Defense Industrial Security Manual

(Provisional Translation)

July 2023

Acquisition, Technology and Logistics Agency (ATLA)
Ministry of Defense, Japan

Formulation of Defense Industrial Security Manual (DISM)

Japan is in demand to fundamentally reinforce its defense capability since the current security environment surrounding Japan becomes increasingly severe due to the unilateral changes to the status quo by force and such attempts and others. The Government of Japan made the cabinet decision on the Three Strategic Documents, e.g. National Security Strategy at the end of 2022. Given that the defense production and technology bases are involved in the entire life cycle of equipment and the equipment and defense industry are inseparable, the documents define Japan's defense industry as virtually integral part of a defense capability. In June 2023, the Japan's Diet enacted "the Act on Enhancing Defense Production and Technology Bases" which incorporates diverse supporting measures for defense industries.

At the same time, the defense industries are being exposed to the risks of intelligence activities by foreign countries, including cyber-attacks. In these circumstances, it is necessary for defense industries to develop, manufacture, and maintain defense equipment while protecting classified information of our national defense appropriately, and to participate in international equipment and technology cooperation while protecting classified information of the ally and like-minded countries. Protecting classified information appropriately by the defense industries, so called "Defense Industrial Security", is a prerequisite for defense production and international equipment cooperation.

Moreover, the Japan's defense industries are now becoming increasingly internationalized as Japan further participates in production and maintenance of advanced equipment introduced from the ally, joint research and development, and transfer of defense equipment. Such international cooperation of the defense industries requires the smooth sharing of classified information, which makes "the strengthening industrial security of Japan based on the international standards" a prerequisite.

Furthermore, Japan joined Multinational Industrial Security Working Group (MISWG) as the first Asian country as a member state this year in 2023. MISWG aims to standardize industrial security procedures among member states and contribute to the smooth implementation of international cooperation.

ATLA has now formulated the Defense Industrial Security Manual (DISM), which is equivalent to the industrial security programs and operation manuals of other countries. The DISM is a document which unifies information protection measures implemented in the defense industry based on laws, regulations, rules etc. concerning the protection of classified information that applies to the defense industry.

ATLA will distribute the DISM to the defense industries in Japan, and share it with the governments and defense industries of the ally and like-minded countries to strengthen defense production and technology bases including international equipment and technology cooperation.

Commissioner, ATLA
TSUCHIMOTO Hideki

Table of Contents

This manual is based on the regulations as of 1 July 2023. Since any modification thereafter is not included, it is requested to refer to the latest regulations as necessary.

INTRODUCTORY CHAPTER: Introduction to Defense Industrial Security

Section1. Defense Industrial Security System

Defense Industrial Security means that taking necessary measures for protecting classified information handled by companies which perform production, R&D, maintenance, repairs and other services related to defense equipment employed by the Japan Self-Defense Forces and Ministry of Defense (i.e. defense industry).

The defense industry, which performs duties such as production of defense equipment for ensuring defense capabilities exercised by the Self-Defense Forces, is the defense capability itself. Therefore, if any classified information handled by such industries is compromised, the national defense posture will be severely damaged.

The Japanese defense industry is exposed of the threats posed by intelligence activities of foreign countries, and there are various types of means for such activities including cyberattacks and HUMINT. It must be also noted that insider threats that may lead to damages can be caused by those who are able to access every asset of companies, including classified information, systems or facilities (whether they are the company employees or not), with malicious intent, for self-satisfaction or even without realizing it.

In this Defense Industrial Security Manual, the rules for protecting classified information applied to the defense industry, which consists of the Japanese defense capability itself, are prescribed.

Section2. Defense Industrial Security in line with the International Standards

The defense industrial security is required to effectively protect information to be classified from the Japanese national defense perspective, while being also an efficient system in order to achieve both strengthening of the Japanese defense industrial security posture and international cooperation.

In other words, it is required to focus on the “safety” of classified information to be protected from the foreign intelligence activities, as well as ensure “efficiency” to share the classified information reasonably and effectively with those who have Personnel Security Clearance (PSC) and Need-to-Know for smooth industrial activities and international equipment cooperation.

From this perspective, ATLA aims to establish rules for achieving both “safety” and “efficiency” in implementing the Japanese defense industrial security based on the international rules and practices for industrial security, which are commonly recognized among advanced countries.

Section3. “Defense Industrial Security Manual” and other related Regulations

The defense industrial security is established based on the Japanese security system explained in Chapter 1 of this manual. There are various legislative grounds such as the Act on the Protection of Specially Designated Secrets (Act No. 108 of 2013; hereinafter referred to as the "SDS Act"), the Act of the Protection of Secrets Incidental to the Mutual Defense Assistance Agreement (Act No. 166 of 1954; hereinafter referred to as “the MDA Act”), and The Self-Defense Forces Law (Act No. 165 of 1954). The defense industrial security regulations set by ATLA are established on the ground of these multiple laws, which make it a complicated system. This manual is established to reorganize the complicated defense industrial security system from the unified perspective so that it is easy to understand.

This manual describes the standard measures concerning defense industrial security, and it is not prohibited to take additional measures depending on the significance of classified information pertaining to defense equipment.

Although this manual is applied to the contract between defense contractors and ATLA, which consists the major part of the contracts involving classified information, the contract with the local supplying bases of the Japan Ground, Maritime or Air Force Self-Defense Forces is also covered by utilizing this manual as a reference.

CHAPTER 1. Security System

Section1. Introduction

Classified information within MOD is categorized into three types: Specially Designated Secrets (hereinafter referred to as “SDS”) based on “the Act on the protection of Specially Designated Secrets (hereinafter referred to as “the SDS Act”)”, MDA Secrets based on “the Act of the Protection of Secrets Incidental to the Mutual Defense Assistance Agreement (hereinafter referred to as “the MDA Act”)”, and “HI (Ministerial Secrets)” protected by “the Self-Defense Forces Law” and other laws and regulations. (Hereinafter SDS, MDA Secrets and HI are collectively referred to as “classified information”). Classified information is classified into each classification level that is substantially equivalent to the international classification of “Top Secret”,” Secret” and” Confidential”. The correspondence is generally as indicated by the below table;

MOD classification	International classification
Specially Designated Secret (KIMITSU)/ MDA Secret (KIMITSU)	TOP SECRET
Specially Designated Secret/ MDA Secret (GOKUHI)	SECRET
HI/MDA Secret (HI)	CONFIDENTIAL

* There are also markings of “CHUI (Sensitive)” and “BUNAI-KAGIRI (For Internal Use Only)”, which are equivalent to a part of “Restricted” and “Controlled Unclassified Information (CUI)” within unclassified information. When contractors handle these types of information, they must take measures to protect such “information to be protected” based on special security clauses.

Each head of Administrative Organs has the authority and responsibilities concerning the protection of SDS based on the SDS Act, and MDA Secrets based on the MDA Act. MOD and ATLA have established respective security regulations such as relevant Directives under each law. Therefore, regarding security measures applied to defense industries that handle classified information, there are JMOD internal regulations established under the multiple laws as described above.

Section2. Laws and Regulations on the Protection of Classified Information

The SDS Act, which is managed by the Cabinet Office, prescribes the protection of information concerning national security which is particularly required to be protected. The scope includes information held by the government of Japan concerning defense,

diplomacy, prevention of specified harmful activities (such as espionage) and prevention of terrorism; among the information, those particularly required to be protected is designated and marked as SDS. SDS is the unified security system applied to all ministries and agencies throughout the government of Japan based on the SDS Act.

MDA Secrets are undisclosed information such as structure, performance, technology concerning storage or repairs, method of use, items or quantity regarding equipment provided by the United States based on the Mutual Defense Assistance Agreement (hereinafter referred to as "MDA Agreement"). MDA Secrets are designated and managed based on the MDA Act. MDA Secret documents must be marked "MDA Secret" and its classification level – "KIMITSU (TOP SECRET)", "GOKUHI (SECRET) or "HI (CONFIDENTIAL).

Finally, "HI" is designated and managed based on the Defense Minister/ATLA Commissioner's Directives on the Protection of Classified Information, and protected by the laws such as the Self-Defense Forces Law. Information related to the national security or interests which should not be disclosed to those who are not relevant personnel is designated as "HI". The materials designated as "HI" must be marked as such. "HI" is also called "Ministerial Secret" or "Agency Secret" in the course of duties.

Section3. Protection of Classified Information based on Contract

When defense contractors handle classified information, ATLA must award a contract with them, to which the special security clauses according to the classification of the information is attached.

By awarding such a contract, contractors are obliged to take appropriate security measures in accordance with the laws and regulations concerning the protection of classified information.

Specifically, in accordance with the provisions on the protective measures contained in the special security clauses for each classification, they are required to establish in-house security regulations and security facilities for handling classified information, implement security education for the designated employees who handle classified information, receive periodic security inspections of ATLA, and take measures to handle classified information on their IT system.

The contract for protecting classified information includes not only the contract for productions that entails financial transactions, but also the contract exclusively for the protection of classified information without payment.

Section4. Penalties

In case where an individual involved in compromise of classified information, criminal

penalties (including imprisonment for up to 10 years) can be applied under the SDS Act, the MDA Act, etc.

In addition, ATLA obligates contractors to establish procedures for disciplinary actions applied to the employees who breached the in-house security regulations, and ensure the implementation based on the “Guidelines for the Security of Classified Information in Procuring Equipment/Services”.

Furthermore, the contract involving classified information contains the clause for monetary penalty in principle. If ATLA verifies the fact that the contractor compromised classified information, monetary penalty up to 60% of the contracting price is imposed on the contractor.

Section5. Termination of Handling of Classified Information

The contractor shall, in principle, immediately submit to ATLA classified materials, (including documents, objects, and objects embodying the classified information") etc. after the termination of the contract. When ATLA considers it is appropriate to get the contractors to cease working with classified information, in case such as they compromised the information, ATLA provides instructions on return, disposition or other necessary measures, with which the contractors must comply.

CHAPTER 2. Security Qualification for Bidding (FOCI)

Section1. Security Evaluation before Bidding

In order to participate in a bidding for a contract that involves classified information or information to be protected, companies must be accredited by ATLA before the bidding that they will ensure an appropriate in-house system and appropriate employees who handle classified information to perform the contract, including FOCI (Foreign Ownership, Control or Influence).

Companies which hope to participate in the bidding are required to submit some documents described in the next section before the bidding takes place.

Section2. Documents Required for Security Evaluation

In order to conduct the above evaluation, ATLA requests the companies to submit the following documents by the deadline set before the bidding:

1. A list of employees involved with the performance of the contract (including name, title, personal history, educational record, native language, nationality, etc.)
2. In-house regulations that prohibit uncleared employees (including board members) from accessing any classified information; the regulations also include the provisions that physically/institutionally separate the organization performing the contract within the company, and effectively deny unauthorized access of uncleared employees.
3. Contracting/capital relationships with a parent company or other companies (including foreign entities) which have any potential influence on the contractor
4. Verification that the company will not share any sensitive information (classified information and “information to be protected”) with the above parent company or other companies

Section3. Actions against Security Concerns

Based on the documents submitted by the companies, ATLA confirms whether the company complies with the requirements from the perspectives of the relationship with foreign entities and the security system.

If the company does not comply with the requirements, ATLA requests the company to take corrective measures such as establishing regulations necessary for an appropriate security systemin order to ensure the company satisfies the requirements.

In case where the company fails to comply with the requirements, it’s not allowed to participate in the bidding.

When there is any change in the matters submitted in the process described in Section2, the company must resubmit necessary documents even in the middle of a contract period.

CHAPTER 3. Facility Security Clearance

Section1. Application for Facility Security Clearance

In order to handle classified information, companies are required to be granted “Facility Security Clearance (FSC)”. Companies which have been granted FSC are called “cleared contractor”.

Companies must apply to ATLA via the competent Regional Defense Bureau in order to handle classified information. FSC will be granted to the company after ATLA (Security Authority) approved the application. In principle, companies are able to submit the application after the tender notice of the contract in which they are willing to participate.

Companies may coordinate with ATLA (Security Authority) via RDBs in advance.

With regard to SDS, the companies must apply for FSC to Director General, Department of Equipment Policy, and they are referred to as “Eligible Contractor” when granted FSC based on the SDS Act.

Companies must apply for FSC as for each classification of Hi, MDA Secrets and SDS.

Section2. Application Contents

This section prescribes the required contents of application for FSC.

Companies must submit information regarding Facility Security Officer, in-house security regulations, security education and security facilities.

1. Facility Security Officer (FSO)

   When applying for FSC, companies must appoint FSO who has the general responsibilities for taking security measures according to each classification level instructed by ATLA. With regard to SDS, FSO is also referred to as “SDS manager”.

   (1) FSO qualification

   FSO must be an employee of the contractor holding FSC, and have Personnel Security Clearance (PSC) at the level of the FSC. FSO is also required to have necessary knowledge in performing duties for protecting classified information obtained through the training using materials authorized by ATLA and his/her experiences. In addition, FSO must be responsible for management of duties concerning the protection of classified information by generally administrating the performance of the contract with ATLA.

   (2) FSO responsibilities

   FSO roles and responsibilities:

   - Selecting and assigning employees handling classified information according to Need-to-Know principle.

- Providing security education to the employees to discipline the security rules
- Taking security measures at security facilities
- Protecting Information Systems processing classified information
- Implementing security reviews and taking corrective measures if necessary and
- Cooperating with security inspections that RDB's officials perform.

(3) Security Organization

FSO must ensure security of classified information by establishing effective security organization to implement security measures within the company.

FSO is required to establish security organization inside departments such as design, manufacturing and other duties involving access to classified information directly. FSO must also establish a dedicated department responsible for establishing in-house security regulation and conducting security education and in-house security inspections.

FSO must appoint the following roles from the department performing designs, manufacturing and other duties by directly accessing classified information. These positions must be assumed by those who has appropriate PSC described in Chapter 5.

(a) Administrative manager

Administrative manager will supervise employees who handle classified information through security manager.

(b) Security manager

Security manager will supervise employees who handle classified information, and performing duties for managing classified information.

(c) Deputy security manager (appointed if necessary)

In the absence of the security manager, deputy security manager assumes his/her duties.

(d) Handling employees

Handling employees refer to those who perform duties (ex. design works, productions, etc.) involving classified information.

2. Security regulations

Companies applying for FSC must develop their in-house security regulations and security procedures (hereinafter collectively referred to as “security regulations”).

The detailed contents of the security regulations are specified in the special security clauses and other ATLA regulations (including instructions and security guidelines) which constitute the contract.

The in-house security regulations must include main provisions below:

(1) Necessary information for in-house security regulations

(2) Prohibition of inappropriate extended interpretation of the regulations concerning handling of classified information

(3) Consultations if any debt arises in interpreting/operating the in-house security regulations

(4) Security organization, appointment of relevant cleared employees and their duties

(5) Security measures for the protection of classified information

(6) Providing/receiving, storage, lending of and access to classified information

(7) Transmission/transportation of classified information

(8) Inspection and reporting

(9) Duplication, creation, photographing and markings of classified information

(10) Designation of classified information

(11) Security measures applied to subcontractors

(12) Security facilities

(13) Return and disposition of classified information

(14) Response and report in case of emergency or security incidents

(15) Details of the in-house security regulations

The security procedures must include main items below:

(1) Purposes and general concepts

(2) Definitions of terms

(3) Applicability of the security procedures

(4) In-house security regulations

(5) Prohibition against disclosing classified information to the third party

(6) Organizational security

(7) Classification and management of classified material

(8) Personnel security

(9) Response to security incidents including compromise

(10) Physical and environmental security

(11) Communications and operational management

(12) Access control

(13) Verification and modification

(14) Receiving official security inspections and investigation

3. Security education

It is mandatory for relevant cleared employees (employees who were designated by FSO and approved by JMOD, having PSC described in Chapter5 and Need-to-Know) to take security education to acquire required knowledge for protecting classified information, including how to handle classified materials at FSC applying companies.

In order to meet this requirement, the companies must submit documents indicating that:

(1) The company has established (or to be deemed possible to establish) the personnel/ physical system to conduct annual security education.

(2) Security education material shall include necessary information for protecting classified information.

(3) The education is provided by persons with specialized knowledge.

4. Security facilities

Companies applying for FSC must have security facilities that prevents theft of/ surreptitious glance at classified materials when receiving such materials necessary for performing a contract.

When establishing security facilities, companies must submit documents such as detailed drawings that represent locations and structures of the facilities (including appendices if any) along with an application form to get an approval.

After submitting the documents, Regional Defense Bureaus conduct on-site security inspections before the approval is granted. The companies must cooperate with RDB to conduct the security inspections.

In case where the company handles classified information only within government facilities or facilities at other entities (such as its prime contractor), it is not required to establish security facilities.

The detailed structural standards will be described in Chapter 10, Section 2.

Section3. Notification of Inspection Results

If the above application is determined appropriate by ATLA through the inspection, ATLA notifies the company that FSC is granted in writing.

The company must retain the notification document appropriately in order to proceed the

process thereinafter with the document number and the issued date.

Section4. Changes of Submitted Information

When cleared contractors (Eligible Contractors for SDS) need to modify their security measures based on which the FSC was granted, they must apply for an approval for the modifications. When modifying security facilities, they are required to obtain an approval from ATLA before starting construction.

Provided that the modification is due to the below factors, the contractors only have to notify ATLA of the modification. In this case, it is not necessary to obtain an approval from ATLA.

(1) Revisions of ATLA regulations

(2) Changes in the name of their businesses, departments, positions, etc.

(3) Other changes that do not affect their security measures

In case of mergers, consolidation or relocation of the company, it is mandatory to the contractors to make a new application or change application.

Section5. Application Process for Another Contract

In case where contractors employ the same security regulations, education materials or security facilities which have been already approved by ATLA for new contract, it is not necessary to obtain new approval and they only have to notice the document number and the issued date regarding the past approval.

Section6. Termination of Security Facilities

Contractors may terminate the security facility once approved by ATLA that are no longer expected to be utilized.

If they plan to use the facility that was once terminated, they must apply for the use of that facility again.

Section7. Review of Security Regulations

In order to ensure sufficient security, contractors are required to continuously review their security measures, including in-house security documents, organizations, management status and security education, and improve them as necessary.

When they have to revise their security regulations according to the change in the circumstances, they must perform appropriate procedures as described in Section 4 of this Chapter.

CHAPTER 4. Contract for Protection of Classified Information

Section1. Security Obligation

As explained in Section 3 of Chapter 1, it is mandatory for contractors to take security measures based on the contract attached with special security clauses. Accordingly, their security obligations arise on the date of concluding the contract.

Section2. Access to Classified Document before Bidding

ATLA may allow companies willing to participate in the bidding concerning equipment to disclose specifications containing classified information, even before the contract formed. More specifically, companies submit an oath and attach company's security regulation, for asking permission to access specifications containing classified information (access only, no recording is permitted) before bidding. This oath is a kind of contract for protecting classified information, and has the legal effect to impose security measures on the company. Therefore, if the company compromises the classified information, they have to bear civil liability.

In addition, ATLA also takes the Need-to-Know of the company into consideration, and the company must have the FSC. The personnel who will access the classified information also must have PSC. If the company does not have the FSC and PSC, they must apply to ATLA as described in Chapter 3 and Chapter 5.

Section3. Contract for Protecting Classified Information without Payment/Production or Other Services

Besides the disclosure before the bidding described in Section 2, if companies which are not in a contract with ATLA have the Need-to-Know of classified information held by JMOD/ATLA, they may be allowed to access the classified information under a contract without payment exclusively for protecting classified information. In this Manual, "without payment" means that there is no any financial payment by ATLA to a company in exchange for performing contract.

This contract has the legal effect to impose security measures on the company. In case the company compromises the classified information, they have to bear criminal and/or civil liability depending on the classification. In addition, ATLA also takes the Need-to-Know principle of the company into consideration, and the company must have the FSC. The individuals who will access the classified information also must have PSC. If the company does not have the FSC and PSC, they must apply to ATLA (the manager of the classified information or their supervisor) as described in Chapter 3 and Chapter 5.

CHAPTER 5. Personnel Security Clearance

Section1. Personnel Security Clearance

The individuals who handle classified information must hold an appropriate Personnel Security Clearance (PSC) according to the classification level of the classified information. PSC will be granted after the contract involving classified information is awarded.

PSC, which is an eligibility required for government officials and contractor employees to access classified information, is also defined in the General Security of (Military) Information Security Agreement concluded with other countries and organizations.

PSC may be granted to employees of contractors holding FSC who are eligible to handle classified information via an evaluation process.

In order to access classified information based on a contract, an individual shall have PSC and be confirmed a need based on Need-to-Know principle related to the information, as well as registered on the relevant cleared employees list.

Section2. Process to Obtain Personnel Security Clearance

PSC is granted in accordance with “Guidelines for the Security of Classified Information in Procuring Equipment/Services” in the course of the confirmation process of the list of relevant cleared employees who are expected to handle classified information after the contract involving classified information is awarded.

FSO selects candidates for relevant cleared employees who are expected to handle classified information and has them follow the procedures to apply for PSC.

The employees who are expected to handle SDS will undergo “Security Clearance Assessment for SDS”, which is a process for evaluating eligibility for handling SDS, based on “Standards to Ensure Uniform Implementation in Connection with the Designation of Specially Designated Secrets and the Termination of the Designation as Well as the Conduct of the Security Clearance Assessment” (Decided by the Cabinet on October 14, 2016. Hereinafter referred to as “Implementation Standards”).

In the process of the Security Clearance Assessment for SDS, the employees who are required to handle SDS fill out a Questionnaire and submit it to ATLA in accordance with the SDS Act and the Implementation Standards. ATLA (Security Authority) evaluates the Questionnaire and notify the result to the applicant. The employees who are considered to be eligible will be granted PSC for SDS. After it is determined that they have the necessity to handle the SDS, they will be registered on the list of relevant cleared employees.

With regard to the contract involving MDA Secrets and HI, contractors must submit a list

of candidates for relevant cleared employees, which is developed by FSO and includes information of characteristics/personalities of the individual employees, to ATLA. Based on the submitted information (and any additional information as necessary), ATLA evaluates whether the employees are eligible to be granted PSC.

Section3. Validity of Personnel Security Clearance

If the employees have already been granted PSC for a certain security classification based on the existing contract and valid, they are allowed to handle the same level of classified information. When it is considered by FSO that they also have to perform duties for another contract, they may be also registered on the list of relevant cleared employees for that contract after approved by ATLA.

The FSO must confirm whether there are any changes in the circumstances of individual employees on/off their working time that are considered inappropriate for handling classified information by taking opportunities such as personnel interviews, even if they have been once granted PSC and registered as relevant cleared employees. The contractor employees who have been granted PSC are obliged to self-report any changes in their circumstances. The FSO must ensure that the employees are aware of their obligation in security trainings. The FSO must also continuously monitor individual situations of the employees through such opportunities as annual personnel interviews by their supervisors, and if there are any changes in the situation, they must report them to ATLA.

Section4. Pledge by Relevant Cleared Employees

Before the relevant cleared employees start to handle classified information, the FSO must set the provisions concerning the criminal/civil liability in case of compromising classified information to clarify their responsibilities for protecting classified information, as well as have the relevant cleared employees submit a written pledge for protecting classified information during their duties and after retirement.

If an employee refused to perform the duties handling classified information, they must not be registered as a relevant cleared employee, or must be withdrawn from the registration when the employee has already been registered.

CHAPTER 6. Security Education Implementation

Section1. Security Education before Handling Classified Information

After approved on the list of relevant cleared employees as explained in Chapter 5 by ATLA, FSO must provide security education to the employees before they start to handle classified information, based on the material developed in accordance with Section 2 of Chapter 3.

The education is also provided to those who are newly designated as a relevant cleared employee during the period of the contract because of hiring, transfers or any other reasons.

Section2. Periodic Education and Training

FSO must provide security education to all the relevant cleared employees at least annually, including the education described in the above section. Regular education to the extent necessary must be also provided to all employees of contractors. FSO also must provide trainings aligned with the above education for each specific site.

Section3. Education and Training Contents

FSO must cover all the below items during a security education;

(1) Text of the Laws, Orders, Instructions, Notifications and other relevant regulations on classified information and the detailed explanations

(2) Need for protecting classified information (including international/domestic influence in case of compromise)

(3) Significance of security education

(4) Roles and responsibilities of relevant cleared employees

(5) Response to emergency situation

(6) How to handle classified information (including providing/receiving classified information, creation, transmission, access, handover, inspection, subcontracting, etc.)

(7) How to set, manage and access restricted areas

(8) Security of information processed on computers

(9) Countermeasures in protecting classified information (including case examples in other countries and counterintelligence)

(10) Ensuring implementation of in-house regulations, guarded work attitude and discreet activities in private life

(11) Other points of concern (including self-reporting of any changes in circumstances)

In addition to lectures, practical training (such as emergency exercise) must be also implemented. RDBs ensure that the training materials used by contractors are developed

based on the standards provided by ATLA. The contractors must obtain an approval on the training materials from ATLA through RDBs.

ATLA supports contractor's security education by some means such as providing education materials concerning counterintelligence.

Section4. Record of Education

It is mandatory for FSO to maintain a record of the education and training conducted based on Section 1 and 2 of this chapter, and to report the implementing status to ATLA based on the special security clauses. RDBs will confirm the implementation of the education and training at the security inspections.

CHAPTER 7. Providing and Receiving Classified Material

Section1. Application for Borrowing Classified Material

Contractors met the requirement described in the preceding chapters may make an application to lend classified materials specified in the specifications after signing a contract. The application should be made to ATLA.

Upon the request, ATLA consults with the department which hold the classified material and answers whether it can be lent to the contractor.

Section2. Receiving Classified Material

Contractors must ensure that classified materials are received by the designated relevant cleared employees in accordance with the below procedures;

(1) When receiving classified materials, a contractor ensures that the classified materials provided by ATLA are consistent with a transmittal letter.

(2) The contractor submits a receipt (or other necessary documents) to ATLA

(3) ATLA maintains a register of the classified materials provided to the contractor.

(4) The contractor brings the classified materials to its own security facility and record on a booklet for storing classified materials.

After bringing the classified material into its own security facilities and confirming whether there are any problems by comparing the classified documents with the transmittal letter, the contractor must report to ATLA that it has received the classified material.

Section3. Hand-Carrying of Classified Material

The classified information received in accordance with Section 2 must be hand-carried by the relevant cleared employees to the security facilities by the relevant cleared employees. In case of SDS or MDA Secret, the information must be hand-carried by two or more relevant cleared employees.

Classified documents must be sealed in an opaque envelop with the classification markings applied to the classified documents. The envelop must be sealed in an outer envelope without any markings that indicate the classification. This double-wrapped envelope must be hand-carried with a lockable container that cannot be seen from the outside.

In case where it is difficult to follow the above method, they can be hand-carried in another way with an approval from ATLA.

When classified material is required to be hand-carried to places other than the security facilities of the contractor, they must obtain an approval from ATLA unless there are no provisions in the contract.

Section4. Transporting Classified Item

When contractors transporting a classified item that cannot be wrapped by an envelope because of its size, weight and other characteristics, they must take appropriate measures to prevent compromise by such a method as tightly wrapping the item.

In case where they have to use commercial freight carrier due to the size, weight or other physical characteristics of the item, the contractor must obtain an approval from ATLA. If the commercial carrier cannot recognize the classified item from the outside of the package, it is not considered to access classified information. Even in this case, however, the contractor ensures that relevant cleared employees accompany the item during transportation so that they can respond to incidents, including in case where the package is damaged and the classified item is exposed.

If the commercial carrier possibly accesses classified information, for example when packaging the classified item, it must have FSC. In this case, if relevant cleared employees of the commercial carrier transport the item, the contractor is not required to accompany the item.

Section5. Storage of Classified Material

When contractors receive classified material, they must store it within security containers located in their security facilities.

Security manager is also required to store classified materials in a centralized storage as possible.

If it is difficult to store classified items in the storage container, they must be vaulted.

The requirements of security facilities, vaults and security containers are outlined in Section 2 of Chapter 10.

Section6. Reciprocal Use of Classified Material

When it is necessary for contractors to use classified materials stored in their security facilities for performing another contract, they can reciprocally use the materials. This is based on the concept that it is more secure to use the same classified documents for multiple contracts as much as possible than duplicating the documents.

The contractor can reciprocally use classified materials only after ATLA coordinating with the manager of the classified material and obtaining his/her consent. The reciprocal use is allowed during the period of the original contract.

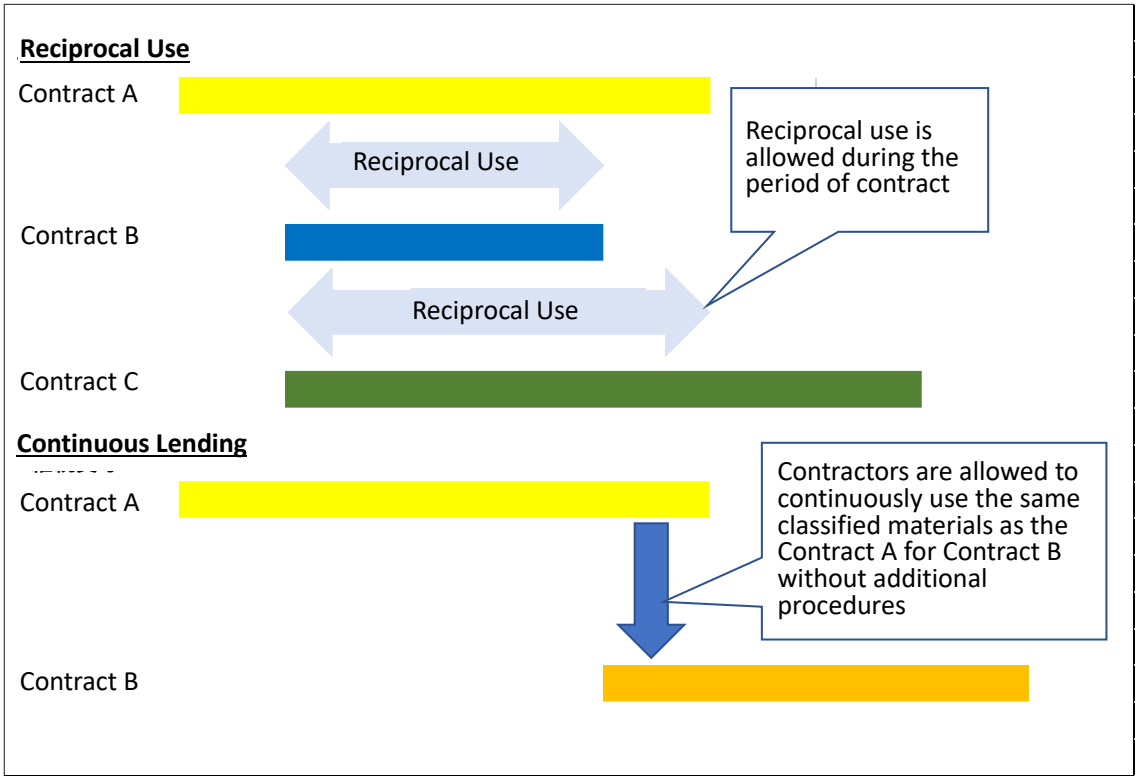
Section7. Continuous Lending of Classified Material

There are some cases where the same classified materials are recognized to be lent

without substantial transfer, including return or submit of the classified materials to ATLA after the end of the contract, for instance when the contractor has multiple contracts for the same project or the same kind of contract every year.

This provision is for avoiding the risk of compromise during transportation from security facilities of contractors.

[Comparison of Reciprocal Use and Continuous Lending]



CHAPTER 8. Access to Classified Material

Section1. Access to Classified Material

It is mandatory for companies to list the relevant employees' name by every project approved by ATLA dealing with classified Information.

When contractors let their relevant cleared employees access classified materials stored in security facilities, they must ensure that the employees are eligible for access the classified information holding PSC and Need-to-Know, with the permission for the individual access, which is essential to the accomplishment of the contract.

It is mandatory for relevant employees to fill in required information on a record book, and for security managers to confirm and fill in check done.

The employees must access the classified materials basically only within the security facilities. If it is necessary to access outside the security facilities, they must also proceed with the procedures described in the next section.

The above procedures are also applied to the case where the relevant cleared employees of other companies (for example subcontractors) access classified information.

Section2. Lending of Classified Material

It is necessary for contractors to take lending process when it takes classified materials to other security facilities from their own ones. Contractors must confirm that borrowers are relevant cleared employees and need to use the classified materials on contract.

It is mandatory for the borrowers to fill in required information on a record book, and for security managers to confirm and fill in check done.

The above procedures are also applied to the case where the relevant cleared employees of other companies access classified information.

Section3. Transmission of Classified Information

Transmitting classified information orally between relevant cleared employees must be done within security facilities. In this case, they must clarify that the information is classified and take measures to prohibit writing down or audibly recording.

The contractors must strictly prohibit their relevant cleared employees from referring to classified information in public transportation or other public places, including on the phone call.

CHAPTER 9. Creating/Marking Classified Material

Section1. Application of Creating Classified Material / Applying Control Number

When contractors create or duplicate classified materials, they must make an application and obtain an approval from ATLA in advance. The scope of secret included documents and quantity of the materials to be created or duplicated must be limited to the minimum necessary.

In case there are contractual provisions that specify creating or duplicating the classified materials, they do not have to obtain further approval.

Contractors must obtain a control number from ATLA applied created or duplicated secret documents.

Section2. Witness by Government Official When Creating Classified Material

Contractors must create classified materials only within security facilities, with witness by government officials (e.g. security officers from RDBs). Therefore, contractors must carefully coordinate with the government on creating classified materials.

Section3. Handling of Classified Material during Creation

If the materials being created are expected to be classified after completion, contractors must treat them as equivalent as classified information.

In case that it takes considerable time to create the classified material for reasons such as analysis, the witness by government officials (e.g. security officers from RDBs) is not required while processing materials if instructed by ATLA.

However, in the final stage of completing the creation, there must be the witness by government officials (e.g. security officers from RDBs) as described above.

Section4. Classification Markings

Contractors must apply markings to the classified materials that they have created or duplicated according to the security classification.

According to the contractual conditions or instructions by ATLA, one of the following markings will be applied; “TOKUTEI HIMITSU (Specially Designated Secrets)”, “TOKUTEI HIMITSU (Specially Designated Secrets) (KIMITSU)”, “TOKUBETU BOEI HIMITSU (MDA Secrets) (KIMITSU)”, “TOKUBETU BOEI HIMITSU (MDA Secrets) (GOKUHI)”, “TOKUBETU BOEI HIMITSU (MDA Secrets) (HI)” or “HI”.

In case of classified documents, it is necessary to apply classification markings in red on the upper right and the lower left of the front and the back cover, as well as the pages that contain classified information. It may be also required to clearly indicate what information

on that page is classified; for classified sentence, it can be underlined/ encircled; for pictures, photographs, figures or tables, they can be surrounded by red frames. In case of classified items, markings will be displayed as appropriate. If it is not physically possible to display the markings on documents or items, contractors must inform their relevant cleared employees of the classification by issuing notification document.

For classified information provided by foreign governments, they must maintain the markings applied by the foreign government, while applying the above classification marking.

Section5. Control Number/Serial Number

Contractors must display the following factors on the upper left of the front cover (in case of documents) or any other appropriate place as instructed in the procedures described in Section1 of this Chapter: the control number, the serial number, the number of pages and the designating conditions.

In case of SDS, the designation number must be also included in the markings.

The designation authority or the responsible department is indicated by the control number.

Section6. Modification on Classification Markings

Contractors must apply any changes in the security markings including the classification and designating conditions when instructed by ATLA in writing.

When requested by ATLA, contractors must return classified materials to ATLA in order to apply the changes in the markings.

Section7. Disposition of Working Papers during Creation

When contractors created interim working papers that include classified information practically, they must deal with care the papers equivalent to a classified information in order not to be detected or collected.

Contractors must dispose working papers in the same way as other classified materials, ensuring that the classified information contained in the papers cannot be reconstructed.

CHAPTER 10. Security Facilities

Section1. Security Facilities

It is mandatory for contractors to handle classified information only within security facilities.

The generic term of “security facilities” represents facilities which classified materials are stored in security containers, closed areas which are designated for a certain period necessary for handling classified information (such as for performance evaluation), storages and vault used in case where the classified items cannot be stored in security containers.

Section2. Structural Standards for Security Facilities

The structural standards for security facilities to protect classified items are listed below. Although those requirements are also applied to the closed areas basically, contractors may take alternative measures by ensuring the equivalent level of protection and considering the characteristics of the facilities on the case-by-case basis, under the instruction of ATLA.

1. Ceilings, Walls and Floors

Ceilings, walls and floors must be constructed of reinforced concrete or sturdy non-flammable material. In case rooms are connected with each other by the space between the ceiling and the roof, they must be separated by sturdy non-flammable material.

2. Partition

If a room can be seen from the outside when the door is open, partitions or curtains must be installed.

3. Entrance

There must be only one entrance in principle. Lightings (night lights) on the entrance/exit doors must keep functioning even in the case of power failure.

In case that it is not possible to carry in/out instruments by that entrance, an additional shipping/receiving entrance can be installed.

If necessary, there can be also emergency doors which can be opened from the inside.

4. Doors and Locks

Doors for entrance, shipping/receiving entrance or emergency exits must be made of steel in principle. In case of double doors, there must be astragals on the joint parts.

If it is necessary to install observation windows, the room must not be seen from the outside through the windows.

The entrance door and the shipping/receiving door must be double-locked with 3-position dial mechanical combination lock (combination patterns more than 100^3) and key-operated lock. As an alternative measure, however, more stringent locking device such as biometric authentication device instead of the mechanical combination lock.

Emergency escape mechanism must be installed in case of emergency.

5. Windows

Windows must not be installed in principle. When it is unavoidable to install windows, they must be limited to the minimum and furnished with iron bars with the diameter of 13mm or more and the intervals of 10cm or more, conforming to the Japanese Industrial Standards (JIS). The window glass must be opaque with a layer of wire netting or simply opaque.

6. Openings/ventilation/duct

To prevent trespassing, snooping or eavesdropping, ducts, ceiling windows, drains, tunnels and other openings must be installed with wire netting or iron bars with the diameter of 13mm or more, with intervals less than 10cm, conforming to JIS.

7. Alarm System

There must be an automatic alarm system that detects opening/closing of the door and intrusions. The alarm system must be directly connected to security control center and set off even in the case of power failure. Wiring must not be cut off easily, and even in case of that, the system must alarm when disconnected.

8. Perimeter

Perimeter must be established on fixed concrete foundation to prevent unauthorized access security facilities. According to circumstances, 2 meters or higher fence topped with barbed wires or IR sensors is required.

The perimeter fence must be installed around security facilities or the entire area including the facilities.

The perimeter fence is not required when an alternative measure for protecting classified information are taken. Such an alternative measure must be considered on the case-by-case basis taking the characteristics of the facility into consideration, and approved by ATLA.

9. Security Containers

Classified materials must be stored in the following security containers depending on the classification: for MDA Secrets (KIMITSU), a safe lockable with three position dial combination lock, for MDA Secrets (GOKUHI) and SDS, a steel box lockable with three position dial combination lock, for HI, a steel box lockable with dial combination lock; and for MDA Secrets (HI), a lockable steel box.

The security containers must not have any labels on the outside indicating they contain classified materials.

10. Peripheral Control Areas

In order to prevent unauthorized access to security facilities, peripheral control areas must be designated and its access to the areas will be strictly controlled.

Section3. Management of Security Facilities

Contractors must take the following measures to appropriately manage their security facilities.

1. Daily Check of Security Facilities

In order to ensure that their security materials and facilities are secured, contractors must confirm the facilities every working days.

2. Key Control

The keys for security facilities and security containers must be controlled by those who are authorized by FSO during working hours. Outside the working hours, they must be stored in a container within the security control office.

The key for the container storing keys must be secured by those who are authorized by FSO.

The number of keys and those who use the keys must be limited to the minimum necessary.

FSO should take appropriate measures to reduce potential risks, which may include the followings as examples:

- Prohibition of creating a master key
- Establishing procedures to duplicate a key
- Protection of keys and locks equivalent to that of classified materials
- Audit for keys and key-operated locks on a periodic basis

- Inventory of keys with each change of custody

3. Passcode for Security Containers

The passcode for security containers must be controlled by the limited relevant cleared employees authorized by FSO. The passcode and the key for the security containers must be managed by different relevant cleared employees so that classified materials will not be theft or glanced by one employee solo.

The passcode must be changed at least annually and at specific timings such as;

(1) When the security container is initially used
(2) When a relevant cleared employee who knows the passcode leaves the company or transfers to another department
(3) When the passcode is compromised or suspected to be compromised

4. Maintenance of Security Facilities

When maintenance personnel other than relevant cleared employees is necessary to access security facilities, they must go through the procedures explained later in Chapter 12 in advance.

CHAPTER 11. Information System Processing Classified Information

Section1. Provisions on Information System

Information systems used by contractors for creating or handling classified information must be appropriately managed in order to prevent compromise.

There are mainly the following requirements for information system:

1. Personnel Security
2. Physical and Environmental Security
3. Communications and Operational Control
4. Access Control
5. Verification and Improvement

Section2. Personnel Security

1. Users of Information System

Contractors must designate appropriate personnel as the users of information system to process classified information within the minimum necessary range. The contractors must also ensure that the users comply with security regulations.

2. Educations to prevent infections to malicious software

Contractors must ensure that their relevant cleared employees are aware of the risk of being infected with malicious software through portable storage media. They must also implement and record periodic education necessary for taking appropriate security measures on their information system.

Section3. Physical and Environmental Security

1. Implementation Planning for the System Security

Contractors must develop the Implementation Planning for the System Security (hereinafter referred to as “Implementation Plan”) and update it as necessary when processing classified information on their information system.

The implementation plan includes the items below, and will be subject to the monthly security inspection.

(1) Configuration list of classified information system for verification

Contractors must prepare a list of components of classified information system including types and versions of hardware, software, network and storage media in order to accurately identify and verify the status of the components.

(2) Operating procedures

Contractors must establish operating procedures regarding the information system utilized within their security facilities so that their relevant cleared employees are able to always refer to them.

(3) Access control policy

Contractors must develop an access control policy that stipulates what types of classified information their relevant cleared employees are authorized to access, and what kind of functions of the information system they are able to utilize according to their positions.

(4) Flow chart of classified data

Contractors must develop a flow chart of classified data processed on the information system in order to ensure that the classified data will not be flown outside the security facilities.

(5) Organization chart for information system security

Contractors must prepare an organizational chart that shows the detailed responsibilities of their employees to clarify who are responsible for the system security of the information system.

(6) Other necessary matters

If the documents from (1) to (5) are insufficient to ensure that the classified data on the network of the information system will not be flown outside the security facilities, contractors must prepare additional documents.

2. Information system taken outside security facilities

Classified information system must be permanently installed within security facilities, and must not be taken outside in principle. Contractors must take necessary measures to prevent an unauthorized taking outside. For instance, when it is unavoidable to take the information system outside the facilities to be repaired or disposed, they must prevent compromise of classified information by such means as physically destroying storage media.

In order to prevent an unauthorized taking outside of information system, contractors must take necessary measures such as fixing the information system by security cables. In

addition, when maintenance personnel repair the information system within the security facilities, the relevant cleared employee designated by FSO must oversee the repair work. It is important to take protective measures in accordance with the actual conditions of the contractors including their duties in order to prevent compromise of classified information. For instance, depending on the circumstances, it would also be required to conduct a baggage inspection at an entrance when entering and leaving the security facilities.

3. Information system brought to security facilities

Contractors must prohibit bringing information system, including portable communication device (e.g. laptops and mobile phones), other than those permanently installed within security facilities in principle. When it is unavoidable to bring information system into the facilities, it is necessary to take measures to prevent compromise of classified information, as well as fill out a record with necessary items. In addition, FSO must ensure that the portable device to be brought to the security facilities is not for a private use before permitting.

Section4. Communications and Operational Control

1. Communications

Classified information system must be stand-alone or only connected to wired network within security facilities, and must not be connected with any networks or devices outside those facilities in principle. It must also be prohibited to use wireless network connection (including wireless keyboard and mouse) within the security facilities.

2. Software to be installed on information system

In order to protect classified information system from malicious software, contractors can only install the minimum software necessary for their duties on their classified information system, and take measures such as utilizing the latest version of anti-virus software that detects malicious software.

3. Maintenance of information system

Contractors must develop a maintenance plan and conduct maintenance (including inspection, diagnosis, repair and updates) of their classified information system based on the plan periodically and as necessary. The maintenance plan must include who will conduct the maintenance, what system will be the subject to the maintenance, what kind of maintenance will be conducted and other necessary items.

When conducting the maintenance, FSO or their designee must witness and oversee the maintenance. They also must maintain records of the maintenance including when the maintenance is conducted, the list of maintenance personnel, the system subject to the maintenance and the details of the maintenance works.

4. Outsourcing of maintenance of information system

Maintenance of classified information must not be outsourced to entities other than cleared contractors in principle. When it is unavoidable to outsource to such entities, contractors must clearly oblige the outsourcing contractor to meet the security requirements. In this case, they also must prevent the access to security facilities without an approval by the RDBs in advance, as well as prohibit the outsourcing contractor from being exposed to classified information.

5. Portable storage media

When handling classified information in the form of electronic data, contractors must store it in portable storage media in principle.

Contractors must establish procedures for managing portable storage media, and inform them of their relevant cleared employees. The procedures must include the followings;

- When relevant cleared employees use portable storage media, FSO or their designee must grant an approval each time; the record of lending/returning of portable storage media must be maintained;
- When storing data in portable storage media, the data must be encrypted by e-Government recommended encryptions; the cryptographic key must be strictly controlled and; the data stored in the portable storage media must be appropriately copied or disposed.

Section5. Access Control

1. Access control policy

Contractors must establish an access control policy that specifies the followings;

- Account manager of information system who manage the accounts (including settings, modifications and deletion) will be designated;
- Privilege granted to each user will be controlled to the minimum extent necessary for performing their duties and;
- Policy for identification of the system components and authentication of the system users will be established.

2. User ID settings

Contractors must ensure that user ID is assigned to each relevant employee who uses information system and the relevant employee set their own passwords in order to identify the users on the usage log explained in the next paragraph.

In addition, contractors must set the limit of logon retries and have the account locked automatically for a certain period if exceeding the limit. They must also set the upper time limit of inactive status and lock the user sessions if exceeding the limit.

3. Usage log of information system

Contractors must maintain a usage log of the information system in order to supplement the investigation in the event of incidents such as unauthorized usage or inappropriate operation of the information system and monitoring of the access control. The usage log must include at least user ID, the date of login/logoff, terminal ID, files or programs that were accessed/used, and success or failure of the access to information system or data. The usage log must be inspected periodically and as necessary.

Section6. Verification/Improvement

Contractors must periodically verify documents, organizations, management status of classified information and education contents. They must also improve these items according to the circumstances.

In this verification, contractors must identify and assess the risk in the department in which classified information is handled, as well as other departments and external entities (such as outsourcing contractors for maintenance) to the extent that there will be an impact on the protection of classified information. This risk assessment includes the damages, threat and vulnerabilities with regard to unauthorized access, disclosure, usage, falsification, and destruction concerning the information system processing classified information.

When the contractors conduct the risk assessment, they must record the result of the assessment.

CHAPTER 12. Visits and Meetings

Section1. Visit Procedures

This section outlines the visit procedures for the personnel other than relevant cleared employees and RDB security officers.

These procedures are intended to;

- Prevent unauthorized access to classified information by ensuring that the personnel are eligible to handle classified information and have necessity to visit the facilities, and;
- Prevent compromise of classified information by ensuring security measures against the personnel who are not eligible to handle classified information.

Procedures applied to international visits are stipulated in Chapter 17.

Section2. Visits involving Handling of Classified Information

Visits involving the handling of classified information must be limited to the minimum necessary. When the personnel other than relevant cleared employees visit security facilities, contractors must obtain an approval from the competent RDB in advance. There are visit procedures established respectively for government officials and relevant cleared employees of other companies.

Those who visit security facilities must have Need-to-Know, which will be confirmed based on a written permission for the visit (in case of government officials) or a contract and a visit request (in case of contractor employees).

1. Visits by government officials

With regard to the visit by government officials, their supervisor issues a written permission for the visit to the contractor via the RDB. The permission includes;

(1) Name, position and department of the supervisor
(2) Date of the visit
(3) Name and ID number of the visitor
(4) Purpose of the visit (Need-to-Know)
(5) Visitor's PSC and the permission for the individual access
(6) Scope of classified information disclosed during the visit

2. Visits by relevant cleared employees of other companies

With regard to the visit by relevant cleared employees hired by other companies, contractors that will receive the visit must submit a visit request to the RDB. The request must include the items same as the above (1) to (6). The request must be issued by FSO of the contractor to obtain an approval from the RDB prior to the visit.

3. Recurring visit

The RDBs may issue a recurring-visit permission for a period not exceeding 1 year. Contractors and RDBs must periodically confirm whether the permission is valid. In addition, those who have been permitted for a recurring visit must report to the RDB immediately when they no longer need to visit the facility for reasons such as personnel changes.

Section3. Visits without Handling Classified Information

When it is necessary to have uncleared personnel to visit security facilities for such purposes as maintenance of equipment or inspection of firefighting equipment prescribed by laws and regulations, contractors must submit a visit request to the competent RDB and obtain an approval prior to the visit.

In this case, contractors must take protective measures for preventing compromise of classified information (such as storing in a security container, relocating to another security facility or covering classified materials), while ensuring security manager or designated relevant cleared employees attend the uncleared personnel.

The visit request must include;

(1) Name of the security facilities
(2) Date of the visit
(3) Name and ID number of the visitor
(4) Purpose of the visit
(5) Classification of classified information handled in the security facilities
(6) Details of the protective measures

Section4. Emergency Visits

When it is deemed to be unavoidable, the competent RDB may approve emergency visits by contractor employees on the condition that they will take appropriate security measures and will undergo the necessary procedures after the visit.

It must be noted that this procedure is approved only for unavoidable cases, and therefore, it must be applied to the limited cases such as a visit conducted based on any laws and regulations.

Section5. Meetings

This Section will cover the security measures generally taken within security facilities, which especially require special attentions during meetings involving classified information

to prevent compromise.
In this Section, it is assumed that the meetings involving classified information are taken place in order to perform the contract with ATLA.
Although contractors may be required to hold meetings involving classified information based on the contract, such meetings must be limited to the minimum necessary.

1. Attendees and venue of meetings

Those who attend meetings involving classified information must be contractor employees or government officials necessary for the meeting, as well as hold PSC. Those attendees must be limited to the minimum necessary in light of the purpose of the meeting.
Such meetings must be taken place within the approved security facilities of the contractor or government security facilities. The classified information handled in the meeting must be limited to the extent related to the purpose of the meeting.
Whether the attendees have a valid PSC and Need-to-Know is confirmed by the visit permission or the visit request in case of the meeting held at the contractor's security facilities. In case of the meeting taken place at the security facilities of ATLA, the sponsor from ATLA of the meeting confirms PSC and Need-to-Know.

2. Points to be considered regarding transmission

As described in Section 3 of Chapter 8, when classified information is transmitted orally, they must clearly state that the transmitted information is classified, while taking necessary measures such as ensuring the information is not written down or audibly recorded.

3. Distribution materials

When it is necessary to duplicate classified materials for distribution at the meeting, contractors must obtain an approval from ATLA in advance unless specified in the contract. In this case, they must also apply serial numbers to each copy of the materials.
The classified materials must be returned to the contractors after the meeting in principle. If they do not collect the materials from the attendees other than the contractor employees, they must take the procedures for transmission with an approval from ATLA.

CHAPTER 13. Subcontract

Section1. Subcontract

Subcontract involving any classified works is not allowed in principle. However, if there are exceptional circumstances, such subcontract may be approved under the following conditions:

- The subcontractor holds the FSC.
- There is a contract for protecting classified information between ATLA, the prime contractor and the subcontractor (hereinafter referred to as a “tripartite contract”).

The subcontractor must be an eligible contractor, and the obligations same as the prime contractor will be imposed on the subcontractor.

Section2. Responsibilities of Prime Contractor

When a prime contractor discloses classified information to its subcontractor or let them handle classified information, the prime contractor must undergo the following procedures in advance;

(Before concluding the subcontract)

1. The prime contractor must apply for subcontracting to ATLA. The application includes the following items;

- Name of the prospected subcontractor
- Details of the classified works performed by the prospected subcontractor
- Extent of classified information which the prospected subcontractor will handle
- Security measures taken by the prospected subcontractor

2. The prime contractor must request the prospected subcontractor to initiate the procedures for a tripartite contract.

3. The prime contractor must obtain an approval for the subcontract by ATLA.

(After concluding the subcontract)

4. The prime contractor must conduct security inspections periodically (separately from the inspections by the RDB).

5. When the prime contractor transfers classified information to their subcontractor, they must obtain an approval from ATLA. In this case, the classified materials will be

transferred to the subcontractor directly by ATLA in principle.

Section3. Tripartite Contract

The tripartite contract will take effect after the subcontract is approved, and stipulates the items below;

1. Obligation to take security measures same as the prime contractor
2. Penalty imposed on subcontractor in case of compromise of classified information depending on the contract amount with the prime contractor
3. Extent which the subcontractor is able to access
4. Cancellation of the subcontract

(1) When ATLA cancels the security contract by reasons attributable to the subcontractor, ATLA notifies the prime contractor of the cancellation.

(2) When the prime contractor cancels the subcontract by reasons attributable to the subcontractor, the prime contractor must notify ATLA of the cancellation.

(3) When ATLA cancels the prime contract by reasons attributable to the prime contractor, ATLA may also cancel the tripartite contract among ATLA, the prime contractor and the subcontractor.

Section4. Termination of Subcontract

When the prime contractor terminates their subcontract, the tripartite contract will be also terminated basically. Therefore, they must make their subcontractors return or submit their classified materials to ATLA in principle. In case where the classified materials have been provided from the prime contractor to the subcontractor directly, the subcontractor must return or submit them to the prime contractor.

Even after the tripartite contract is terminated, the subcontractor must not compromise any classified information obtained in the course of the contract.

Section5. Transportation of Classified Items to Subcontractor

As described in Section 2 of this Chapter, classified materials must be transferred directly from ATLA to the subcontractor in principle. However, the prime contractor may transport classified items to their subcontractor, and vice versa, with an approval from ATLA.

When transporting classified items, the prime contractor and the subcontractor must undergo the procedures described in Section 4 of Chapter 7.

CHAPTER 14. Security Inspection

Section1. Security-related Booklets

In order to ensure and verify the implementation of transfer, access, creation, storage, submission, disposition and other items pertaining to classified information, FSO must maintain necessary security-related booklets as below;

- Records of storage (including title/document number of classified documents and the date of transmission)
- Access/lending log (including the date of access/lending and individuals involving the access/lending)
- Record of visits to security facilities (including individuals who entered the facilities, individual PSC number, works performed in the facilities and time of entering/leaving the facilities)
- Records of inspection (including the record of in-house security inspections by the contractor)

FSO must retain the security-related booklets until three years have passed after expiration of classification or declassification.

Section2. In-house Security Inspection by Contractor

FSO must conduct in-house security inspection at least once a month. The in-house inspection covers every security measure taken by the contractor, including the review of the security-related booklets described in the previous section.

FSO must maintain the records of the in-house security inspection.

Section3. Security Inspection by RDBs

Contractors must receive the security inspection conducted by the competent RDB at least once a month after their in-house security inspection.

The contractor must also cooperate with the RDB to conduct the security inspection. The in-house security inspection must be done by the date of the RDB inspection, which will be coordinated with RDB officials, taking the overall schedule of inspections over their jurisdiction into consideration.

In addition to the regular inspection, ATLA may conduct an extra inspection if necessary.

The security inspection will cover the all security measures, including the following items;

- Handling status of classified information (creation, duplication, transfer, disposition, etc.)
- Inventory of classified information
- Security facilities (including access control procedures)

- Usage log of information systems
- List of relevant cleared employees
- Implementation status of security training
- Results of in-house security inspection
- Supervision over subcontractors (if applicable)

The result of inspection will be evaluated on 3 grades as follows;

- Good: All the security measures are implemented appropriately based on the requirements.
- Needs improvement: Security measures are generally sufficient, though there are some observations.
- Failed: Some of the security measures are inappropriate and need to be corrected.

Although the RDB reports the inspection results to ATLA every 3 months basically, the RDB must report it immediately when there are any items to be “Failed”. In such cases, the contractor must develop and implement a plan to take necessary corrective measures to resolve the items pointed out by the RDB. The RDB confirms the plan submitted by the contractor and the implementation of the plan, while providing instructions if necessary. The due date for taking the corrective measures is specified by the RDB, or determined by consultation between the contractor and the RDB.
In case the RDB does not consider that the corrective measures are sufficient to resolve the deficiency, any additional measures may be required.

Section4. Reporting Storage Status of Classified Materials

In addition to the in-house security inspection and the RDB security inspection described in this chapter, contractors must report their storage status of classified materials to ATLA at the end of June and December every year in principle. The storage status is usually reported at the same time with the report within JMOD.

Section5. Reporting Compliance with Standards pertaining to SDS

Eligible contractors must report the security measures taken in accordance with the Article 13 of the Cabinet Order pertaining to the SDS Protection (Cabinet Order No. 336, 2014) to ATLA (Director General, Department of Equipment Policy) by the end of April every year.

CHAPTER 15. Report and Response concerning Security Incidents

Section1. Response to Security Incidents

In case of actual or potential loss, compromise or destruction of classified information, and receiving/finding classified materials which contractors are not authorized to hold, contractors must take appropriate measures immediately.

The “potential loss, compromise or destruction” includes any inappropriate behavior or unauthorized handling of/access to classified information by their employees, and contact with foreign governments officials without permission by FSO.

When finding these situations, contractors must immediately confirm the circumstance and make efforts to prevent further incidents by taking necessary measures for protecting classified information, as well as report every information they have at that moment to ATLA (Equipment Security Management Division) and the competent RDB.

The necessary measures for protecting classified information include restriction of access to the building including security facilities, tentative relocation of the classified materials to a secured area as instructed by FSO, or submission of the classified materials that they have inappropriately received to ATLA (Equipment Security Management Division).

After the report, the contractor must conduct detailed investigation on the below items without delay, and submit the result with their comments and preventive measures to the Contracting Authority.

- Date and location of the incident and the name/position of those who were involved with the incident
- Title, control number, serial number, quantity and contents of the classified materials relevant to the incident
- Cause and timeline of the incident
- Impact by the incident
- Measures taken in response to the incident
- Other matters

The contractor must also report to the police authority if the incident is deemed to be any criminal acts.

Section2. Emergency Contacts

In order to maintain a smooth contact in case of the incident or emergency as described in the preceding section, contractors must establish an emergency contact network and inform their relevant cleared employees of it.

The point of contact for ATLA is represented by Equipment Security Management Division,

Department of Equipment Policy and the RDB as below:

- Equipment Security Management Division, Department of Equipment Policy, Acquisition, Technology and Logistics Agency (ATLA)
  Phone Number: +80-3-3268-3111 (Ext. 21043-21045)
  (The emergency phone number will be notified after contract conclusion.)

The contact information of the RDBs is included in the Appendix.

Section3. Emergency Measures

When it is deemed that there are no any other appropriate means to prevent compromise of classified information in the event of emergency in which the information might be compromised, contractors may destroy them by such means as incineration, pulverization, shredding, dissolution and destruction so that the information cannot be reconstructed.
In that case, the contractor must obtain an approval from ATLA (in case of SDS, Minister of Defense or ATLA Commissioner via Director General, Department of Procurement Operations) in advance. In case there is no time or means to obtain such an approval, however, the contractor must promptly report after the destruction.

Section4. Whistleblowing

When there are any facts or concerns that contractor employees or board members (including those who retired) in charge of performing the contract with ATLA are violating laws and regulations, it can be reported to the point of contact for Whistleblowing.
Contractors must not dismiss or treat their employees due to the Whistleblowing.
The Whistleblowing can be addressed to the below contact point by e-mail, mail or phone, while describing the name, organization, contact information of the Whistleblower and details of the act to be reported (including by whom, where and how the act has been committed), as well as the legal grounds for the Whistleblowing as detailed as possible. The whistleblowing must not include any classified information.

- Point of Contact for Whistleblowing
  e-mail: atla-koeki-tsuho@atla.mod.go.jp
  Address: 5-1 Ichigaya-Honmuracho, Shinjuku-Ku, Tokyo 162-8870
  Audit and Evaluation Division, Secretariat, Acquisition, Technology and Logistics Agency (ATLA)
  Phone Number: +81-3-3268-3111 (Ext. 35841 or 35843)

CHAPTER 16. Return and Disposition of Classified Material

Section1. Return/Submission of Classified Material

Contractors must return classified materials that are no longer necessary for performing the contract to ATLA.

They must also submit the classified materials created or duplicated based on the contract as specified in the contract.

Even in the middle of the contract period, they must return the classified materials if instructed to do so by ATLA.

In addition, they must return or submit the classified materials promptly in case of cancellation of the contract.

When returning or submitting classified information, contractors must keep a record and report it to ATLA.

Section2. Disposition of Classified Material

Contractors must return the classified materials provided by ATLA and submit the ones created or duplicated to ATLA in principle. When instructed by ATLA, however, they may dispose of the classified materials.

When disposing of classified materials, contractors must destroy them by means such as incineration, pulverization, shredding, dissolution and destruction to make it difficult to find as classified information in presence of one or more relevant cleared employees designated by FSO in accordance with the instruction by ATLA.

In such cases, the contractor must keep a record of the disposition and report it to ATLA.

CHAPTER 17. Security Measures concerning International Projects

This chapter covers how to manage classified information related to international projects. It is the foundation of defense equipment and technology cooperation that the Japanese companies are able to share classified information with foreign governments and companies “safely” and “reasonably”.

Section1. National Laws and Regulations, and Bilateral Security Framework

When sharing classified information with foreign governments or companies, the international frameworks as well as the national laws and regulations concerning the protection of classified information are applied.

The classified information provided by Japan will not be disclosed to other countries until the Agreement between the government of Japan and the foreign country or the Arrangement between defense authorities concerning the protection of classified information is signed in principle.

As the frameworks for information security applied to Japanese defense companies, there are the General Security of Information Agreement, which sets forth protecting measures of classified information exchanged between two countries in the interest of national security, the General Security of Military Information Agreement, which stipulates protecting measures of classified military information exchanged between two countries, and the Arrangement on Information Security between defense authorities.

Some of these information security frameworks are undisclosed in relation with the partner country.

Section2. Disclosure of Classified Information to Foreign Interests

It is necessary to obtain an approval from ATLA Commissioner in accordance with the national laws and ATLA regulations regarding the protection of classified information in order to disclose classified information to foreign government or companies.

With regard to providing classified items or technology to foreign countries, it is required to obtain an export permission based on the Foreign Exchange and Foreign Trade Act (Act No. 228 of 1949), in addition to complying with the laws and regulations for protecting classified information.

Section3. Foreign Government Classified Information

1. Receiving classified information of foreign governments

The Japanese national laws and regulations and the Agreement/Arrangement for information security require that classified information provided to Japanese companies

be transferred via the government of Japan from foreign governments. This is mainly because the obligations to protect classified information are imposed on the Japanese companies based on the contract for the protection of classified information between the government of Japan and the companies (See also Section 4).

If Japanese companies need to receive any classified information of the foreign government for defense equipment and technology cooperation (e.g. Japanese defense industry participating in the project of the foreign government or company), they are able to receive such information under a contract for the protection of classified information with ATLA so that they are legally obliged to protect such information. In this case, the Japanese company must hold the FSC.

Even if that the Japanese company is not expected to enter into such a contract as for production or maintenance of defense equipment supplied to ATLA, they are able to receive the classified information by awarding a contract for the protection of classified information without financial transactions so that they are legally obliged to protect such information.

The point of contact for this type of contract for the protection of classified information without financial transactions is ATLA (Equipment Security Management Division).

2. Handling classified information of foreign government

With regard to the classified information received from foreign governments, the security classification marking applied by the foreign government must be maintained. In addition to that, the corresponding security classification in Japan and the originating country must be marked in red in accordance with ATLA regulations in principle.

Some countries have the forth security classification of “Restricted”, which corresponds to nothing in the Japanese security classifications directly. Such information will be protected as classified information of “HI”, or Controlled Unclassified Information of “CHUI” and “BUNAI KAGIRI” in Japan, in accordance with the notification by the providing country based on the Agreement or Arrangement.

The classified information received from foreign governments must not be disclosed to third parties without a prior written approval of the providing country in accordance with the Agreement or Arrangement.

Section4. Security Aspects of International Project

In order to proceed with international cooperative projects, ATLA (Development Divisions and Research Centers) makes Project Security Instruction (PSI) with the department of the

partner country relevant to the project with an approval by ATLA (Equipment Security Management Division).

PSI is an implementing procedure to coordinate different security regulations between countries participating in a joint project, and to smoothly implement the project.

The government officials and contractors of each country will implement the project in accordance with the provision of PSI. The PSI is obliged to the contractors as an attachment to the contract with ATLA.

The standard items of PSI include the followings, but any additional requirements may be applied as necessary;

- Introduction and glossary for definition of terms (e.g. purpose, authority, responsibility and applicability)
- Security instructions (including access to classified information, international transmission, markings, procedures for the protection of CUI, security classification, compromise and security violations)
- Release of program information (*) (including unilateral release, release to third parties, release at conferences, public release and release in exhibition)
- International visits
- Subcontracting
- List of security cleared facilities
- Security plan upon termination of the joint program or the contract
- Security education and awareness

* Program information: Information which is provided, developed or used in joint programs

Section5. Transmission of Classified Information by Companies with Foreign Entity

Classified information is transmitted between foreign countries through the government-to-government channels, against some backgrounds, such as the Japanese relevant laws and regulations assume that classified information is provided by the government of Japan to foreign government or Japanese companies as the fundamental framework.

Alternatively, it is sometimes indispensable not only to transmit classified information between the governments directly, but also transmit and promptly share it between the Japanese and foreign industries by physical or electronic means, in relation with defense equipment and technology cooperation.

In such cases, if there is prior consent between ATLA and the other countries, and it is possible to ensure the implementation in line with the Japanese legislation to protect classified information, it becomes possible to transmit classified information by industries.

For instance, in case of SDS, transmission between industries can be regarded as the provision of classified information from the government of Japan to foreign government or Japanese companies by complying with the below conditions;

1. Necessary items for ensuring security of classified information have been confirmed with the foreign country implementing defense equipment and technology cooperation
2. Instruction or approval from ATLA to Japanese industries to provide/receive classified information beforehand
3. Sharing information by a company regarding the classified information they have provided/received (i.e. ensuring sufficient management and oversight by the Japanese government)

In addition, whether the specific transmission of classified information between industries is possible or not, as well as the detailed procedures for each transmission, must be considered based on the individual circumstances including the provisions of the Agreement or Arrangement on Information Security with each country. In case there is a necessity of such consideration, including the matters concerning classified information other than SDS, ATLA (Equipment Security Management Division) will be consulted.

Section6. Restriction on International Visit and Access

This section outlines the procedures applied to international visits to security facilities of Japanese contractors involving access to classified information.

(1) Visit Request Procedures

This manual describes specific visit procedures as the standard (Attachment 2: Request for Visit, RFV).

However, it is not prohibited to prescribe the alternative visit procedures in accordance with the mutual determination in writing such as the individual Project Security Instruction (PSI) between the two countries.

(2) Application Procedures for Visits

The procedures applied to foreign visitors are as below;

a. The foreign government submits RFV to ATLA (Equipment Security Management Division) through government-to-government channels (basically via the Embassy in Japan).
b. ATLA confirms PSC and Need-to-Know of the foreign visitor related to the visit to the

security facilities and notifies the RDB of the result and the RFV

c. The RDB determines whether visit is acceptable or not and notifies the company of the result.

(3) Types of RFV

There are three types of RFV applied to international visits;

a. One-time visit: A visit for a single, short-term occasion (normally 30 days or fewer) for a specified purpose. The visit period will not be in excess of PSC validity.

b. Recurring visit: Intermittent, recurring visits to a certain location over a specified period of time, up to one year in duration, for a specified purpose. The visit period will not be in excess of PSC validity.

c. Emergency visit: A visit for a single occasion, which cannot satisfy the deadline described in paragraph (4), and failure to make the visit could be reasonably expected to lead to a serious impact. When requesting the emergency visit, it is required to coordinate with the company for the visit and demonstrate the justification of the visit to ATLA.

(4) Deadline for submitting RFV

RFV must be submitted no later than 20 working days before the first day of one-time visit or the recurring visits.

(4) Changes on RFV

a. If it is necessary to change the approved or submitted RFV, the corrected RFV must be submitted.

b. However, the type of the visit and the request for an emergency visit cannot be changed by this process.

c. It takes at least 5 working days to process the change after ATLA (Equipment Security Management Division) receives the amended RFV.

Appendix 1: Point of contact for the Defense Industrial Security Manual

- Point of contact for the DISM

Equipment Security Management Division, Department of Equipment Policy, Acquisition, Technology and Logistics Agency (ATLA)

Address: 5-1 Ichigaya-Honmuracho, Shinjuku-Ku, Tokyo 162-8870

Phone number: +81-3-3268-3111 (Ext. 21043, 21044 or 21045)

E-mail address: hozen-manual@ext.atla.mod.go.jp

- Point of contact in case of security incidents

Department of Equipment Policy, Acquisition, Technology and Logistics Agency (ATLA)

Address: 5-1 Ichigaya-Honmuracho, Shinjuku-Ku, Tokyo 162-8870

Phone number: +81-3-3268-3111 (Ext. 21043, 21044 or 21045)

(The emergency phone number will be notified after contract conclusion.)

- Point of Contact for RDBs

Hokkaido Defense Bureau	Procurement Planning Division, Department of Procurement	+81-11-272-7512
Tohoku Defense Bureau	Koriyama Defense Office	+81-24-961-7681
North Kanto Defense Bureau	Equipment Planning Division, Department of Equipment	+81-3-3908-5121
	Utsunomiya Defense Office	+81-28-638-1384
South Kanto Defense Bureau	Equipment Division, Department of Procurement	+81-45-641-4741
Kinki-Chubu Defense Bureau	Equipment Division, Department of Procurement	+81-6-6949-6472
	Maizuru Defense Office	+81-773-62-0305
Tokai Defense Branch	Equipment Division	+81-52-952-8281
	Gifu Defense Office	+81-58-383-5935
Chugoku-Shikoku Defense Bureau	Equipment Division, Department of Procurement	+81-82-223-8014
	Tamano Defense Office	+81-863-21-3724

Nagasaki Defense Branch	Internal Affairs Division	+81-95-825-5303
Okinawa Defense Bureau	Procurement Planning Division, Department of Procurement	+81-98-921-8131

Appendix2: Standard RFV format

All fields must be completed and the form communicated via Government-to-Government

REQUEST FOR VISIT

TO: _____

(Country/international organisation name)

1. TYPE OF VISIT REQUEST	**2. TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS**	**3. SUMMARY**
☐ One-time ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Agency/Facility For an amendment, insert the NSA/DSA original RFV Reference No._____	☐ CONFIDENTIAL or above ☐ Access to security facilities without access to classified information/ material	No. of sites: _____ No. of visitors: _____

4. ADMINISTRATIVE DATA:

Requestor: To: ATLA, Japan Ministry of Defense	NSA/DSA RFV Reference No._____ Date *(dd/mm/yyyy)*: _____/_____/_____

5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:

POSTAL ADDRESS:
E-MAIL ADDRESS:
FAX NO:
TELEPHONE NO:

6. GOVERNMENT AGENCY(IES) , ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED - *(Annex 1 to be completed)*

7. DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. TYPE OF INITIATIVE *(Select one from each column)*:

☐ Government initiative	☐ Initiated by requesting agency or facility
☐ Commercial initiative	☐ By invitation of the facility to be visited

9. IS THE VISIT PERTINENT TO:

☐ Specific equipment or weapon system
☐ Foreign military sales or export licence
☐ A programme or agreement
☐ A defence acquisition process
☐ Other

Specification of the selected subject:

10. SUBJECT TO BE DISCUSSED/JUSTIFICATION/PURPOSE *(To include details of host Government/Project Authority and solicitation/contract number if known and any other relevant information. Abbreviations should be avoided)*:

11. ANTICIPATED HIGHEST LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:

☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐ Other

If other, specify: _____

12. PARTICULARS OF VISITOR(S) - *(Annex 2 to be completed)*

13. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE
(dd/mm/yyyy): _____/_____/_____

15. REQUESTING NATIONAL SECURITY AUTHORITY / DESIGNATED SECURITY AUTHORITY:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE
(dd/mm/yyyy): _____/_____/_____

16. REMARKS *(Mandatory justification required in case of an emergency visit)*:

ANNEX 1 to RFV FORM

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1. ☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:
ADDRESS:
TELEPHONE NO:
FAX NO:

NAME OF POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

NAME OF SECURITY OFFICER OR
SECONDARY POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

2. ☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:
ADDRESS:
TELEPHONE NO:
FAX NO:

NAME OF POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

NAME OF SECURITY OFFICER OR
SECONDARY POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

3. ☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:
ADDRESS:
TELEPHONE NO:
FAX NO:

NAME OF POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

NAME OF SECURITY OFFICER OR
SECONDARY POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

4. ☐ Military ☐ Government ☐ Industry ☐ Other

If other, specify: _____

NAME:
ADDRESS:
TELEPHONE NO:
FAX NO:

NAME OF POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

NAME OF SECURITY OFFICER OR
SECONDARY POINT OF CONTACT:
E-MAIL:
TELEPHONE NO:

(Continue as required)

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)

1. ☐ Military ☐ Defence Public Servant ☐ Government

☐ Industry/Embedded Contractor ☐ Other (Specify: _____)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

2. ☐ Military ☐ Defence Public Servant ☐ Government

☐ Industry/Embedded Contractor ☐ Other (Specify: _____)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

3. ☐ Military ☐ Defence Public Servant ☐ Government

☐ Industry/Embedded Contractor ☐ Other (Specify: _____)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

4. ☐ Military ☐ Defence Public Servant ☐ Government

☐ Industry/Embedded Contractor ☐ Other (Specify: _____)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

(Continue as required)