguard the National Technology and Industrial Base (NTIB)." From its inception, the NTIB was defined to include entities in Canada, reflecting a history of defense cooperation between the two countries. The NTIB also underscored that defense and industrial supply chains have global, not merely domestic, reach.

Section 881 of the National Defense Authorization Act for Fiscal Year 2017 revises the definition of the NTIB to include the UK and Australia. The addition of the UK and Australia to the NTIB is in part a product of the U.S. interest in strengthening alliances and bolstering interoperability between the United States and its allies. The 2018 National Defense Strategy (NDS) emphasizes the importance of cooperating with allies and the need for "a healthy and secure national security innovation base that includes both traditional and non-traditional defense partners." As CSIS scholars noted in a March 2018 report,

> In the new global strategic environment the NDS describes, where the development of technologies with major national security application is increasingly led by commercial firms, the United States cannot assume that all of the capabilities in needs will be found domestically or that the availability of these capabilities can easily be manages through U.S. technology controls.[27]

Prior to the addition of the UK and Australia to the NTIB, Defense Trade Cooperation Treaty agreements between the United States, UK, and Australia were signed in 2007 to

[27] McCormick, Rhys, Samantha Cohen, Andrew P. Hunter, Gregory Sanders, Samuel Mooney, and Daniel Herschlag. "National Technology and Industrial Base Integration: How to Overcome Barriers and Capitalize on Cooperation." Center for Strategic & International Studies, 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180307_McCormick_NationalTechnologyAndIndustrialBaseIntegration_Web.pdf?Yd28kTbbpfedujBec.QYCbUtwMDC4qaJ

facilitate movement toward country-wide ITAR exemptions.[28] Before that, in 2000, the U.S. Secretary of Defense and the UK's Secretary of State for Defense signed a nonbinding Declaration of Principles; the same year, a Statement of Principles was signed by the United States and Australia. These agreements encompassed "five pillars of cooperation," as designated by former Deputy Secretary of Defense John Hamre: "export control processes; *industrial security policies and procedures*; intelligence cooperation on matters of industrial security; law enforcement cooperation; and access to defense markets."[29]

In all three cases—Canada, Australia, and Great Britain—industrial security standards formed the foundation for substantially raising the defense industry cooperation between the United States and these countries. The same applies to the issue of foreign ownership. Australia, the UK, and Canada are subject to a review of the foreign ownership, control, or influence (FOCI) requirements of the National Industrial Security Program (NISP). The Secretary of Defense–after consulting with the Director of the Information Security Oversight Office and subject to the approval of the Secretary of State– then determines whether entities whose ownership or majority control is located in an NTIB country should be exempted from one or more of the FOCI requirements. An exemption should be granted if doing so facilitates improved cooperation between NTIB countries; furthers U.S. national security interests; and "will not result in a greater risk of the disclosure of classified or sensitive information consistent with the National Industrial Security Program."[30]

The question then arises: why not Japan? Japan offers a technical-industrial base even more proficient than the other FVEYs, and desirable not only to DoD but to U.S. companies. Application for NTIB status for Japan and Japanese industries would constitute a major advance in U.S.-Japan defense industrial cooperation; since the three other foreign countries currently part of NTIB—Canada, UK, and Australia—are also FVEY's, such a development could be a halfway house to eventual full "Sixth Eye" status.

The first necessary step forward, of course, would depend on resolving the "equivalence" issue with regard to IS. Without that gold standard, being formally approved and included in the NTIB network would be highly problematic. With it, however, the possibility of admission, and of where it could lead seems tantalizing.

[28] Herman, Arthur. "Breaking the Defense Trade Barrier: Defense Trade Cooperation Treaties and the Future of the U.S.-Japan Alliance." Hudson Institute, 2018.
[29] Ibid., p. 124-125.
[30] National Defense Technology and Industrial Base, Defense Reinvestment, and Defense Conversion, 10 U.S.C. § 148 (2000).

What Are Japan's Next Moves?

Until recently, much of the activity surrounding defense industrial security for Japan has been focused on safeguarding U.S. technology and information in a Japanese setting, including CMI. This was the case with Aegis in the 1990's, SM3 Block IIA in the last decade, and it is the case with F-35 today.

This case-by-case approach will be inadequate and even counter-productive for the long-term future of Japanese IS. Instead, it will be important that Japan develop a "gold standard" that protects Japanese information and technology first and foremost, but which also has the important additional effect of protecting the information and technology of Japan's defense trade partners on a sound and verifiable equivalence basis.

This will be particularly important when it comes to securing the interoperability of Japanese defense systems with those of allies, particularly the United States. The broadening of the strategic threats in the Indo- Pacific and around the world will inevitably require increasing levels of integration of information and technologies shared by Japan's allies that will be grounded in shared networks and common algorithms, not just common platforms. [31]

This kind of modern interoperability is something the Japanese Self Defense Force (JSDF) itself lacks, let alone shares with the US: yet that requirement will have to be based on a strong system of IS all partners trust.

Such trust ultimately rests on how the U.S. and other allies view Japan's approach to risk assessment and management, which is the central issue in every IS regime.

In the end, IS professionals understand that a modern IS system functions according to a familiar risk management formula:

Risk = Threat x Vulnerability x Assets (i.e. current or replacement cost of asset).[32]

In short, even in the case of low-level threats, high vulnerability and high asset value equals considerable risk. On the other hand, risk can be reduced in the face of a high-level threat to high value assets (e.g. stealth technologies) if major steps are taken to reduce vulnerability to negligible levels (assuming that the assessment of the threat is accurate).

Risk assessment and management are, of course, familiar terms to financial institutions, including Japan's. An illuminating example is when Japanese banks in the 1990's responded to the risks involved in holding large portfolios of non-performing loans held by Yakuza members by developing a system of "enhanced due diligence."[33]

To deal with the challenge, banks employed former intelligence officers to carry out a third

---

[31] Col. Hiroaki Uchikura, "U.S.-Japan Interoperability" (statement, Defense Challenges and Future Opportunities event at Brookings, Washington, D.C., March 26, 2010).
[32] Arlow, Pieter and Russell, David, Industrial Security: Managing Security in the 21st Century (Hoboken, New Jersey: John Wiley & Sons, 2015).
[33] Kattoulas Velisarios, "The Yakuza Recession," Far Eastern Economic Review, January 2002.

level of review after the usual financial and credit reviews: that of a rigorous criminal record and personal association review.

This significant shift in how financial institutions registered risk assessment allowed Japanese banks to bring their non-performing loan portfolios under control.

Additionally, the existence of a more flexible review system also enabled Japanese banks to respond quickly to later changes in banking regulations and requirements both from government and international bodies, while avoiding having to adopt expensive global standards that would have been inefficient in a Japanese context.

Japanese banks came to look at their loan portfolios on the basis of 3 R's: Risk, Revenue, and Reputation, meaning the reputation of the bank if it were seen as a haven for Yakuza monies. The 3 R's are significant for industrial security, as well, given that risk management is at the core of how IS works, from personnel screening and issuing security clearances to cybersecurity and protecting IP. Revenue represents the monetary losses incurred by poor attention to IS, particularly the loss in IP: in the European case in the 1980s, more than $600 billion.

Japan's reputation as a reliable defense trading partner is also important. While there is general agreement that Japan closely reviews third-party technology transfers where other countries do not, including some leading arms exporters, it does face the challenge of large-scale foreign investment in Japanese companies that sometimes allows sensitive technology, including IP, to leak into unwanted hands. Arriving at an equivalence standard in monitoring Chinese direct investment, for example in the use of Chinese-made components in Japanese technology, especially defense technology, would go a long way to reassure allies like the U.S. that Japan is making important strides in addressing its IS concerns.

As noted, Japan has already shown success in the IS arena in the past decade, from GSOMIA and the Secrets Protection Act to cooperation on the F-35 program and the recent METI guidelines. Japanese companies working with their American counterparts have secured ITAR-protected technologies and articles through the Technical Assistance Agreement (TAA) process administered the U.S. State Department's Directorate of Defense Trade Controls (DDTC) and other mechanisms.

In addition, many if not most Japanese companies involved in defense-related industries have their own IS programs for protecting IP and other proprietary data, which they manage with considerable success.

For the Japanese government, then, its next steps will be the same that any country must take to makes its IS program a "gold standard," including the United States.

The Path Forward for Japan

The first step is determining where IS rules will apply, based on who the government of Japan is doing business with currently and which government contractors will have to comply.

The second is defining the broad categories to be covered, including personnel security, physical security, and cyber information security, as well as export control and technology transfers.

The third is identifying the executive agency that will oversee IS, with ample coordination from other agencies, including intelligence agencies.

The fourth is establishing a clearing process, through which companies sponsored by other cleared companies or government agencies can enter, and be certified in a timely manner.

In the U.S. this process is done primarily by the DSS (see Section V). A Japanese counterpart may have the same responsibilities, but it is bound to have different methods.

This is particularly true in the area of personnel security, and in enforcement of IS rules and protocols.

Currently jurisdiction over provisions of Secrets Protection Act is in the hands of the Cabinet Intelligence Research Office (CIRO), the Cabinet-level foreign intelligence service created in 2015 and part of the Japanese intelligence community along with the National Police Agency, the Public Security Intelligence Agency (PSIA), the Defense Ministry's Defense Intelligence Headquarters, and the Foreign Ministry. However, CIRO is primarily charged with collecting intelligence on North Korea and China, as well as intelligence necessary to prevent terrorist attacks. Its staff is largely drawn from other agencies, and most chief positions are occupied by police officers. In 2001, the Cabinet Satellite Intelligence Center was set up as a subordinate agency, so CIRO now does signals intelligence (SIGINT) as well -- while individual agencies actually implement the law.

It is not clear how much experience these officers have in the industrial security or information security realm; nor has CIRO's record in enforcing or prosecuting cases of violation of the Secrets Protection Act or other rules (such as lying on personnel resumes) been exemplary. This is not criticism of CIRO; rather such elements underline the need for a separate agency to oversee and enforce these laws.

As for personnel security, the answer to Japan's industrial security issues may not be in the government at all, but in the financial and data services industries. In the U.S., for example, private companies like Google, Microsoft, and Amazon have amassed far more information about people's activities, associations, and backgrounds than the U.S. government, thanks to privacy concerns.

Therefore, one solution may be to move Japan's effective systems in the financial sector into the industrial space. Since one of the most important aspects of industrial security is the human factor, including insider threats, Japan's strengths in banking, data analytics, and electronic medical records can speed rigorous and rapid personnel screening, as well

as provide benchmarks for determining security clearances—which artificial intelligence capabilities can accelerate and make even more accurate. Japan's expertise in drones and robotics can provide new ways to carry out security inspections and supervise facilities; developments in facial recognition and AI can be powerful multipliers in these areas as well.

Nonetheless, in both the areas of overseeing and enforcing IS and in personnel security, two important challenges will have to be addressed: one requiring a mindset adjustment and the other a modification in Japanese bureaucratic norms.

The first is that a security clearance is a privilege, not a right. Investigation of a person's background must be understood as a pre-condition of employment, rather than a presumption of guilty until proven innocent (in Japanese, the word for "investigation" can imply a crime has been committed).

Most employees and prospective employees are honest and trustworthy. The purpose of a security clearance system is to prevent the tiny minority who are not from handling sensitive materials or data; and the purpose of the background check is to prevent that minority from getting into the system at all.

The second challenge is that building an effective IS cadre requires time for training, acculturation, and the accumulation of experience. The tradition of Japanese civil servants to move to another department or division after two or three years undercuts that requirement. U.S. officials have often expressed frustration with helping to establish IS protocols with Japanese officials because officials leave just as they are "getting the hang of it" and an entirely new team has to then be trained and acclimated.

Japan needs a security cadre that receives extensive training and experience on the job, as well as its own system for advancement and promotion. Such a cadre will be crucial to an effective IS system, together with a personnel classification system that can deter insider threats, and creation of a single authority that oversees IS issues, including coordinating interagency efforts such as export control and third-party transfers.

In terms of building such a cadre, attendees at the Hudson workshops were enthusiastic about the idea of hiring retired JSDF security personnel as the basis of the new IS cadre, alongside graduates of the DSS's training program (some of whom, it was noted, are even more up-to-date on latest IS methods than their U.S. counterparts).

Even more important is finding ways to modify the usual pattern for career advancement in the Japanese bureaucracy in order to build such a cadre. This will require careful thought and creative action, particularly from the top of Japanese leadership. But this modification will be necessary if Japan is to create a robust indigenous IS system, and the United States needs to encourage the Japanese government to take significant steps in that direction.

The fifth and final step in achieving the IS "gold standard" will be determining the costs involved in implementing effective IS, both for government and industry. Some of those costs will be defrayed on the part of private industry as "allowable costs" in government contracts. However, there must also be an awareness of what the government will need to

spend in order to initiate a broad and comprehensive IS regime that meets equivalence standards for allies, but also is flexible to grow and adapt in the future.

Even with the implementation of these remaining steps, closing the IS gap for Japan will involve a shift in mindset, that will be even more important than an institutional shift.

In Japan's case, developing a modern government-led IS system that Japanese industry can fully embraced might be expedited by conditioning participants to see IS not as a cost burden or imposition, but as the natural extension of the same investment in improving Japan's economic competitiveness that governed Japanese industry's adoption of Total Quality Management (TQM) in the 1960's and 1970's.[34]

Like TQM, modern IS can be viewed positively as a concept borrowed from American sources that can be adapted to Japanese conditions and culture, in order to give a new boost to Japanese economic competitiveness and co-development opportunities, including exports and direct investment.

By seeing modern IS not as an impediment but as an investment opportunity for both government and industry, Japan will even be poised to become a global leader in applying advanced technology like AI and robotics to the IS process, in transformative ways that benefit not only Japan but its allies, including the United States (see Section VII). The bottom line is that whatever kind of cultural framework Japan chooses for its own IS system will be crucial to determining its success.

Flexibility will be key. A key requirement for a Japanese IS program is that it not be seen as a straitjacket—especially not a straitjacket imposed by outsiders. Today's information age will require fundamental shifts in thinking about how to implement industrial security in ways that NISPOM is not designed to address, but that Japan can help to initiate.

Japan will require a system that is calibrated to embrace, not exclude, new technologies for handling and protecting sensitive data, including background checks; one that makes industrial security provisions a regular part of defense agreements as well as FMS and transfer of equipment agreements; and one that distinguishes between the application of commercial technologies for defense purposes, which necessarily fall under regulatory authority, and those that do not.

It will be a system that protects the IP of Japanese companies and individuals; it will also allow room for interpretation of the guidelines and finessing the details when feasible—or necessary. In the current U.S. system, investigators know there are some companies that require constant supervision, while others with a proven track record and personnel, require less—another advantage of long-term service and continuity of personnel.

In short, the path forward should include leveraging technical advantages Japan already enjoys into an IS gold standard both for government and industry. In fact, more than one participant in the Hudson conferences voiced the feeling that they were somewhat jealous of Japan: It has the opportunity to start fresh and build an effective IS system from the

[34] H. Yui, "The Japanese-style production system and total quality management," Total Quality Management 8, no. 2 (1997): 333-336.

ground up.

In either case, Japan can “pull on the thread of opportunity,” and envision building a system that not only works, but can become a model for other Asian countries.

Balancing Risks and Opportunities in Industrial Security

Indeed, by continuing to build on past successes and "best practices models," and by incorporating new technologies such as big data analytics, facial and retinal recognition, and artificial intelligence , Japan can pass beyond the standards of "equivalence" with American and NATO programs to become a global leader in IS for decades to come.

In the final analysis, the goals for a "made in Japan" IS program are two-fold.

The first is establishing a standard operating procedure across the board, which is the same regardless of agency. It is sometimes a disconcerting experience for Japanese visitors examining the security classification system in the United States to discover that DoD, State, the CIA, and the FBI all share the same procedures and the same classification systems.[35] Achieving the same uniformity, and unity of effort, will be important within the Japanese government, as it will be as applied to industry.

The second is to establish a "virtuous cycle" in IS, in which standards are consistently raised in ways that increase confidence among allies. For example, initial standards will open the door to more and deeper cooperation; which in turn will lead to raising standards further as a means of gaining still more confidence and cooperation from allies. This cycle will in the end achieve important foreign policy and trade policy goals, as well as satisfy defense and alliance priorities—one more reason why IS needs to be a broadly defined national security issue for Japan.

One ally where there is ample opportunity for Japan to cooperate is India. India has joined several mechanisms for defense trade cooperation with the U.S. such as the Defense Trade and Technology Initiative (DTTI), the U.S.-India Interagency Task Force, and the India Rapid Response Cell (IRRC), in addition to a GSOMIA signed in 2002.[36] But like Japan, India needs an effective and comprehensive IS program in order to complete the circle. Similarly, Japanese methods cannot apply directly to the Indian example any more than U.S. examples apply to Japan. Indian industry occupies a very unique place in the hierarchy of advanced technologies; a successful "made in Japan" IS program could point the way forward for India to achieve an equivalence standard—and serve as the basis for a trilateral alliance of defense trade and industrial cooperation, the long-term strategic and geopolitical impact of which would be hard to overestimate.

Indeed, Japan could even provide leadership in industrial security for Western countries, including the U.S., by showing how to integrate new technologies seamlessly into a flexible and proactive IS regime. For example, in using AI for continuous monitoring and sifting of data for discovering new areas of vulnerability requiring action and using AI to achieve greater transparency and responsiveness in the supply chain.

---

[35] "Executive Order 13526 of December 29, 2009," Code of Federal Regulations, title 3 (2009), https://www.archives.gov/isoo/policy-documents/cnsi-eo.html.

[36] Ankit Panda, "LSA, CISMOA, BECA and the Future of the U.S.-India Defense Partnership," The Diplomat, April 7, 2016, https://thediplomat.com/2016/04/lsa-cismoa-beca-and-the-future-of-the-us-india-defense-partnership/.

Just as the U.S. Department of Defense is currently looking at blockchain, i.e. a distributed ledger system, to protect data, so too could JMOD/ATLA c point the way forward in emerging technology. For example, quantum technology could be implemented as the ultimate tool for protecting data and networks, through integrating research in quantum communications at the National Institute of Communications Technology to address IS concerns.[37] Such a venture could inaugurate a cooperative relationship that other countries will want—and eventually need—to emulate.

For Japan, the path to effective industrial security is one that is full of promise, both for the country's national security and alliances, but also for its economic and technological competitiveness—if the government and its corporate partners are willing to take the first significant steps forward now.

If Japan doesn't close the gap, however, the flow of defense technology sharing from the U.S. is bound to dwindle to a trickle and possibly cease altogether. Failure to close the gap will place increasing limits on technological and industrial cooperation, not just with the U.S., but with other allies.

A good example is Japan's plans for the Future Fighter program. Currently Japan is seeking proposals for a new advanced jet fighter based on an existing Western aircraft and wants American and British cooperation to help kick-start development of the project. In March 2018, Japan issued a third request for information (RFI) to defense companies, seeking proposals for the new aircraft, dubbed the F-3. Existing airframes Japan could use include Lockheed Martin's F-35 Joint Strike Fighter; Boeing's F/A-18E/F Super Hornet; or the Eurofighter Typhoon, which is built by a European consortium including BAE Systems Plc.[38]

Japan wants to introduce its own air superiority fighter, similar to the F-22 Raptor, to be ready in the 2030's to help deter future hostile intruders into its airspace. To defray the costs of development, which are estimated to be around $40 billion (Mitsubishi Heavy Industries has already tested a prototype stealth jet in 2016, the ATD-X or X-2, which cost the Japanese government $350 million to develop), Japan wants a F-3 model suitable for export; for example, as a candidate to succeed the U.S.'s own F-22 and one that Britain, which is seeking closer security ties to Japan, including cooperation on developing new defense equipment, might consider as a possible successor to the Typhoon.

None of these plans will be feasible without access to advanced U.S. technologies, including technologies currently on board the F-35 JSF. Japan's access will be blocked, however, unless the U.S. sees signal improvements in IS along the lines this report has outlined. Furthermore, the F-22 itself should be a cautionary tale for Japan of what can happen without adequate IS safeguards.

---

[37] Elana Broitman, "The Pentagon Has the World's Largest Logistics Problem. Blockchain Can Help," Defense One, October 3, 2017, https://www.defenseone.com/ideas/2017/10/pentagon-has-worlds-largest-logistics-problem- blockchain-can-help/141500/.

[38] Kelly, Tim and Kubo, Nobuhiro. "Exclusive: Japan's new advanced fighter may be based on existing foreign design - sources." Reuters, 2018. Retrieved from https://www.reuters.com/article/us-japan-defence-fighter-jet-exclusive/exclusive-japans-new-advanced-fighter-may-be-based-on-existing-foreign-design-sources-idUSKCN1GK06R

The Pentagon developed and built the Raptor stealth fighter at a time when its cybersecurity measures were still relatively rudimentary. When China unveiled its stealth fighter prototype, the J-20, in 2013, observers noted its uncanny, even sinister, resemblance to the F-22. The explanation was distressingly simple: China had simply penetrated the U.S.'s poor cybersecurity and stolen key Raptor technologies while reverse engineering the rest.[39]

It would be a tragedy if Japan's Future Fighter program suffered the same fate by enabling China or other hostile actors to highjack key technologies that could render the F-3 obsolete before the prototype leaves the hanger. The U.S. learned valuable IS lessons from the F-22 example—lessons which Japan can heed before embarking on its F-3 flagship program.

[39] Ling, Justin. "Man Who Sold F-35 Secrets to China Pleads Guilty." Vice News, 2016. https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty

Basic Principles and Policy Recommendations

By the conclusion of the Hudson workshops in Washington DC and Tokyo, six important principles for designing a "made in Japan" IS program had emerged:

1) It is imperative that the United States help Japan close the industrial security gap, because the future of the alliance's technology-sharing and defense trade and industrial cooperation hinges on it—as well as the future security of the region.

2) The government of Japan needs to create a single national authority able to prescribe standards and practices across government and industry—standards that are enshrined in law—and empowered to enforce and supervise all aspects of IS, from personnel to cyber.

3) Japan will also need a trained security cadre to staff its IS agency. The U.S. can help to develop, but there must be a commitment on the part of the Japanese government to professionalize IS.

4) Japan has already shown success in the IS arena in the past decade, from GSOMIA and the Secrets Protection Act to cooperation on the F-35 program and the recent Ministry of Economy, Trade, and Industry (METI) guidelines. In addition, Japanese companies working with their American counterparts have secured ITAR-protected technologies and articles through the Technical Assistance Agreement (TAA) process administered the U.S. State Department's Directorate of Defense Trade Controls (DDTC) and other mechanisms. Many, if not most, Japanese companies involved in defense-related industries have their own IS programs for protecting IP and other proprietary data, which they manage with considerable success.

5) Indeed, by building on "best practices models," and by incorporating new technologies Japan can pass beyond the standards of "equivalence" with American and NATO programs to become a global leader in IS, ultimately increasing its economic competitiveness in the defense and commercial spheres for decades to come.

6) If Japan doesn't close the gap, however, the flow of technology-sharing from the U.S. is bound to dwindle to a trickle, and possibly cease altogether. Unfortunately, this gap will become increasingly more apparent, as the definition of defense technologies requiring high levels of IS protection equivalent to that provided by U.S. companies and U.S. allies, continues to expand. Those systems with advanced technologies that can provide Japan with unique capabilities, and vital force multipliers, will be particularly at risk.

In the final analysis, political will and firm leadership will be necessary from industry and from government, in order for an industrial security system "with Japanese characteristics" to succeed.

So what are the immediate steps forward Japan should consider next?

The first is identifying the political center of gravity for IS reform. Who will make the key decisions leading to creation and implementation, and who is to assume the responsibility for creating the system and making it work? The single-authority model that exercises oversight and enforces rules and regulations remains the best model for IS. Implementation can be an interagency process; but a mechanism must be put in place with authority to initiate the process, and exercise decision-making powers.

The second step is arriving at a list of minimum requirements, which will provide the first steps in initiating the process. This report's specific recommendations include:

- **Designate industrial security reform as an integral part of Japan's national strategy in the 5-year Mid-Term Defense Program, and the 10-year National Defense Program Guidelines.**

  By integrating industrial security reform into Japan's long-term defense planning, the government and Ministry of Defense will send a clear message that IS reform is an important goal for Japan's own national security, as well as for cooperation with allies.

- **Establish funding in the FY2019 defense budget for a feasibility study on creation of a Japanese defense security service, including training, staffing, and integrating advanced technology.**

- **Establish funding for and creation of an interagency industrial security working group, which will examine the steps needed to create a unified industrial security program that can regulate and oversee both government and industry, including a uniform security classification system.**

- **Require Japan's defense industry to establish an Information Sharing and Analysis Center (ISAC) for sharing data regarding cyberattacks, which will also be shared with agencies responsible for industrial security.**

  ISAC's already exist in other Japanese industry sectors such as the financial and information technology sectors. A similar center for defense companies can serve as a useful template for mobilizing cybersecurity measures including as part of an interagency consultation group to be led by NISC.

- **Continue and extend cooperation with the U.S. in key areas of industrial security cooperation such as the Bilateral Information Security Cooperation discussions (BISC), and the F-35 joint strike fighter program in order to formulate general rules and regulations.**

As already mentioned, the U.S. has an essential role to play in leading and encouraging Japan's path to a comprehensive government-led IS regime and there are important steps it can take.

The **first** is to encourage the government of Japan to consider extending current joint efforts at IS as stepping stones to developing an indigenous "made in Japan" IS system, such as for the Future Fighter Program, which will achieve "equivalence" without the need for U.S. help or oversight.

The **second** would be to progressively ease export controls for Japan under the International Traffic in Arms Regulations (ITAR) in response to demonstrative improvements in Japan's IS regime.

The **third**, and the most important, would be incentivize a Japanese surge in IS improvement by offering the U.S. help in Japan enjoying full membership in the Five Eyes intelligence-sharing alliance, along with the UK, Australia, Canada, and New Zealand. Achieving status as "the Sixth Eye" would not only be a landmark for Japan, but also for the U.S.-Japan alliance and the special relationship.

In addition, encouraging Japan to take the steps necessary to achieving Sixth Eye status will bring Japan into this unique network for intelligence-sharing at a crucial time in the Indo-Pacific region, when cooperation in gathering and analyzing intelligence regarding the activities of countries such as China, North Korea, and Russia will be more imperative than ever. It will also help to put the stamp of "special relationship" on the US-Japan alliance, in parallel ways to the relationship with the United Kingdom.[40]

Fourth, a major step in achieving this Sixth Eye status would be incorporating Japan as part of the National Technology and Industrial Base (NTIB), alongside other Five Eye members UK, Australia, and Canada. Japan could swiftly become a major factor in the Pentagon's goal to build a global supply chain to undergird the U.S.'s defense industrial base; while becoming part of NTIB would also open the way for Japan to begin direct investment in the U.S. defense sector, under the terms of FOCI and CFIUS.

Becoming part of NTIB would require major advances in Japan's industrial security efforts—advances that match the equivalence standards of UK, Canada, and other Five Eyes. Those advances could clear the way for formal consideration for Sixth Eye status.

America's role in helping Japan close the industrial security gap, then, is more indispensable than ever. However, the main responsibility still remains with Japan and the Japanese government. Despite the impressive steps the current Abe administration has already taken to modernize and build a strong indigenous IS regime, without bold leadership Japan's industrial security gap will continue to exist—while the future of U.S.-Japan defense technological and industrial cooperation will hang in the balance.

[40] Arthur Herman, "Pacific Partners," Hudson Institute, 2017.

Participants

Hudson Institute would like to thank and acknowledge the organizations that participated in the workshops in Washington DC on March 23, 2018 and in Tokyo on May 21-22, 2018:

Japan

Acquisition, Technology & Logistics Agency
Center for Information on Security Trade Control
Fujitsu Ltd.
Global Insight Corporation
IHI Corporation
Institute for Future Engineering
Itochu Corporation
Manufacturing Industries Bureau, Ministry of Economy, Trade, and Industry
Ministry of Foreign Affairs
Mitsubishi Heavy Industries, Ltd.
National Graduate Institute for Policy Studies
National Security Secretariat
NEC Corporation
Office of the Minister of Defense

United States and Other

Advanced Concepts and Technologies International
Avascent
Department of Homeland Security
F-Secure Corporation (headquartered in Finland)
Lockheed Martin
Navigators Global LLC
Nisos Group
Northrop Grumman
Office of Japanese Affairs, Department of State
Defense Technology Security Administration, Office of the Undersecretary of Defense for Policy, Department of Defense
The Boeing Company
U.S. Embassy in Tokyo
White & Case LLP

Acknowledgments

The author would like to thank his Research Associate and Project Manager Ms. Idalia Friedson for her assistance in editing the report and organizing the conferences. He also extends his gratitude to Dr. Satoru Nagao, Visiting Fellow and to Mr. Thomas Keelan, Hudson Institute Research Assistant, for their invaluable work coordinating the Tokyo conference. Finally, his interns Ms. Isabella Emanuele and Mr. Brent Cronce provided crucial administrative and research support.

List of Names and Acronyms

ATLA	Acquisitions Technology and Logistics Agency
BISC	Bilateral Information Security Consultations
CDSE	Center for Development of Security Excellence
CMI	Classified Military Information
CFIUS	Committee on Foreign Investment in the United States
CoCoM	Coordinating Committee for Multilateral Export Controls
CTSP	Cooperative Technology Security Program
DCSA	Defense Security Cooperation Agency
DSS	Defense Security Service
DTSA	Defense Technology Security Administration
DTTI	Defense Trade and Technology Initiative
FACO	Final Assembly and Check Out
FCL	Facility Security Clearance
FedRAMP	Federal Risk and Authorization Management Program
FMS	Foreign Military Sales
FOCI	Foreign Ownership, Control, or Influence
FSO	Facility Security Officer
GSOMIA	General Security of Military Information Agreement
IRRC	India Rapid Response Cell
IS	Industrial Security
ISAC	Information Sharing and Analysis Center
ISP	International Security Policy
JMOD	Japanese Ministry of Defense
JSDF	Japan Self Defense Force
METI	Ministry of Economy, Trade, and Industry
MOFA	Ministry of Foreign Affairs
NCIRSC	National Center of Incident Readiness and Strategy for Cybersecurity

NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NPA	National Police Agency
NPASB	National Police Agency Security Bureau
PSIA	Public Security Intelligence Agency
SDS	Special Designated Secrets
TQM	Total Quality Management

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Hudson Institute
1201 Pennsylvania Avenue, N.W.
Suite 400
Washington, D.C. 20004

P: 202.974.2400
info@hudson.org
www.hudson.org