

Deepening Japan's Information Security Regime:

The Need of Domestic Legislation

By Masahiro Matsumura

November 2013

Mr. Masahiro Matsumura is a Professor at St. Andrew's University in Osaka, Japan. He was a Visiting Research Fellow in the Center for Strategic Research, Institute for National Strategic Studies (INSS), at the National Defense University during the summer of 2013.

The author is grateful for comments and editorial suggestions of Dr. James J. Przysup, who hosted his visiting fellowship at INSS. This research was made financially possible by the Short-term Overseas Research Grant of St. Andrew's University.

In August 2007, the United States and Japan concluded a General Security of Military Information Agreement (GSOMIA) to facilitate the sharing of classified information. Based on some 60 precedents, the agreement has established common security standards to allow for sharing of intelligence as well as information on defense programs and operations. Given the well developed U.S. legal and administrative regime governing the protection of classified information, U.S.-Japan bilateral information sharing will be greatly facilitated by Japan's adoption of a similar domestic regime.

However, for the past 6 years, the Japanese government has failed to take concrete legislative steps to fully satisfy GSOMIA requirements. From 2007 to 2009, the ruling Liberal Democratic Party's (LDP) government lacking a majority in the Upper House, was unable to adopt the necessary legislation. In September 2009, the progressive Democratic party of Japan (DPJ) came to power. Initially disinterested in building a domestic security regime, it moved to consider such legislation following the leak of Coast Guard video, which had just been classified in light of its China policy considerations, to Youtube on the September 2010 fishing boat incident in the Senkakus. To prevent similar leaks, the government organized an advisory committee on information security under the Prime Minister's office charged with producing policy recommendations.¹ The policy document was drafted by bureaucrats who tried to balance GSOMIA requirements with their respective institutional interests.

The LDP returned to power in December 2012, with the intention of introducing a major security information bill (Tokutei-Himitsu-Hozen-Hoan) or Secrets Protection Bill in this autumn session of the Diet. This would be taken together with legislation to establish, for the first time in Japan's post war history, a professionally staffed, intra-governmental national security council. The Secrets Protection Bill is a necessary legal measure to ensure the effective operation of the national security council, which is anticipated to exchange significantly more classified information with the United States and enhance collective security.

The Secrets Protection Bill will cover ranking political appointees, including Ministers, Senior Vice-Ministers, Vice Ministers, the national public service, prefectural police and private

sector contractors, such as defense firms, with access to classified information. The legislation, however, does not extend to Members of the Diet, who have the constitutional oversight responsibilities and may be provided access to classified information.²

The LDP government expects the Diet to approve the legislation during the autumn session, but with some amendments limiting its scope in order to secure the support of its coalition partner, the New Komeito.

Long overdue, the adoption of the Secrets Protection Bill is but the first step toward the development of a domestic information security regime. However, the interplay of bureaucratic infighting among Ministries anxious to preserve their privileged position with regard to classified information, and political passivism is likely to retard implementation of the legislation, in particular the adoption of a document similar to the U.S. National Industrial Security Program Operating Manual (NISPOM), which establishes the standards and procedures for all government contractors with access to classified information.

In the 6 years since the conclusion of the GSOMIA with the United States, Japan has concluded a series of similar information security agreements with NATO (2010), France (2011), Australia (2012), and the U.K. (2013); in the offing is a similar agreement with South Korea. In effect, the government has widened the information security regime internationally without deepening it domestically. In doing so, Japan has demonstrated a commitment to advance security cooperation through information sharing but, at the same time, has failed to develop the necessary domestic legal framework to facilitate security cooperation.

Accordingly, this paper focuses on the policy dynamics of “widening” and “deepening;” the bureaucratic politics at play at the Ministry of Foreign Affairs (MOFA), the Ministry of Defense (MOD) and the Ministry of Justice that have hampered efforts at “deepening;” as well as the political disinclination, to date, to confront the bureaucracies.

The Strategic Dimension: Strengthening the Alliance through Intelligence Sharing

The GSOMIA of 2007 is a result of longtime Alliance security consultations. The Two Plus Two Statements of October 2005 and May 2007 called attention to the need to enhance security and intelligence cooperation as well as the need to address the evolving gap between the treaty framework and specific operational needs.³

Information sharing is a high priority in alliance policy, and serves to improve common security interests of all parties. It is critical to enable Japan to provide rear area and logistical support for U.S. in contingencies in areas surrounding Japan as agreed to in 1997 Japan-U.S. Guidelines for Defense Cooperation. Faced with intensifying security challenges from North Korea and China as well as an increasingly unstable Middle East and constrained defense budget, even allowing for modest increase in FY 2014, the alliance remains central to Japan’s security. In this context, intelligence cooperation stands as a relatively inexpensive policy instrument to enhance both the operational effectiveness of the Self Defense Forces (SDF) and U.S. confidence in Japan as a reliable security partner. Solidifying U.S. confidence in Japan is indispensable to sustaining the alliance, as is enhancing shared understanding of information and technologies.

The complex nature of the evolving 21st century at both global and regional levels underscores the need for Japan to enhance peacetime bilateral cooperation, which, in the event of unforeseen contingencies, would allow for the smooth transition to wartime cooperation at strategic, operational and tactical levels. During the Cold War, the alliance was focused directly on the defense of Japan, without specific operation planning to deal with major regional contingencies.

At the end of the Cold War, the alliance was initially transformed into an international public good with objective of maintaining peace and stability on the Korean Peninsula, the Taiwan Strait and across the broad Asia-Pacific region. Under the revised 1997 Japan-U.S. Guidelines, Japan assumed supplementary and complementary roles in support of regional order, agreeing to provide rear area and logistical support to the United States in contingencies in area surrounding Japan. To be effective operationally, this requires coordinated planning and information sharing.

The Policy Dimension: Evolutionary Deepening of Information Sharing and Its Limitation

For more than a decade prior to the 2007 GSOMIA, the United States provided Japan with considerable classified military information. The need to share information grew dramatically as the U.S. and Japan coordinated policies on North Korea, missile defense contingency planning and the global war on terror. For example, the U.S. shared satellite photos of North Korean missile launch sites, while the U.S. benefited from Japan's Signal Intelligence

(SIGINT) and Human Intelligence (HUMINT) on North Korea. Similarly, Japan benefited from higher levels of access to U.S. weapons systems software, real-time electronic data related to Command, Control, Computers, Surveillance, and Reconnaissance (C4ISR) in general and missile defense in particular.

In a Cold War context, information sharing was not critical, because, by and large, the prevailing Cold War structure subsumed conflicts on the Korean Peninsula, Taiwan and the Middle East. And Japan used U.S.-made or U.S. designed weapons systems whose classified technologies and information were almost all embedded. Accordingly, the need for information sharing was low. When necessary, arrangements were made on a case-by-case basis. In 1988, Yukio Okamoto, then-Director of the Security Policy Division of the North America Bureau of the Ministry of Foreign Affairs, told the House of Representatives Committee on Cabinet that the government considered the existing case-by-case method of information sharing as sufficient, that there was no need to conclude a GSOMIA.⁴

Today, the conditions that made Japan's avoidance of a GSOMIA no longer exist. As this author has analyzed elsewhere, U.S. military technology transfer is no longer embedded in individual weapons or platforms but is based on systems integration, which fuses individual technologies, strategic/operational/tactical data, encryption technologies via computer and communication. The closely intertwined nature of the classified information involved in this process requires a comprehensive measure to govern information security.⁵

GSOMIA today is indispensable to Japan's security, allowing Japan to maintain its military strength and enhance its preparedness.⁶ Under increasing budget pressures, security can only be enhanced by increasing the operating ratios of existing major U.S.-made or U.S. designed platforms that depend on U.S.-controlled black boxes, most notably the F-15 fighters. Under existing arrangements, the black boxes have to be shipped back to the United States for maintenance and servicing. Japanese firms are unable to service the black boxes without necessary access to classified data and technology, even though they have the necessary technological capabilities. With access under GSOMIA, the same functions will be able to be performed in Japan, significantly improving the efficiency of bilateral training through streamlined maintenance, servicing and logistics.

As the U.S. military moves to the acquisition and deployment of more advanced weaponry, its defense sector will be burdened by the continued maintenance and servicing needs of legacy systems and platforms. With the necessary access to classified information, Japanese defense firms would be able to meet servicing requirements for both Japan's SDF and U.S. forces in Japan. This would enhance the technological level of Japan's defense industries, create opportunities in the defense sector at a time of declining acquisition spending, and very importantly, strengthen the U.S. military presence centered on Japan.

GSOMIA is critical to meet these operational and defense industrial objectives. At the same time, it is also necessary to establish a solid domestic information security regime, based on a firm classification system, a solid security clearance system and a document similar to the

NISPOM. The first Abe government concluded the GSOMIA to facilitate bilateral intelligence and defense industrial cooperation. To date, however, successive governments have failed to advance legislation necessary to develop an information security regime.

The Domestic Political Dimension: “Widening” without “Deepening”

Article 2 of the 2007 GSOMIA stipulates that the agreement must be consistent with all existing Japanese and U.S. laws and regulations.

Establishing a full information security regime is politically challenging in the pacifist Japanese state, a product of the U.S. post-war occupation. Unlike post-war occupation policy in Germany, the U.S. occupation ruled indirectly through the existing Japanese bureaucracies. Given the historical legacy of a strong state versus society, the bureaucracy has continued basically intact and preserved its *de facto* if not *de jure* predominance in policy making in the existing democratic parliamentary system.

Today, there is an inherent tension between the need for a stepped-up information security regime to meet the security challenges of the 21st century and a bureaucratic disinclination to support such a system in order to sustain the bureaucracy’s substantial policy-making role as well as its influence as a provider of selective information to members of the Diet and media.

Bureaucratic interests are in play. The post-war bureaucracy has worked assiduously to prevent the reemergence of the military as an institutional competitor, reflecting the collective

memory of the prewar military dictatorship that developed an information security regime to maintain control over society. Today, within the bureaucracy, a GSOMIA, buttressed by a domestic information security regime, could enhance MOD power at the expense of MOFA, which, in the post-war years, has served as the primary organ for national security policy making. During the occupation, MOFA served as the sole contact with U.S. authorities. Even after the restoration of sovereignty in 1952, with the government's reliance on the alliance for Japan's security, MOFA continued to serve as the alliance manager, while the Defense Agency solely managed the SDF and was not a policy-making organ.

While the Defense Agency was elevated to ministerial status in 2007, MOD is still in the process of becoming a first-tier policy-making organ. MOD bureaucrats and SDF leadership remain challenged by a lack of human resources and the Ministry's own organizational structure as embedded in laws, regulations and practices⁷ -- which have resulted in a series of serious leaks of classified information.⁸

The Office of the Prosecutors in Ministry of Justice⁹ is also likely to see potential conflict between its established legal primacy and a strengthened information security system. Under the existing legal framework, while various judicial police are in charge of criminal investigations, the Office of the Prosecutors alone has the power of indictment. Lacking military status under domestic law,¹⁰ the SDF also lacks a military justice system independent of the judiciary and the Office of the Prosecutors. However, a fully developed information security regime will most likely require a military judicial system to deal with cases involving classified military

information *in camera*. Establishing a military justice system would challenge the both Office of the Prosecutors' legal primacy in law and its monopoly of the power of indictment.

Over the years, the existence of conflicting bureaucratic interests and imperatives have contributed to the dynamics of “widening” without “deepening” with respect to evolution of an information security regime.^{1 1}

The Legal and Regulatory Dimension: Shortcomings and Pitfalls

On September 3, the Abe government published a detailed outline of the new Secrets Protection Bill and requested public comment.^{1 2} If enacted, the legislation will apply to the national public service, including the MOD and SDF personnel, the prefectural police, and those in the private sector with access to classified information. It would impose a maximum ten year sentence on those found guilty of leaking classified information.

This new legislation is in sharp contrast with the existing Public Service Law that imposes a maximum 1-year sentence and/or fine of 500,000 yen (less than \$5,000) solely on the offending official and his immediate collaborator.^{1 3} Also, the key concept in the draft legislation is “specific secret,” which covers not only classified military information but classified diplomatic, counter-intelligence and internal security information as opposed to existing law which extends only to classified military information with a maximum penalty of from five to ten year imprisonment. The new legislation has been drafted to be fully consonant with existing U.S. law and the requirements of the GSOMIA.

However, the legislation does not extend any heavy sanction and legal penalty to those Members of the Diet who participate in *ad hoc* closed committee deliberations and plenary sessions, in the case of disclosure and leak. In addition, the separate Rules for the House of Representatives and Councillors are devoid of specific measures to handle classified information in general and secret sessions in particular. The Cabinet-proposed legislation does not cover the legislature under the constitutional principle of the separation of powers. It has to be noted that the legislators are not required to obtain a security clearance. Nor does the legislation explicitly cover Diet Secretariat personnel and legislative staffs of individual legislators. Evidently, the legislation does not provide any substantial information security in the legislative process, particularly because it does not assume the regular holding of secret sessions by standing committees, a common practice among the U.S. Congress committees on intelligence, national security, and foreign affairs issues, among others.

The new legislation provides an expanded list of classified military, diplomatic, counter-intelligence terrorist-related information that is in accordance with U.S. standards and incorporates classified military information under the Self Defense Law. In accordance with established Japanese judicial precedent, an action of the executive branch to classify information is necessary but not sufficient to establish its final legal status. Only review by the judiciary can determine if the information deserves protection, particularly when a broad statutory definition of classification is invoked.^{1 4} The specific requirements of the expanded list, therefore, will

deter arbitrary classification for political expediency, thereby considerably lessening the need of judiciary review.

The clarification of “specific secret” will reduce significantly uncertainty inherent in the existing classification of “defense secret” under the Self Defense Force Law and the MOD “secret” under the National Public Service Law. This will correspond to the U.S. classification top secret, secret, and confidential.^{1 5}

The bill also provides for a personal security clearance system built on criteria and procedures on a par with U.S. standards, including background checks; implementing ordinances and regulations, however, remain to be developed. This gap is significant because under the GSOMIA, the Japanese government has agreed to grant access to classified military information on a need-to-know basis to individuals with security clearances. The existing MOD Directives and Special Contracts to date focus on non-human factors of information security, not personal security resulting from careful background investigation.^{1 6}

The bill takes for granted the capacity of existing institutions to process denial of or objection to denial of personal security clearances as well as declassification of classified information in accordance with the Freedom of Information Law.

Finally, passage of the Secrets Protection Bill will make it possible for Japan to establish an equivalent of the U.S. NISPOM, which is indispensable to the further strengthening of defense industry cooperation. To date, Japan has not been able to do so because critical features

of the NISPOM are incompatible with existing Japanese laws and regulations. Absent passage of the Secrets Protection Bill, any NISPOM would be sub-optimal.

Policy Support

From an Alliance perspective, it is critically important for the United States to support efforts of the Abe government to establish an information security regime. Specifically, the United States can share its expertise with respect to the information security system of the Congress, with a major focus on the necessary legal elements necessary to conduct secret sessions at committee levels. This can be done both through diplomatic channels as well as direct contact and exchange programs between the Congress and the Diet.

To avoid risks involved in establishing a sub-optimal information security regime, the United States should:

- Underscore the importance of establishing a comprehensive security regime that will enable Diet committees to conduct secret-level sessions fully capable to protect classified information, and the need to impose heavy legal penalties in the event of disclosure not only on the legislators but also on Diet Secretariat personnel and legislative staff to individual Diet members.
- Emphasize, following passage of the legislation, the importance of implementing ordinances, directive and other administrative regulations.

- Be prepared to share expertise with respect to process of granting or terminating personal security clearances as well as declassification of classified information.
- Encourage Japan to produce a NISPOM-like manual and be prepared to share its experience and expertise in this matter.

Notes

¹ “Himitsu-hozen notameno Hosei no Arikata nitsuite (A Report on the Need of an Information Security Law)”, August 8, 2011, available at <http://kantei.go.jp/jp/singi/jouhouhozen/dai3/siryou4.pdf>.

² Tokutei-Himitsu-Hogo-Hoan (the Secrets Protection Bill), available at http://www.shugiin.go.jp/index.nsf/html/index_gian.htm. Tokutei-Himitsu no Hogo ni kansuru Houritsu-An no Gaiyo (Outlines of the Secrets Protection Bill), available at <http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=060130903&Mode=0>.

³ Available at <http://www.mofa.go.jp/region/n-america/us/security/scc/>.

⁴ The Committee on Cabinet book of minutes, House of Representatives, 112th Diet, May 17, 1978, Available at <http://kokkai.ndl.go.jp/SENTAKU/syugin/112/0020/main.html>.

⁵ Masahiro Matsumura, *Gunji Jyoho Senryaku to Nichi-Bei Domei* (Military Information Strategy and the Japan-U.S. Alliance), Tokyo: Ashi Shobo, 2004, 99.

⁶ Over the last several years, a GSOMIA has become a focal point in the selection of Japan’s next-generation jet fighter. Due to the central importance of GSOMIA, the U.S. would see Japan as less reliable with a weaker information security regime, given that Japan was not equipped with one while some 60 countries, including major U.S. West European and other allies, already concluded ones. For his statement, see, Fumio Kyuma, keynote speech at a major conference on U.S.-Japan strategic relations, held in Tokyo, sponsored by the National Security Research Group, November 11, 2005, available at <http://www.ja-nsrg.or.jp/forum2005-6/f2005-6.htm>.

This concern loomed large after a series of incidents in Japan that involved grave leaks and compromises of classified military information, such as the leak in 2004 through file-sharing software, the leak to a media in 2005 by a colonel at the Defense Intelligence Headquarters about some navigation record of a PLA Navy submarine's intrusion into the territorial waters, and the leak in 2007 about the AEGIS system from a lieutenant commander with proper security clearance to a petty officer without, whose wife was a PRC national. These incidents cumulatively caused strong U.S. concern about Japan's weakness in information security, particularly when Japan continually made requests to the U.S. to sell the most advanced 5th-generation stealth F-22 jet fighter involving a lot of classified military technologies. When the U.S. refused to sell the fighter to any country including Japan, the country naturally considered that the conclusion of a GSOMIA became essential to ease the U.S. concern and to facilitate its sale of the similarly advanced F-35 to Japan.

As some details of these leaks, the 2004 case occurred because personally-belonged laptop computers were longtime permitted to use in office at the MOD and the military's organizations and to bring back home with classified information installed. When file-sharing software was installed in one of such a computer and got infected with a disseminating virus, a great deal of classified information, including of U.S. origin, was digitally leaked.

As for the 2005 case, the *Yomiuri* of May 31, 2005, reported that, due to an accident, a submerged PLA Navy submarine was unable to navigate in the South China Sea. The newspaper's article included some classified information of U.S. origin.

As 2007 case, A lieutenant commander at the First Service School of the Maritime Self-Defense Force spread information on the AEGIS system to those without proper security clearance, first within the School and then beyond it, while fully aware that the special defense secrets, which is similar to U.S. top secrets, were included.

⁷ As the indivisible two sides of the same coin, the ministry also has to redefine the existing relationship of the internal bureau and the SDF in which the former maintains a strict bureaucratic control of the latter. Today, serious discussion on the need to enhance the military's roles at least at operational levels is underway, but the necessary organizational reform will not be possible without strong support of legislators who are elected in and represent the predominantly pacifist political culture of the postwar Japanese society. Reform is not

necessarily impossible but will be exceedingly difficult. As for the discussion on MOD reform, see, “Boeisho–Kaikaku no Hokousei (On a Direction of MOD Reform), August 31, 2013, available at <http://www.mod.go.jp/j/approach/others/kaikaku/index.html>.

⁸ As for three major leak incidents, see in the Endnote (5).

⁹ In the semi-formal hierarchical ranking order of the MOJ bureaucracy, the Public Prosecutor General is highest, followed by the Tokyo Superintendent Public Prosecutor, the Osaka Superintendent Public Prosecutor, Deputy Prosecutor Public Prosecutor, and Administrative Vice-Minister of Justice to all of which top ranking prosecutors have been appointed. A large majority of the MOJ Bureau Director-Generals are also high ranking prosecutors.

¹⁰ From a domestic law perspective, despite its significant military capability, the SDF resembles a police force that operates according to the positive list of authorization, in the sense that it is allowed to take action as specifically authorized by law. This is in contrast to the military that operates according to the negative list, in the sense that it is permitted to do whatever is necessary to do unless prohibited under international law. The SDF is not authorized to exercise the use of force, except the case of an act of necessity, such as self-defense, unless Prime Minister issues defense mobilization which requires either approval in advance of the Diet or, in the case of emergency, its *ex post facto* approval.

¹¹ Despite the conflict of the abovementioned bureaucratic interests, the GSOMIA of 2007 was made possible by strong initiatives of the ruling LDP, especially the defense policy caucus, known as Kokubo-Zoku, consisting of the first Defense Minister Fumio Kyuma, former Defense Agency’s Director-Generals and other ranking LDP legislators specializing in national security. The Kokubo-Zoku relied on the National Security Research Group (NSRG) and the U.S.-Japan Center for Peace and Cultural Exchange (CPCE) to lay almost all the necessary intellectual and organizational groundwork prior to intra-LDP policy review, Diet committee-level deliberation, and Cabinet’s formal decision to conclude the agreement. NSRG is a nonpartisan political organization of legislators, while CPCE is a policy advocacy non-profit organization whose members include academics and practitioners knowledgeable about security affairs.

The Office of Prosecutors punched a counterblow against NSRG and CPCE after the conclusion of the GSOMIA, which forced them dormant until recently. Naoki Akiyama, executive director of these organizations, was arrested and convicted on a charge of tax evasion for his non-profit activities in the U.S, while embroiled in a separate defense acquisition scandal centered on a case of bribery and corruption by a defense trade firm and then-Administrative Vice-Minister of Defense Takemasa Moriya.

Akiyama played a central role in organizing major defense policy discussions among legislators, bureaucrats, and industrialists, including one on the acquisition of Japan's missile defense system. In particular, through such non-profit activities, he served as the behind-the-scenes fixer who promoted the conclusion of the GSOMIA, which the Prosecutors probably saw challenged their privileged position in law. As the result, they suspected him, without a clear proof, as the first step to reach a greater defense acquisition scandal involving the LDP defense tribe and industrialists. The Akiyama's case suggests a case of the use of judicial system to advance bureaucratic interests.

As for the NSRG, see: <http://www.ja-nsrg.or.jp/>, accessed on September 1, 2013. Also, for the CPCE, see: <http://www.ja-cpce.jp/>. Naoki Akiyama, *Boei-Gigoku* (A Major Defense Acquisition Bribery Case That Has Become a Political Scandal), Tokyo: Kodansha, 2008.

^{1 2} “Tokutei-Himitsu no Hogo ni kansuru Houritsu-An no Gaiyo”, *op.cit.*

^{1 3} Under the existing laws, only classified military information is well protected with the maximum penalty of ten or five years' imprisonment. This is in accordance with the legal measures on U.S. classified information (or, the Special Criminal Law and the MSA Secret Protection Law) and the Self-Defense Force Law respectively.

The full name of the latter is the Special Criminal Law Attendant upon the Enforcement of the Agreement under Article VI of the Treaty of Mutual Cooperation and Security between Japan and the United States of America regarding Facilities and Areas and the Status of United States Armed Forces in Japan.

The 1952 Special Criminal Law imposes maximum ten year's imprisonment on those who detected or collected classified U.S. military information in order to use it for the purposes to damage the safety and security of the U.S. bases, facilities, and forces in Japan. The MSA Secret Protection Law inflicts the same imprisonment on those who leak “special defense secret”,

which is classified information on U.S. weapons and other equipment, for the purpose to damage Japan's security or to detect or collect the information by improper means. This act effectively covers offense of those in the defense industry who are engaged in license-production of U.S. weapons and equipment or in the maintenance and servicing of them. And, the Self-Defense Force Law imposes maximum five years' imprisonment on those who leak "defense secret", which is classified information on SDF weapons, equipment, doctrine, communications, and others. This law applies to offense committed not only by the MOD and the SDF personnel but also by those who made access to the information, including those in defense firms.

^{1 4} On May 31, 1978, the First Petty Bench of the Supreme Court established this ruling in the dismissal of final appeal of the accused in the case of a MOFA secret telegram leak.

^{1 5} The existing Japanese classification does not have the equivalent of "top secret", except the secret under the Special Criminal Law and "special defense secret" under the MSA Secret Protection Law, both of which deal with U.S. military information. Given the difference in the Japanese and the U.S. classification categories, the GOSMIA sets the rule in which Japan employ three classification categories even though there are only two under the existing laws. This means that, when released to the U.S., some Japanese "defense secrets" are designated as the equivalents of U.S. "top secret" or "secret". Japan's equivalents of U.S. "confidential" and those pieces of the unclassified information may be designated as the equivalents of U.S. "top secret", "secret," or "confidential"

^{1 6} To date, the MOD Directive on the Protection of Classified Information merely stipulates a list of executive members of the MOD and the SDF who shall appoint officials and officers in charge of the protection of classified information and that they then designate who shall have access to classified information. Yet, the Directive fails to provide specific procedural requirements of personal security clearance, particularly the criteria and procedures of the background checking. The MOD Special Contract on the Protection of Classified Information only requires contractors and their employees to pay due attention to information security without providing any procedural requirements of personal security clearance. The state of affairs is essentially true to the Directive on the Protection of Special Defense Secret and the Special Contract on the Protection of Special Defense Secret, except the general broad requirement of designating proper individuals in the handling of the Secret.