Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRIME MINISTER

General Secretariat
for Defence and National Security

Protection
and Security of the State

Paris, November 30, 2011
N**o. 1300**/SGDSN/PSE/PSD

GENERAL INTERMINISTERIAL DIRECTIVE ON THE PROTECTION OF THE NATIONAL DEFENCE SECRET

Courtesy translation

"Only the version which is published in the Official Gazette of the French Republic is the authentic version"

51 boulevard de la Tour Maubourg 75700 PARIS 07 SP - Tel: 01. 71. 75. 81. 89 - Fax: 01 71. 75. 82. 00

The present directive is attached to the decree reproduced hereunder.

Decree of November 30, 2011 bearing approval of the general interministerial directive on the protection of national defence secret

PRM D 1 1 3 2 4 8 0 A

The Prime Minister,

Having regarding to the Criminal Code, especially its Articles 413-9 to 414-9;

Having regard to the Defence Code, especially Articles R.*1132-2, R.*1132-3, D. 1132-5 and R. 2311-1 to R. 2312-2;

Having regard to the Labour Code;

Having regard to the Procurement Contracts Code;

Having regard to the Law no. 75-1334 of December 31, 1975 as amended relating to sub-contracts;

Having regard to the Decree no. 2004-16 of January 7, 2004 as amended, taken in application of article 4 of the Procurement of Contracts Code and concerning certain procurement contracts for defence requirements, especially its article 17;

Having regard to the Decree no. 2005-1124 of September 6, 2005 as amended, used for the application of Article 17-1 of the Law no. 95-73 of January 21, 1995 and fixing the list of administrative inquiries leading to personal data automated processes consultation as mentioned in Article 21 of law no. 2003-239 of March 18, 2003;

Having regard to the decision no 2011-192 QPC of November 10, 2011 of the Constitutional Council,

Decree

Article 1: The General Interministerial Directive no 1300 on the protection of national defence secret, hereafter attached, is approved.

Article 2: The Decree of July 23, 2010 relating to the protection of national defence secretis hereby rescinded.

Article 3: The present Decree will be published in the Official Gazette of the French Republic.

Paris, November 30, 2011

For the Prime Minister and by delegation,
The General Secretary for Defence and National Security,
F. Delon

CONTENTS

INTRODUCTION

This new general interministerial directive 1300 has been made necessary due to the amendments brought in by the Law no. 2009-928 of July 29, 2009 related to military programming for years 2009-2014 and containing various clauses related to defence as well as Decree no. 2010-678 of June 21, 2010 concerning the protection of national defence secret. As a follow-up to the recommendations of the White Paper on Defence and National Security of June 2008, and in accordance with the decision of the Constitutional Council of 10 November 2011[1], this Directive's objective is to reinforce the judicial security of the protection of national defence secret while keeping in mind the disintegration of the traditional divide between defence and security.

In case of disclosure, some information represent such a risk of breach to defence and national security that only certain persons are authorised to access them. Knowing that the information contains such a hazard leads the public authorities to classify it, that is, to confer upon it the character of national defence secret and to make it benefit of a strict judicial and material protection.

The present directive describes the general organisation of the protection of national defence secret. Through attempts to clarify the judicial and material obligations inherent to this protection, the directive specifies the conditions in which each minister, for his own department, implements these measures, while seeing to it that the number and level of security clearances are limited and the production of classified documents restricted to what is strictly necessary in order to guarantee the optimum efficiency of the system.

It defines the security clearance and control procedures of individuals who can access the secret, the conditions of creating, processing, exchange, conservation or transport of classified documents and see to their protection. The security of classified information must be a major and constant concern of their holder. Any person, who, in contravention of the applicable provisions, would compromise the secret, subjects himself/herself to administrative and criminal sanctions.

The Directive determines the criteria, levels and conditions of the classification of the information and materials concerned, as well as access rules to sites holding such information. It describes the procedure, reconciling the two constitutional objectives that represent the safeguard of the interests of the Nation and the search of the perpetrators of criminal acts, which allows a magistrate of inquiring his investigations without compromise, when confronted to the rules governing the protection of the secret.

It also takes into account the increase noted in the exchange of classified information, at national level, at european level or at international level. Since all the States protect their classified information, France, under the security agreements it has signed, is under a duty to

[1] Decision of the Constitutional Council N°2011-192 QPC of 10 November 2011.

guarantee, on a reciprocal basis, the protection of classified information sent to it by States Parties.Finally, the protection of the secret is not limited to classified documents on paper and specifically extends to information technology and electronic means which allow the development, processing, storage and transmission of such information. The information and communication systems, which innervate today critical infrastructure, economic and social life as well as the action of public powers, have its own vulnerabilities. The constant threat of a multiform[2] cyber attack and the possibility, at any time, of a compromise without the user's knowledge even, counter demands information systems security rules adapted to rapidly changing techniques and a high degree of expertise to be spread among all public or private players.

[2] Malevolent blocking, hardware destruction, neutralisation of a system, theft or alteration of data, hijack of a device for hostile ends …

TITLE I:-
PRINCIPLES AND ORGANISATION OF THE PROTECTION

→The protection of the secret concerns all domains of activities relating to defence and national security: political, military, diplomatic, scientific, economic, industrial...
→ Those information are classified whose disclosure is likely to cause prejudice to defence and national security;
→France can also protect the information exchanged with international organisations and foreign States;
→The protection of the secret is ensured by a chain of responsibility applicable to both public and private domains;
→The General Secretariat for Defence and National Security (SGDSN) is the national security authority ; it can delegate security authorities in specific domains.

Chapter 1:
General Principles of the protection of the secret

Article 1: Foundations of the protection

The national defence secret constitutes a major target for foreign services and the groups or isolated individuals who have an objective of destabilising the State or society. This threat aims all fields of activities relating to defence and national security: political, military, diplomatic, scientific, economic, industrial ... Certain information which interest defence and national security require a specific protection, allowing their distribution to be controlled and limited under the conditions defined in the present directive.

The prejudice which can be caused to defence and national security by the disclosure of certain information or certain materials justifies their classification. The affixing of the classification mark as defined in Articles R. 2311-2, R. 2311-3 and R. 2311-4 of the Defence Code, materially confers the secret nature to the concerned information or materials and justifies, in case of violation of the applicable provisions, the application of specific criminal rules.

Three levels of classification exist: *Très Secret Défense*, *Secret Défense, Confidentiel Défense*[3]. The objects of these classifications can be: procedures, objects, documents, information, information technology networks, computerised data or files whose disclosure is of such a nature that it can harm national defence or can lead to the discovery of a national defence secret.

[3] Article R. 2311-2 of the Defence Code.

Failure to respect the protection measures induced by the classification will generate the implementation of provisions for criminal law sanctions[4]. The secret protection policy aims to make any person having access to the classified information or materials, criminally and administratively liable.

Classified information is compromised when it is brought to public knowledge or to the knowledge of person who does not hold a personnel security clearance nor has the need to know it. With regards to the fundamental interests of the Nation, the assessment of the risks ofcompromising classified information or materials and of the vulnerabilities of individuals or systems processing them is essential to guarantee the protection of the secret. The strict application of security measures defined in the present directive, completed by the distribution of instructions and the awareness of personnel, will contribute to the efficiency of the system and enable the fight against malevolent actions, which are often made easier through ignorance, carelessness, inattention or negligence.

The protection of the secret, whether related to information or a material, must be ensured by physical beings or legal entities[5], from public law or private law. In case of breach, even involuntarily, these persons shall be held guilty of compromise and incur the penalties provided in Articles 413-10 and seq of the Criminal Code.

Article 2. : Definitions

The present directive will use the following terms:

- "**personnel security clearance**" (PSC), to denote the explicit decision, issued after a specific procedure defined in this directive, allowing a person, according to his need to know basis, to have access to classified information or materials at the level specified in the decision, as well at lower level(s);
- "**classified information or materials**"[6], to denote the procedures, objects, documents, information, information technology networks, computerised data or files possessing an attribute of national defence secret;
- "**Information systems**", to denote all the information technology methods whose purpose is to develop, process, store, transport, present or destroy the information;
- "**contract**", to denote any contract, agreement, deal whatever be its legal regime or denomination, in which a candidate or a contract holder, public or private, has to take cognizance, in the course of the drafting of the contract or its execution, and possibly to keep in its locations, the classified information or materials.

Article 3: Scope of application

The clauses of the present directive are applicable in all the central administrations, all the decentralised services of the State and the national public establishments placed under the authority of a minister, in any entity, public or private, concerned by national defence secret,

[4] Article 413-10 and following of the Criminal Code.
[5] Same as physical entities, the legal entities are criminally liable of compromising acts which can be attributed to them, by application of articles 121-2 and 414-7 of the Criminal Code.
[6] Article R2311-1 of the Defence Code.

as well as to any person holding, even provisionally, such a secret, included in the framework of the writing and the execution of a contract.

The classified information or materials given to France in application of a security agreement benefit from the protection measures of the secret in accordance with the equivalences defined by the said agreement, as soon as they bear the classification mark equivalent to one of the three defined levels [7].

Article 4: The classification

The decision to classify information or materials according to national defence secret has the result of placing it under the protection of specific provisions of the Criminal Code[8]. The affixing of the classification marking constitutes the only method of giving this specific protection.

The articles R. 2311-2 and R. 2311-3 of the Defence Code define three classification levels:

- *Très Secret Défense*, reserved to information and materials which concern government priorities in matter of defence and national security and whose disclosure is of such a nature that it could cause very serious harm to national defence;
- *Secret Défense*, reserved to information and materials whose disclosure is of such a nature that it could cause serious harm to national defence;
- *Confidentiel Défense*, reserved to information and materials whose disclosure is such that it could cause harm to the national defence or could lead to the discovery of a classified secret of the level *Très Secret Défense* or *Secret Défense*.

Information not having been subject to a classification decision at any of the three defined levels is not protected criminally in accordance with the national defence secret. Therefore, the act of omitting to proceed to the classification of information whose disclosure is of such a nature that it could harm defence or national security constitutes a fault, which has to be appreciated and, failing which, sanctioned, at the discretion of the hierarchical authority.

Article 5.: Specific marks of confidentiality

Certain information which do not need to be classified can however receive, from their originator, a confidentiality mark meant for restricting their distribution to a specific domain (specified by a specific mark[9]) or to guarantee their protection (such as *Diffusion Restreinte*).

These marks, which do not convey a classification, are not sufficient to confer to the given information the criminal protection afforded to national defence secret. Their only objective is to sensitise the user to the required discretion which he must exercise in the manipulation of information covered by this mark.

[7] Article 414-8 and 414-9 of the Criminal Code.

[8] Article 413-9 and following of the Criminal Code.

[9] For example, Confidential Personnel, Confidential Medical, Confidential Technology, Confidential Industry, Confidential Business, Confidential Support, unclassified information subject to a check, or another Special France (see art. 67 of this directive).

The person responsible for disclosure, whether he is from public or private domain, exposes himself to disciplinary or professional[10] sanctions, without prejudice to the possible application of specific clauses relating to the processing and the protection of personal data[11].

The mark *Diffusion restreinte* can be affixed on the information and materials that the originator intends to submit for restricted distribution. Contrary to certain foreign regulations, it does not correspond to a classification level but has the objective of calling the user's attention to the necessity of respecting the discretion in the processing of this information. It indicates that the information must not be rendered public and must only be communicated to persons needing to know it in the exercise of their duties. The rules mentioned in **annex 3** are applicable to this information and materials.

A mark of restricted distribution below the level equivalent to the French classification *Confidential Défense*, attributed to a document by a foreign State or an international organisation which brings it up in the classification level, submits the document in France to the protection rules mentioned in **annex 3**.

Article 6: Access to national defence secret

Only qualified people can access national defence secrets. The qualification requires the meeting of the two cumulative conditions:

- The need to know or access classified information, attested by the employment authority: the assessment of the need to know is based on the principle as per which a person can only have knowledge of classified information within the scope of his duties or if the fulfilment of his mission requires it[12]. It is carried out according to the conditions prescribed by Article 20 of the present directive.
- The issue of the personnel security clearance corresponding to the classification level of the information in question: the decision to grant a PSC is an explicit authorisation, issued after a specific procedure defined in this directive, allowing a person, on his need to know basis, to have access to classified information or materials at the level specified in the decision as well as at lower level(s). The decision to grant a PSC is accompanied by an undertaking to comply with, after having duly taken cognizance of same, the duties and responsibilities linked to the protection of classified information or materials.

Article 7: The sites holding classified information

The sites holding the elements covered by national defence secret are the premises in which classified information or material are kept, irrespective of their level, by individuals duly security cleared at the required level.

[10] Article L4121-2 of the Defence Code for the Military and article 26 of the law No. 83-634 of July 13, 1983 concerning rights and duties of government civil servants.
[11] Law no. 78-17 of January 6, 1978 modified relative to the IT, files and freedoms.
[12] Article R 2311-7 of Defence Code.

The access to these sites, for reasons of service, is governed by the provisions related to employment law, service delivery contracts, criminal law, criminal procedure[13], or issued from international conventions.

Article 8: Controls and inspections

The controls and inspections are organised periodically to verify the application, by the organisations emitting, receiving, processing or storing classified information, of instructions and directives related to the protection of the secret.

For the organisations processing the information or materials classified as *Très Secret Défense*, the inspections and controls are ensured by the General Secretariat for Defence and National Security (SGDSN). The latter proposes all measures for improving the general security conditions. The inspections and controls are organised in link with the ministerial departments. In case of anomalies noted, the SGDSN can question, through the concerned ministries, the services which lead to repression of crimes and misdemeanours. The summary reports including the recommended measures for correcting the deficiencies found and their planning are addressed to the authorities responsible for the checked organisations and to the relevant ministerial authorities.

At the request of the minister, for his department, or at the initiative of the investigating services, within the framework of their duties, the periodical controls and inspections are managed in the organisms processing information or materials classified as *Secret Défense* and *Confidentiel Défense*. The SGDSN can inspect such organisations.

[13] Title IV of the present directive.

Chapter 2:
Organisation of the protection

The protection of the secret falls on different authorities which, by relying on a specific organisation, ensures the proper application of measures defined in this directive.

Section 1:-Competent authorities

Article 9: The Prime Minister

As per Article 21 of the Constitution, the Prime Minister is responsible for national defence.

Articles R. 2311-5, R. 2311-6, and R. 2311-7 of the Defence Code specify the powers of the Prime Minister, who:

- for the *Très Secret Défense* level:

- determines the organisational criteria and modalities of the protection and defines the special classifications corresponding to different governmental priorities;
- fixes the conditions in which each minister determines the information and materials which should be classified at this level[14] for his own department;

- for the levels *Secret Défense* and *Confidentiel Défense*:

- fixes the conditions in which each minister determines the information and materials which should be classified and the modalities of their protection[15] for the department he is responsible for;

- for granting of the personnel security clearances (PSC):

- defines the procedure prior to the granting of a PSC;
- grants PSC at *Très Secret Défense* level and indicates the special classifications to which the cleared person can access[16].

To exercise these powers, the Prime Minister is assisted by the General Secretary of Defence and National Security.

Article 10: The General Secretary for Defence and National Security (SGDSN)

Under the authority of the Prime Minister, the General Secretary for Defence and National Security defines and coordinates, at interministerial level, the security policy for the protection of national defence secret[17]. As such he proposes, distributes, makes apply and controls the measures required for the protection of this secret[18].

The SGDSN powers are applicable in a national and an international framework.

---

[14] Article R 2311-5 of the Defence Code.
[15] Article R 2311-6 of the Defence Code.
[16] Articles R. 2311-7 and R. 2311-8 of the Defence Code.
[17] Article R 2311-10 of the Defence Code.
[18] Article D2311-12 of the Defence Code.

- At the national level:

For all classification levels, the SGDSN is responsible for the distribution and checking of the implementation of protection measures for the secret. As such, he makes sure that, on the basis of a report which must be provided to him annually, these protection measures are respected within each ministerial department.

For the *Très Secret Défense* level, he takes security clearance decisions through delegation from the Prime Minister.

He ensures the implementation of measures relating to special classifications and ensures checking, especially through inspections. He defines and organises the corresponding security networks. He designates, for each special classification, a central security agent whose duties are defined by specific instructions.

In the matter of information systems security, the SGDSN functions are defined in Title V of the present directive.

- At the international level:

The SGDSN, National Security Authority (NSA) for national defence secret, for the application of agreements and international treaties providing such an authority, is the interlocutor of the foreign security authorities. It negotiates the general security agreements with foreign States, international organisations, institutions and organs of the European Union and is consulted as soon as an agreement seems to interest, in full or in part, reciprocal protection and exchange of classified information.

It is informed, by the ministers, of the negotiation, in their specific domain, of the agreements bearing, in full or in part, on the reciprocal protection and exchange of classified information. It participates, with its foreign partners, in the development of regulations within the security committees of international organisations and the institutions and organs of the European Union. It determines the PSC procedures required and organises, manages and controls the corresponding security networks.

The SGDSN implements the international agreements concerning granting of PSC for the French citizens residing or having resided abroad as well as for foreign nationals in France.

The SGDSN ensures, in application of international agreements, the security of classified information entrusted to France. Moreover, it defines the protection measures of information and materials held by France, which have been classified by a foreign State or an international organisation and which do not bear any classification level equivalent to those defined in article R.2311-2 of the Defence Code[19].

Article 11: The Ministers

[19] Article R 2311-11 al. 2 of the Defence Code.

Each minister ensures, in the department under his responsibility, the implementation of the clauses related to the security of classified information or materials detained by any service or any public or private entity falling under his scheme of duties. He goes ahead with the periodical inspections in order to verify compliance.

He takes the security clearance decisions for the *Secret Défense* and *Confidentiel Défense* levels.

He determines, within the conditions fixed by the Prime Minister, the information or materials which should be classified at one of three levels, and the modalities of organisation of their protection for the levels *Secret Défense* and *Confidentiel Défense*.

For matters within his scheme of duties, each minister defines, by a specific instruction[20], the usage conditions of the classification levels *Secret Défense* and *Confidentiel Défense* and the information which should be classified at the level *Très Secret Défense.*

In the matter of information systems security, his duties are defined in title V of this directive.

Article 12: The senior defence and security civil servants

Each minister is assisted by a senior defence and security civil servant (HFDS)[21] whose functions are fixed by the Defence Code[22]. The HFDS reports directly to the minister and has his own specialised service. For carrying out his mission, he has the authority on all the boards and services of the ministerial department[23].

Within his ministerial department and the organisations attached to this department, the HFDS is responsible for the distribution and the application of clauses relative to defence security and the protection of the secret. He ensures the smooth functioning of services which manage the classified information and materials, verifies the accuracy of the inventories, proceeds to the required controls and inspections and proposes all dispositions aimed at reinforcing the efficiency of protection measures in place.

He takes, by delegation of the minister, subject to other delegations possibly granted according to the provisions of Article R. 2311-8-1 of the Defence Code, the security clearance decisions for the levels *Secret Défense* and *Confidentiel Défense*. He ensures the necessary links with the SGDSN for granting the personnel security clearances at *Très Secret Défense* level, and, as for foreign nationals or French citizens having lived abroad, for the personnel security clearances to national and international classifications of levels *Secret Défense* and *Confidentiel Défense*.

[20] Recommendations for the drafting of this instruction in annex 2.
[21] Pursuant Article R 1143-1 of the Defence Code and in compliance with the specific organization of some ministries, the Ministry of Defence and the Ministry of External Affairs are assisted by their respective ministerial departments, a corresponding senior defence and security civil servant (HFCDS), the Ministry of the Interior by a Senior defence civil servant (HFD) and the other ministries by a senior defence and security civil servant (HFDS). In the rest of this Directive, the term HFDS will be used in a generic way.
[22] Articles R 1143-1 and after of the Defence code.
[23] Article R 1143-2 of the Defence code.

He is in constant touch with his counterparts from other ministries and with the General Secretary of Defence and National Security, to whom he sends, before March 31st, within the framework of his annual activities report[24], an assessment of the protection of the secret within his department and the attached organisations. This report indicates especially, for each level, the number of people which are granted security clearance every year, the number of valid security clearances, the number of sites holding elements covered by national defence secret, the volume of classified documents, the status of jobs catalogues and inventories, the number of inspections and controls carried out, the deficiencies found in the provisions of the protection of the secret, the corrective actions made, the compromise cases found and the training or awareness campaigns led. This report is classified at the level *Confidentiel Défense* and marked "Spécial *France"*[25].

For the ministerial departments using the information systems requiring protection, an information systems security civil servant (FSSI) is selected by the HFDS and placed under his authority in order to drive the security policy of these systems and thus controls its implementation[26].

In accordance with the structures belonging to each minister and if required, at least one civil servant for security and defence (FSD) can be designated to the attached organisations, public establishments under its charge, public companies or within the HFDS service. The FSD assists the HFDS and, under him, checks the execution of protection measures of classified information.

Section 2:-Functional organisation

Article 13: The delegation of signature and competence

At the levels *Confidentiel Défense* and *Secret Défense*, the granting of security clearance decisions are taken by each minister for the department under his wing. The ministers have, for the security clearance decisions, the capacity of giving signature delegations to HFDS as well as to prefects for the agents placed under their charge and the individuals employed in the organisations as per their functions. For facility security clearances (FSC), the signature can be, moreover, delegated by the ministers, in compliance with the agreements or international treaties recommending explicitly such a delegation, to a delegated security authority.

The ministry of defence may delegate the competence of delivering the security clearance decisions to certain authorities under his ministerial department's responsability.

Article 14: The role of hierarchical authorities

[24] Article R 1143-8 of the Defence code.
[25] The mark " *Spécial France*" is processed in article 65 of this instruction.
[26] Article R 1143-5 (8) of the Defence code.

Within the different ministerial departments, the decentralised services and armies, the hierarchical civil or military authorities having received delegation of the minister whom they report to, undertake each in his level and in the scheme of his duties, the responsibility of security measures relative to the protection of the secret.

Within the public or private companies authorised to handle or detain classified information or materials, the hierarchical authority takes on the responsibility of security measures relative to the protection of the secret.

When the classified information or materials at the level *Très Secret Défense* have to beused within an organisation, the hierarchical authority must request, within the conditions fixed by a specific instruction of the Prime Minister, the creation of a Top Secret registry.

For the management, the recording and conservation of classified information or materials at *Secret Défense level*, the secret protection offices are created in the areas corresponding to the security norms, in accordance with this directive.

The hierarchical authorities shall ensure that the personnel placed under their responsibility are appropriately security cleared and initiate the clearance procedure at the level required by the jobs catalogue.

Article 15: The security officer

The security officer, appointed by the Head of the employer service, is the correspondent of the HFDS and investigating services. He has as mission, under the directives of his employment authority and in accordance with the modalities corresponding to each structure, to fix the security rules and procedures which have to be set up concerning the individuals and the classified information or materials, and of controlling compliance. He participates in the training and awareness of the personnel concerning the protection of the secret. He is responsible for the management of personnel security clearances and, in relation to the investigating services, for access control to protected areas. He may manage the secret protection office.

The public or private companies keeping national defence secrets or holders of contract implying the handling or storage of classified information or materials must designate a security officer.

Article 16: The Designated Security Authorities

Pursuant to Article R. 2311-10-1 of the Defence Code, one or several authorities can be designated by the NSA, on proposal from one or more interested ministers, as Designated Security Authorities (DSA) in specific domains, e.g. the industrial domain. These Designated Security Authorities are responsible to the NSA for the implementation of the security policy of national defence secret in the concerned domain and provides the direction and required assistance for its proper compliance, especially in the case of security agreements.

Pursuant to agreements or the international treaties, the DSA can be specifically charged with the management of security clearances for the personnel under its jurisdiction, liaising with other national or foreign DSA. It can also, if the agreement or treaty thus provides, take by itself the security clearance decision. It is responsible for the authorisation procedure for access to protected areas under its responsibility.

Article 17: Security networks *Très Secret Défense*

The protection of classified information or materials at the level *Très Secret Défense* is organised in the framework of the specific regulation of special classifications[27], which completes the general provisions of the present directive.

No service or organisation can develop, process, store or carry classified information or materials at the level *Très Secret Défense* without getting prior authorisationfrom SGDSN. The distribution of these information by electronic means is prohibited.

The service or the organisation shall moreover obligatorily have at its disposal a registry of the corresponding special classification. These registries are created by the decision of SGDSN on proposal from the concerned minister. Through application of the principle of compartmentalization of the information, separate registries are provided for each special classification.

The distribution of these classified information and materials mandatorily follow a security network constituted for guaranteeing the protection of each special classification. A central security agent, designated by SGDSN, exercises the centralised control of this distribution among the different registries.

The person in charge of each of these registries is selected among the personnel admitted to the special classification and is assisted by a security agent, who ensures compliance with the rules concerning protection of the secret.

Article 18: The secret protection Office

Each minister ensures the creation of one or several secret protection offices within which are carried out the development, processing, marking, storage and follow-up of the destruction of classified information or materials at the level *Secret Défense*. Each office makes an annual inventory of classified information or materials that it processes.

This office is also responsible for the registering, sending, receiving and distribution of classified materials at the level *Secret Défense*, which can only pass through its own intermediary, to the exclusion of those having the mark "ACSSI"[28], whose management is defined in title V of the present directive.

---

[27] Practical application directive no. 02/SGDN/SSD/CD of February 3, 1986 on the organisation and functioning of special classifications *Très Secret Défense.*

[28] Controled devicesof IT systems security, as defined by the interministerial instruction no. 910/SGDN/DISSI/SCSSI/SSD/DR of December 19, 1994.

This office, exclusively constituted of individuals holding a PSC at the level *Secret Défense*, is located in a restricted area, corresponding to the security norms defined in the present directive[29].

Such an office, mandatory for the level *Secret Défense*, is recommended for the information or materials of level *Confidentiel Défense*.

For fulfilling its duties, the secret protection office can set up a system ensuring the following functions by electronic means:

- identification of information materials (registration number of coming and going, originator or originating service, creation date, domain, title or object, page numbering, classification level, recommended mode and date of declassification, number of copies managed by the secret protection office);
- traceability of events concerning the materials copies (arrival, departure, reproduction, archiving, destruction, declassification, event reference number, event date, individual reference of copies, name and function of the physical holder of each sample);
- possible modification of previous data;
- search on the information materials (successive holders of a sample, creation date, originating service ...);
- inventory of information materials;
- provision of statements relative to actions carried out on the information materials (history, record file, follow-up file, sent receipt, minutes of destruction, declassification notice, archiving, reproduction ...).

[29] Article 74.

TITLE II:-
SECURITY MEASURES RELATING TO INDIVIDUALS

→Only those individuals who have been duly security cleared and having a need to know can have access to classified information;

→The personnel security clearance is a heavy procedure which should only be carried out when it is strictly necessary and complying to the jobs catalogue;

→The security screening enables to verify if we can trust a person sufficiently to grant him access to a site holding national defence secrets or entrust him with a specific mission;

→The decisions relating to personnel security clearances are notified to all concerned parties.

Chapter 1:
Access to national defence secret

Article19: Principle

Pursuant to Article R 2311-7 of the Defence Code, no one is authorised for knowing the classified information or materials if he is not security cleared at the required level and if he does not need to know them.

Article 20: Jobs catalogues

The senior defence and security civil servants [30](HFDS) develop the necessary instructions required for establishing, by a competent authority, within each State service and public or private organisation, and for each classification level, the list of jobs or functions requiring access to classified information or materials. These lists are designated "jobs catalogues". It is up to the HFDS to verify that these catalogues are set up for each of the three levels.

This is in reference to the jobs catalogues that the personnel security clearance requests are established. When a personnel security clearance request reaches it, the security clearance authority verifies the registration of the concerned function in the corresponding jobs catalogue. It examines, exceptionally, the merits of the request when the employment is not found in the catalogue.

These catalogues can be established by direction, by service or at the decentralised service levels of the State. They are updated at least once a year, especially at the time of service

[30] Article 12 of this instruction.

reorganisation. So as to facilitate the update, it is verified with the holders of listed employments if they have effectively had access to classified information for the concerned level.

The hierarchical authority estimates the posts or functions really requiring access to classified information or materials. It seeks to limit the resulting personnel security clearance requests to what is strictly necessary. Thus, it is agreed to avoid the securiy clearance procedures undertaken for ease for all service personnel, if each member does not individually have a proven requirement to access an element covered by national defence secret.

In companies holding a contract involving access or possession of classified information or materials, a directory of security cleared people exists in lieu of the jobs catalogue.

Article 21: Need to know

The PSC does not allow unlimited access to all the classified information or materials at the corresponding level. An cleared person only accesses classified information or materials if his hierarchical authority estimates that this access is required in the exercise of his function or for fulfilment of his mission.

The hierarchical authority firmly and gradually appraises the need to know basis of classified information.

Article 22: Information for candidates at Personnel Security Clearance

During their PSC request, the candidates are informed, through personal notice given to them, of the obligations to be fulfilled induced by the PSC as well as the provisions relating to their criminal liability in case of compromise[31].

At the notification of the granting of a favourable security clearance decision by the security officer, the initial information is completed by an awareness session to the risks of compromise, then, afterwards, by periodical reminders of the regulation in force.

An awareness to the investigations threats or approaches by unknown people or foreign organisations is made to individuals before they leave the national territory, whether the destination State is linked to France by a security agreement or not. Before their departure, basic cautionary rules are reminded to them[32].

[31] Articles 411-6 to 411-8 and 413-9 to 413-12 of the Criminal Code.

[32] The search for information remains the essential aim of special foreign services. The latter try using all the vulnerability elements presented by the travellers. It is possible that a traveller has been "targeted" by the intelligence and security services of the destination country. His behaviour should always take note of this potential risk. Also, different caution rules and common sense should be respected while travelling abroad. The recommendations can be made before departure and completed by passport of advice to travellers edited by ANSSI announcing best practices during the missions abroad with especially a mobile telephone, a personnel assistant or a laptop.

Chapter 2:
Personnel Security Clearance

Article 23: The object of the PSC

The hierarchical authority shall ensure that the personnel placed under his responsibility is appropriately security cleared and, thus, initiate, by the constitution of a file, the security clearance procedure at the level required by the jobs catalogue.

The PSC request triggers a procedure meant to verify that a person can, without risking the defence and national security or his own security, know classified information or materials in the exercise of his functions. The procedure includes a security inquiry allowing the security clearance authority to take its decision after knowing the entire reason.

Classified information or materials cannot be brought to the knowledge of people who have not been granted a PSC. Also, any person wanting or occupying a post for which the requirement for a PSC is proved and who refuses to submit to the security clearance procedure shall be removed from the considered post.

Article 24: Personnel security clearance procedure

The procedure prior to granting the security clearance decision is an operation costly in time and personnel. Therefore, when a post vacancy requires a PSC at the level *Secret Défense* or *Confidentiel Défense*, the procedure is only engaged for the benefit of the person effectively named in the job, except in rare cases. Anticipating the filling of the post by going through the security clearance procedure without waiting for the effective commencement of duty can be a measure of good management, which allows the newly hired person to know about the classified information without wasting time. He should however avoid any useless overcharge of services responsible for this mission by limiting as many PSC requests as possible.

When the PSC required is of *Très Secret Défense* level, it is up to the employment authority to appreciate the opportunity for an inquiry on each candidate to the concerned post.

1) Constitution of the file

The PSC file aims at gathering the elements which will be verified during the security inquiry[33].

In order to simplify the constitution of PSC requests files and to accelerate their circulation between the different actors, the dematerialisation of procedures should be encouraged.

[33] The collection of personal datas is subject to strict conditions, pursuant to Law no. 78-17 of January 6, 1978 relative to IT, files and liberties.

In electronic format, the PSC request and personal notice can be downloaded and completed electronically. The transmission of file to the investigating services can be made electronically, on the condition that the information system employed guarantees the identification and the authentication of the sender and the recipient, ensures the confidentiality and the integrity of datas and allows tracing of actions to be carried out.Where it is not possible to use the electronic procedure, the PSC file is constituted of[34];the PSC request formulated by the Head of the employer service attesting the need to know classified information or materials at a given level, for a person designated by name, along withthe personal security notice, filled completely by the concerned person and checked by the security officer of the service or the organisation to which he belongs. It is made in three copies (one original and two photocopies, dated and covered by the original signature of the candidate) and ofthree original identity photographs, identical and recent.

The PSC file is addressed by the Head of the employer service to the security clearance authority (SGDSN, HFDS, ASD, prefects) who checks that it is complete and sends it for instruction:

- for the *Très Secret Défense* level, to SGDSN, which manages the inquiry by the competent investigating services;
- for the levels *Secret Défense* and *Confidentiel Défense*, directly to the competent investigating services.

2) Instruction of file

The security inquiry led in the framework of the security clearance procedure is an administrative inquiry allowing detection of possible vulnerabilities in the candidate.

It is duly conducted by:

- the investigating service of the Ministry of the Interior[35]for Civil Personnel (including those working for the police) or organisations working in the civil domain;
- the investigating services of the defence ministry[36]for the civil or military personnel of the defence ministry, the military personnel of the police, the personnel employed in organisations or companies working for the Ministry of Defence[37].

The administrative inquiry is founded on objective criteria allowing to determine whether the concerned person, by his behaviour or by his surroundings, presents a vulnerability, or because he himself is a danger for the secret, or because he is found exposed to a risk of blackmail or pressure that can put the interests of the State in danger, blackmail or pressure exercised by a foreign information agency, a terrorist group, an organisation or a person engaged in anti-social activities.

[34] Model 02/IGI 1300 in annexe.
[35] Central department of internal intelligence.
[36] Defence security protection department or general external security department for all the personnel working for him.
[37] The files of military or civil personnel which have been submitted to a security notice sent by the investigating services of the defence ministry remain attached to them, in the assumption of a new administrative inquiry, during a period of five years after the end of their functions.

3) Closing of the inquiry and security notice

The administrative inquiry led in the PSC framework ends by sending a security notice, by which the investigating service informs of its technical conclusions to the only authority competent for taking the security clearance decision.

This notice is an evaluation of possible vulnerabilities detected during the inquiry and allows the decision-making authority to appreciate the opportunity to grant a PSC to the concerned person, with regard to the elements communicated and the guarantees that it presents for the level of PSC required.

The conclusions of the security notice are of three types[38]:

- "no objection notice", when the instruction has not revealed any element of vulnerability constituting a risk for the security of classified information or materials nor for that of the concerned person;
- "restricted notice":, when the concerned person presents certain vulnerabilities including direct or indirect risks for the security of classified information or materials to which he would have access, but that the specific security measures taken by the security officer would allow to control;
- "unfavourable notice", where specific information shows that the concerned person presents vulnerabilities which put on the secret such risks that no security measure seems sufficient to neutralise.

The security notice is emitted for a given level of PSC. The "no objection" notice is valid for the specified level as well as for lower levels. For restrictive or unfavourable notices, the investigating services give their opinion on a case by case basis, on the opportunity to grant security clearance for lower level[s].

The restrictive or unfavourable notices may be classified at the discretion of the investigating service.

The restrictive or unfavourable notices are accompanied by a confidential file indicating the reasons for the notice. This file is composed of two distinct parts, allowing the separation of elements, non classified, which can be communicated to the candidate, and those which are classified, which can only be brought to the knowledge of the clearance authority. Since it cannot be copied, the confidential file is returned after communication and without delay to the investigating service which despatched it, for storage purposes.

The validity of the duration of the security notice is in accordance with the required level of clearance. It cannot exceed:

- five years for the level *Très Secret Défense* ;
- seven years for the level *Secret Défense*;
- ten years for the level *Confidentiel Défense*;

[38] Each minister can decline each of these three categories for adapting it to his own requirements.

The security notice does not include in itself an authorisation or a refusal, and does not bind the security clearance authority, who takes its decision after having appreciated the different elements collected during the inquiry into the matter.

Article 25.: The decision

The decision to grant or to refuse a PSC is delivered by the security clearance authority[39] with regard to the conclusions of the investigating service. Whatever be the meaning of the security notice, to which it has however made no reference in the decision, the security clearance authority can accept or reject a request to grant security clearance.

The security clearance authority can decide, when the inquiry has highlighted some elements of vulnerability, of not granting clearance before taking specific precautions. Thus, so as to guarantee the most efficient protection possible for the classified information or materials, the attention of the employer, by a warning procedure, or that of the concerned person itself, by an alert procedure, is drawn on the risks to which one or the other is found exposed. The caution and alert procedures can be cumulated.

1) The decision to grant a personnelsecurity clearance

The security clearance decision is the authorisation given to a person, in accordance with his need to know, for accessing classified information or materials at the level specified in the decision, as well as at lower level[s].

For the level *Très Secret Défense*, the decision specifies the special classification in issue. When a person must have regular access to information relevant to several special classifications, a security clearance decision shall be sent for each classification. Therefore, a person can be subject to several security clearance decisions.

2) The warning procedure

When a security notice is restrictive or unfavourable, the security clearance authority can nevertheless decide to grant security clearance while warning the competent security officer. This procedure allows the security officer to implement security measures or take specific precautions with regard to the concerned person, if required with the advice of the HFDS or the investigating services. The investigating services, attached to the HFDS, estimates, among the elements revealed by the inquiry, what it needs to tell the security officer and, if required, the employer.

At the issue of the warning interview, a specific attestation[40] is signed by the security officer of the employer service. The security clearance decision is only granted at the issue of the procedure. The attestation is conserved by the security clearance authority.

At level *Très Secret Défense*, the warning procedure is managed by the SGDSN, who maintains the attestation.

[39] Article R. 2311-8 of Defence Code.
[40] Model 17/ IGI 1300 in annexe.

3) The alert procedure

When the security clearance authority decides to give the PSC on the basis of a restrictive security notice or in spite of an unfavourable security notice, it can select requesting alerting the concerned person, which consists of creating awareness in the latter on the communicable elements of vulnerability revealed by the inquiry[41]. The alert is managed by the security clearance authority, in the presence of the concerned security officer. The security clearance authority defines the modalities of the alert procedure attached to the investigating service and can, on a case by case basis, solicit its presence during the meeting with the concerned person. As required, the security officer studies with this service the additional security measures to be implemented with regard to the situation.

At the issue of the alert interview, a specific attestation[42] is signed by the security clearance authority representative, failing which, by the security officer of the employer service and by the concerned person.

The security clearance decision is only granted at the end of the procedure. The attestation is maintained by the security clearance authority.

At level *Très Secret Défense* , the alert procedure is managed by the SGDSN, who maintains the attestation.

4) Refusal to grant security clearance

The concerned person is informed of the unfavourable decision taken about him. A PSC refusal does not need to be justified when it rests on classified information[43].

Article 26.: Notification of the decision

The decision taken by the security clearance authority is forwarded to the security officer. On receipt, the latter notifies the candidate waiting for security clearance of the personal decision taken on his case, whether it is favourable or not.

1) Favourable decision and responsibility commitment

The decision to grant security clearance is notified by the competent security officer to the concerned person, who signs a responsibility commitment[44]. By this act, the candidate recognizes having knowledge of specific duties imposed by the access to classified

[41] It can be, for example, his tiees with foreign countries or various particularities of his environment. It is up to the investigative services of appreciating, for each case, what can be considered as a vulnerability.
[42] Model 18/ IGI 1300 in annexe.
[43] The provisions of article 1 of the law 79-587 of July 11, 1979 relating to the justifications of administrative acts and the improvement of relations between the administration and the public impose the justifications of unfavourable administrative decisions. It however makes an exception especially during the consultation or communication of these decisions brought to affect national defence secret, in pursuance of art. 6 of the law no. 78-753 of July 17, 1978 bearing various measures of improvement of relations between the administration and the public and various administrative arrangements, social and fiscal (article 6- 2, b).
[44] Model 08/ IGI 1300 in annexe.

information or materials, as well as sanctions provided by the Criminal Code in case of non-compliance, intentional or not, of the regulations protecting national defence secret.

It is also notified to the concerned person that he is bound to inform the security officer at the earliest, during the entire duration of his PSC, of any change affecting his personal life (marriage, divorce, PACS, starting or breaking of a live-in relationship ...), his professional life or his residential address. He is told that he should inform him of any ongoing or frequent relationship, exceeding strictly professional relationships, with one or several foreign citizens. The security officer should then make him fill, so as to update the information, a personal notice 94 A and send it to the security clearance authority (electronically when the procedure is dematerialised). This change of situation can justify a re-examination of the security clearance file and, if required, the referral to the investigating service in view of delivering a new notice.

The second part of this commitment is signed by the concerned person at the end of his functions or at the withdrawal of the PSC, and specifies that the duties related to the protection of classified information to which he could have been given access, persist beyond the term given to his functions or his PSC. Once signed, this second section is returned to the security clearance authority.

2) Refusal of PSC

The PSC refusal is notified to the concerned person by the security officer. person At this occasion, the individual concerned is informed, according to the modalities defined by the ministerial department he belongs to, of the ways to appeal and the time periods which are open to him for contesting this decision.

If the candidate solicits, through appeal, an explanation of the refusal of the PSC request, he obtains communication of the reasons if they are not classified. When they are, the candidate will find the rules applicable to the information protected by the secret applying to him.

Article 27.: Duration of the PSC validity

The PSC validity duration is linked to the occupancy duration of the post which has justified its clearance. It ceases when the concerned person leaves his job.

The security clearance decision specifies in principle itself its duration of validity. It cannot exceed that of the security notice with regard to what has been taken.

In the sole case of a request for renewal of the PSC formulated within the time given in Article 31, and if no observation has been sent by the investigating services, the security clearance decision is implicitly extended for a maximum duration of twelve months.

Article 28.: PSC and change of assignment

When a person who has been granted security clearance is re-assigned, his PSC for the initial post ends[45] and another decision can be taken if the new assignment requires it, on the basis of the security notice in progress.

If the competent security clearance authority changes, the security officer of the service left sends the security clearance decision and the responsibility commitment to the authority which has decided to grant the security clearance. So as to inform the new security clearance authority that a security notice is valid, the security officer of the service left sends him a security certificate. If the notice is restrictive or unfavourable, the new security clearance authority can, for taking its decision, ask to know the reasons.

For the *Très Secret Défense* level, when the PSC becomes moot due to the change of assignment of its holder, the competent authority notifies it to the SGDSN and returns to him immediately the security clearance decision as well as the responsibility commitment (part 2), duly signed.

Article 29: Storage of decisions

During their validity period, the security clearance decisions are stored by the security officer of the employer service. These documents, which carry a mark of protection [46] are not in any case given to the concerned parties nor copied.

If necessary, a security certificate[47] delivered for a determined mission and a limited period, can be given to the concerned parties by the security clearance authority. The issue of these certificates can be delegated to the security officer. It is the responsibility of the individual concerned to destroy or to ensure that the certificate is destroyed as soon as he returns from mission.

The elements related to the PSC are stored for a duration which is defined by each minister for the department under his responsibility. This duration cannot be less than five years to be counted from the expiry date.

Article 30.: PSCs Directory

In each ministerial department, it is required, for each of the three classification levels, a directory:

- of PSC files in the course of instruction;
- of valid PSCs.

The SGDSN updates the central directory of PSCs at *Très Secret Défense* level, included in the international domain.

[45] Except for the security clearance decision expressly covering several posts, in accordance with the article R. 2311-8 of the Defence code.
[46] Confidential Personnel.
[47] Model 07/ IGI 1300 in annexe.

For allowing the SGDSN to evaluate the total number of PSCs delivered and of people having access to classified information or materials, the HFDS sends him, at the end of the year, a status of people in his own department holding a PSC at the levels *Secret Défense* and *Confidentiel Défense*, within the framework of the annual evaluation report mentioned in article 12 of this directive.

Article 31: End of PSC

The PSC ends in three ways: either when the concerned person quits the post which has motivated his security clearance, or when the validity of the PSC expires, or because the PSC is withdrawn.

1) Termination of services

The PSC linked to the occupation of a post or to the exercise of a determined function expires when its holder changes his assignment or stops his functions. In quitting the employment specified in the security clearance decision, the holder signs, in accordance with the provisions of Article 26 of this instruction, the second part of the responsibility commitment.

2) Expiry of validity and renewal

The holder of a PSC whose term fixed in the decision is going to expire, signs in accordance with the pre-cited Article 26, the second part of his responsibility commitment.

Only, with regard to the provisions of Article 27 of this directive, a renewal request initiated in the required notice and time allows to provisionally extend the validity of the PSC, so as to avoid an inappropriate interruption of the conditions of employment, of the function or of the mission of the holder.

The renewal request shall be carried out within six months and, at the latest, one month before the expiry date of the PSC in progress.

It is composed of a new PSC request file identical to the one described in article 24 of this directive.

When the procedure can be dematerialized, the new request is sent in the same conditions as the initial request.

The validity of the initial PSC decision is extended by a maximum period of twelve months after expiry of the security notice, when the need to know classified information remains beyond the duration of validity of this notice, in accordance to the provisions of Article 27 of this directive, and to the imperative condition that a renewal request has been regularly made, waiting for the conclusions of the inquiry of the new file.

This extension is authorised in the same conditions when a request, at a higher level, is formulated within six to one month (at the latest) preceding the expiry date of the PSC in progress.

3) PSC withdrawal

The decision to grant security clearance does not give its beneficiary any acquired right for its maintenance. The PSC can be withdrawn in the course of validity or at the time of a renewal request if the concerned person does not fulfil the required conditions for its delivery, which can be the case when the vulnerability elements appear, indicated for example by:

- the investigating service;
- the hierarchical superior or the concerned security officer, after change in situation or behaviour revealing a risk for defence and national security.

The withdrawal decision is notified to the concerned person in the same notice as the PSC refusal, described in article 26 of this directive, without the justifications being communicated if they are classified. The concerned person is informed of ways to appeal and time periods which are open to him for contesting this decision.

Chapter 3:
Specific cases

Article 32: The security screening procedure

Different from the PSC by its nature and by its objective, the security screening procedure is a simplified administrative inquiry, solicited by the security clearance authority, meant for ensuring the integrity of a person. It guarantees that the degree of trust which is possible to give this person is compatible with the function, assignment or recruitment for which it is sensed or allows him to have access to certain protected areas. It is specifically applicable to the case of maintenance personnel.

The security screening requests are investigated by the competent investigating service, which sends an opinion to the applicant. The validity duration of this notice is left to the discretion of each ministerial department.

Article 33: Decision for approval

When a person, whose position is not registered in the jobs catalogue, is allowed, within the framework of his functions or for a special mission, in a limited manner, to access classified information or materials or to view them, he can be issued a 'decision for approval'. The same is applied when the concerned person holds a PSC at a certain level and when he needs, in a limited manner, to access classified information at a higher level.

The approval, given following a request, duly justified by the competent authority and after an ordinary administrative inquiry procedure or a simplified procedure in accordance with article 34 of this directive, occasionally authorises access to classified information or materials.

The approval must not, in any case, be considered as a PSC in reserve, given as a precaution to an unspecified number of people to meet vague requirements.

At the level *Très Secret Défense*, a catalogue of jobs requiring an approval must be drawn up.

Article 34: Simplified procedure

Public officials, civil servants or contractual staff, civil or military, can be security cleared at the level *Confidentiel défense* by the authority to which they report and without intervention of the investigating services to this effect, provided that:

- they are subject to a security screening[48] procedure at the time of their recruitment or their assumption of duties;
- they occupy a post figuring in the jobs catalogue;
- they fill the security clearance notice, certifying on oath the accuracy of information declared;

[48] Article 32 of this directive.

- they have signed the responsibility commitment defined in Article 26.

At any time the hierarchical authority can demand that an administrative inquiry may be carried out by the competent investigating service.

The PSC decision by simplified procedure is notified to the concerned person under ordinary conditions.

Article 35: Emergency procedure

The emergency procedure is an exceptional procedure allowing the issuing of a PSC to a person within a very short period of time, so as to allow him to access classified information or materials as soon as he resumes his duties. Validity duration of this provisional security clearance cannot exceed six months.

Persons belonging to the following categories can particularly benefit from this procedure:

- senior officials, diplomats, generals;
- persons sent on mission in the framework of unexpected operations;
- high level officials appointed under conditions not allowing compliance with ordinary deadlines.

The file is constituted according to ordinary procedure but the Head of the employer service must, in the request, specify and give the grounds for urgency of PSC and the impossibility to proceed otherwise.

For the *Très Secret Défense* level, the SGDSN, with regard to elements transmitted by the Head of the employer service, is the sole competent authority to begin such a procedure.

Within fifteen days following their submission, the investigating services issue a provisional security notice in view of which the competent authority can take a provisional PSC decision.

The emergency procedure can concern only a very limited number of people. It can neither replace nor interrupt the normal procedure, which continues after the issue of provisional security notice.

When a provisional PSC has been given in the framework of the emergency procedure, its validity expires:

- either when the decision of PSC or rejection is taken by the competent authority, on receipt of the final security notice, at the end of the ordinary clearance procedure
- or at the latest six months after its date of issue.

Article 36: Courier security decision

Without prejudice to the provisions foreseen in articles 57 and following of this directive, a classified document or materials at the *Confidentiel Défense* and *Secret Défense* level can be

transported by personnel internal to the department or body, holding a "courier security" decision [49]. This decision is made by the security clearance authority after carrying out, by investigating services, a security screening procedure which is valid, according to the request by security clearance authority, either for a special mission or for a period of not more than three years[50].

This decision does not, in any case, grant an authorisation to access classified information.

The decision can be renewed. When the decision is made for a given duration, not exceeding, in any case, three years, the renewal request must necessarily be made before the expiry of the fixed deadline.

For the *Très Secret Défense* level, the transportation complies with specific modalities, defined by special instructions[51].

Article 37: PSC of foreign nationals

Foreign nationals in a job requiring access to classified information or materials, and within strict 'need to know' limits, can be granted security clearance at the *Confidentiel Défense* and *Secret Défense* levels.

The clearance procedure is carried out by the concerned ministry, its delegate (HFDS, prefect) or the Designated Security Authority (DSA). The security clearance decision is taken by the same authority.

The SGDSN, in its capacity of NSA (National Security Authority), ensures the link with foreign NSA to obtain elements allowing instruction of the PSC file of the concerned person. Communication with foreign NSA takes place through its intermediary. However, it can authorise direct exchanges between Designated Security Authorities (DSA) and their foreign counterparts.

If a PSC intervenes in the framework of either an international organization having a specific regulation related to protection of classified information or materials or of a multilateral agreement containing special provisions in this domain, or of a bilateral security agreement, one should refer to specific provisions of these texts so as to determine conditions and clearance procedures to be applied. In case of difficulty, the NSA defines the procedure.

When provisions expressly provide it, a PSC given by a foreign NSA can be taken into account by relevant French authorities when the foreign national has a job in France requiring access to classified information or materials. Considering the security certificate produced by the foreign NSA, a security clearance decision can be issued by the concerned security clearance authority.

[49] Model 05/ IGI 1300 in annex.
[50] Article 32 of this instruction and model 03/ IGI 1300 in annex.
[51] Directives for practical application no. 02/SGDN/SSD/CD dated February 3, 1986 on the organization and functioning of special classifications Très *Secret Défence*.

When there is no security agreement between France and the State of which the concerned person is a national, no PSC, at any level, must, in principle, be issued by a French authority. Under exceptional circumstances, if the need to know is proven, the requesting authority can approach the French NSA which will assess the advisability of the PSC and will define, if necessary, the procedure to be followed, before taking its decision.

Article 38: Impact of the PSC decision in International matters

Any decision to grant PSC to classified information or materials in the national field can by itself, in the absence of a specific PSC and subject to the need to know, give access to classified information or materials of the corresponding or lower levels of international matters or entrusted to France pursuant to Security Agreement concluded between the signatory States of the North Atlantic Treaty, legal provisions introduced in the framework of the European Union and Security agreements signed by France.

A PSC decision for classified information or materials in international matters does not give access to classified information or materials at national level.

TITLE III:
SECURITY MEASURES RELATED TO CLASSIFIED INFORMATION OR MATERIALS

→ The decision to classify an information or a material under National Defence Secret aims to restrict access to this information or materialss only to people holding the appropriate PSC and having a need-to-know;
→ It is taken according to criteria defined by a ministerial directive;
→ Its appropriateness must be rigorously assessed;
→ It places this information or material under the protection of specific criminal provisions [52];
→ The classification is evidenced by affixing a specific mark allowing characterization of the crime in case of compromise.
→ The compromise can result from a malevolent act as from simple negligence.

Chapter 1:
General principles of classification

Section 1: The rules of classification

Article 39: Responsibility for the decision of classification

For the *Très Secret Défense* level, the means for protecting classified information or materials are determined by the Prime Minister through specific instructions[53].

For Secret *Défense* and *Confidentiel Défense* levels, each minister determines, under conditions laid down by the Prime Minister, which information or materials should be classified at which level and the means for ensuring their protection.

Within each ministry, the decision for classification is taken on a proposal from the author of the document, at the best hierarchical level to be able to evaluate its potential. The person responsible for this decision, who must be in a position to justify it to his hierarchy, is called the classifying authority or the originating authority.

The decision to classify results from the analysis of the importance of the information in relation to its context, applicable rules and instructions from the competent minister. The

[52] Article 413-9 and the following articles of the Criminal Code.
[53] Article R2311-5 of the Defence Code and practical application guidelines no. 02/SGDN/SSD/CD dated February 3, 1986 on the organization and operation of special *Très Secret Défense* classifications. Complete or partial reproduction of this information or materials, which can only be done by the issuing registry, is formally forbidden to the holder.

classifying authority ensures that the level of classification is appropriate for the concerned information or materials, that is, it is both necessary and sufficient. It thus seeks to limit the proliferation of classified documents and to avoid improper classifications, which generate operational costs, heavy workloads and alter the value of national defence Secret. This evaluation includes assessment error risks which may lead, inversely, to information, which deserves classification, to not be classified, which constitutes a breach of the rules of confidentiality for which the originating authority is responsible[54].

In case of modifications, over time or due to circumstances, of the sensitivity of the classified information, the classifying authority can decide to declassify, downgrade or upgrade the information[55]. It shall notify its decision of modification or of deletion of the classification to the recipients of the information or materials.

Obvious cases of over-classification or under-classification are reported by the recipient(s) to the originator who will, if necessary, by appropriate amendment, inform all recipients and take the necessary measures in order to avoid any breach when the document's level changes.

Article 40: Criteria of classification

The criteria for classification and the importance of only classifying what is really necessary are stated in a ministerial directive[56].

The classification level is determined by the nature of the classified information or materials. The source of the information can also be considered when its sensitivity justifies its protection[57].

When a document includes various parts, some requiring classification and others not, one should strive to display them separately so as not to hinder the distribution of unclassified information. Distribution of unclassified part of the document is made possible by placing the information covered by national defence secret as classified annex.

Any group[58] of documents containing information classified at different levels must itself be classified at least at the highest level of these documents.

[54] Article 4 of this directive.
[55] This means deleting the classification, lowering or raising its level respectively. These operations are carried out in the same way as the classification.
[56] See classification guide in annex 2. Additional guidelines, corresponding to specific needs of each department, can be produced.
[57] By source, we understand the intelligence system(s) that produced the information.
[58] Pages, paragraphs, annexes, or attached documents.

A group of information or materials, sometimes called “aggregate”, is classified if the grouping of information or materials of which it is made, justifies it, even though none of these elements, taken individually, is classified.

An extraction of classified information retains the level of classification of the original information itself, unless the classifying authority decides otherwise[59].

Article 41: Identification of the classification

Any information or materials, legally comes under National Defence Secret, from the moment it is subjected to classification measures intended to restrict its distribution, signaled by a reference to the level of classification on the information materials[60].

The preparatory materials used in the preparation of the classified information (drafts, paper prints, portable IT equipment[61]), and which are not identified, are placed under the responsibility of those who prepared them. They must be destroyed or deleted as quickly as possible once they have served their purpose, in any event, no later than when the classified document is issued.

Section 2: The marking

Article 42: The general principle of marking

Marking, by its three components that are the stamp, identification and pagination, allows for the verification of authenticity and integrity of the information materials. Each copy of a classified document bears mention of the classification level of the contained information.

Paragraphs, clauses and annexes dealing with classified information at a lower or unclassified level are highlighted, as appropriate, by noting their specific level of classification in the margin and by a layout that clearly sets them apart from the general context of the document.

Up to the *Secret Défense* level, abbreviations indicating the classification can be used to specify the classification level of paragraphs of the text. The allowed abbreviations are:

- *Confidentiel Défense*: CD;
- *Secret Défense* : SD.

These abbreviations do not replace the mention in full of the classification on the paper copy of the document, done by the stamping.

If it is physically impossible to place the marking on a classified material or containing classified information, it is advisable to implement safeguards designed to eliminate any ambiguity that may arise from the absence of visible indications of classification. To this end, each ministry shall produce specific directives, after liaising with the SGDSN, in order to adapt to the characteristics of the materials, the rules and regulations related to marking and allow the identification of the required classification level.

[59] For the marking of paragraphs, please see article 42 of this directive.
[60] Articles 2311-4 of the Defence Code and 413-9 of the Criminal Code.
[61] USB keys, floppy disks, CD, CD-ROM, etc.

The lack of implementation of these instructions voids the criminal protection granted by national defence secret. Strict compliance with guidelines is therefore a major challenge.

Article 43: The marking of paper copies

The marking of a paper copy includes the stamp, identification and pagination:

- the stamp indicates the classification level and allows, by its position, size and color, to immediately draw attention to the secret character of the information or materials;
- identification consists of the references of information materials;
- Pagination consists of the numbering of each page and the mention of the total number of pages contained in the document.

1) Stamp

The stamp with the mention of classification is affixed, in red ink, or, under exceptional circumstances, in a color that contrasts with that of the information materials, in the middle top and bottom of each page. For bound documents, a larger model stamp is affixed in the middle bottom of the cover and the title pages[62].

When documents are produced on a computer, marking must be added electronically on the page header and footer.

The stamp, whose size can be adapted to that of the information medium, is permanent and always visible.

2) Identification

Any classified document is identified right from the first page. In addition to common references of all administrative documents, special measures are taken. Thus, on the first page of the document, there are references of the issuing department, date of issue, registration number, classification level stamp and time period stamp (i.e. date on which the classification of the document is re-examined). Where appropriate, indications of downgrading or declassification is affixed on the same page.

For documents classified at the *Secret Défense* level, each copy is personalized and the total number of copies is indicated on the document. The registration number originates from the relevant secret protection office.

3) Pagination

Each page of the document is numbered. At the bottom of the first page, the total number of pages, annexes or plans that make up the document are mentioned.

The pages of each annex are numbered independently of the pagination of the document itself, and bear the mention of the total number of pages of the annex.

[62] Model 15/ IGI 1300 in annex.

For documents classified at the *Secret Défense* level, blank pages and interleaves are also numbered. All blank pages bear the mention “NO TEXT” in the middle.

Article 44: The marking of a non-paper copy

The marking of a non-paper copy of classified information is adapted to the type of material and is permanent and always visible. It consists of a stamp and an identification.

1) Stamp

The stamp specifying the level of classification has a size that is adapted to that of the materials and bears mention of this level in full. In case of practical difficulties, abbreviations referred to earlier can be substituted.

2) Identification

Identification of non-paper copies of classified information is provided by the inscription of references and, where applicable, of the volume of each recorded information. When it is impossible to write all references on the materials, identification is made possible by the registration number.

For the *Secret Défense* level, the registration number is issued by the secret protection office and is possibly accompanied by a sheet where regulatory references of the contained information are registered.

3) Pagination of electronic documents

Each page of the document is numbered. At the bottom of the first page, the total number of pages, annexes or plans that make up the document are mentioned.

The pages of each annex are numbered independently of the pagination of the document itself, and bear the mention of the total number of pages of the annex.

For documents classified at the *Secret Défense* level, blank pages and interleaves are also numbered. All blank pages bear the mention “NO TEXT” in the centre.

4) Special provisions

Due to the technical possibility of recovering information that has, in principle, been deleted, an IT medium of classified information always retains its initial level of classification. It can only be downgraded or declassified if the information that it contains or contained has itself been earlier subject to such a measure.

Section 3:-Logging

Article 45: Logging of classified information or materials

Any medium containing classified information is logged, in chronological order, by a manual or computerized logging system, allowing for the identification of recipients.

The recording unequivocally establishes the allocation of an information medium to a holder, an individual, who is clearly identified. This holder then assumes the responsibility for protecting the information medium. This logging is the only reference of this allocation of responsibility.

The mention of the purpose of the document, if this purpose is classified, must not figure in the logging system, unless it is a classified and dedicated system. This obligation to classify and to dedicate the logging system itself is imposed at the *Secret Défense* level.

At the *Confidentiel Défense* level, the logging system can be linked to a mail management database provided that access to the database is restricted and allows tracking documents up to its last holder.

At the *Secret Défense* level, the logging system is kept up to date by the secret protection office. *Secret Défense* documents are mandatorily subject to a double numbering, in the notice of a fraction: they bear the registration number of the originator and that of the secret protection office responsible for processing them.

Section 4: -Duration of classification of the classified information or materials

Article 46: The classification life cycle

Given that the sensitivity of classified information or materials may evolve with time or due to circumstances, it is the responsibility of the originating authority to assess the duration of the need for classification. The originating authority mentions on the document[63] the date from which the document will be automatically declassified. When this date cannot be determined, the originating authority mentions the date or deadline after which the classification level must be re-evaluated. The re-evaluation can result in maintaining the classification level, downgrading or declassifying the document. The originating authority can also set as threshold, not a date but a specific event (for example, the start of production of a materials, withdrawal of a materials, end of fiscal year, etc.), following which the document will be automatically downgraded to a specified level or will be declassified. It reserves the possibility of extending, at any time, the deadline that it has set.

In any event, the review of the need and level of classification of the information or materials must be conducted rigorously at intervals not exceeding ten years, clearly specified by each minister for the department under his charge. This rigorous management is even more important, given that upon expiry of a delay of fifty years from the date of issue of a classified document, under the conditions stated in article 63 of this directive, arises the question of communicability of the document and its prior declassification.

In case of classified information or materials of foreign origin, only the foreign originating authority may conduct a declassification or downgrading.

[63] See stamp model in annex.

Chapter 2:
Management of classified information or materials

Section 1: Storage of classified information or materials

Article 47: Physical conditions of storage

Outside the usage periods, classified information or materials are stored in safes or armored cabinets compliant with the instructions relating to secured furniture mentioned in this directive. No details related to the type of information contained should be visible on the outside of the safe or cabinet.

The combination of the safes, sufficiently complex to be reliable, is known only to the users. A copy of this combination is kept in an opaque and sealed envelope, in the safe of a specially designated authority, the key of this safe is itself kept in a different safe.

The combinations are changed at least every six months, and each time that there is a transfer of users, a risk or suspicion of compromise.

The keys are imperatively secured, especially outside working hours, following a clearly established procedure by each responsible authority (deposited in a wall safe, without key, with combinations and with single-control or with use of a safety badge, permanent guards with alarm system).

It is strictly forbidden to take out of the work sites:

- classified information or materials, except on urgent service requirements;
- keys for safes or cabinets where such information or materials are stored.

The responsibility for maintaining *Secret Défense* classified information or materials is incumbent upon the trusted holder or the head of the secret protection office.

Section 2: Reproduction

Article 48: General rules of reproduction

The generalization and diversity of reproduction means increase the risks of uncontrolled distribution of classified information or materials.

For the *Secret Défense* and *Confidential Défense* levels, detailed instructions are established by each minister or his representative (HFDS – Haut Fonctionnaire de Défense et de Sécurité) for the department under his charge, in order to set up:

- the appointment, by directors or service managers, of authorities empowered to authorize reproduction;
- procedures for controlling reproduction;

- the need to record in a logging system the number of documents reproduced and their holders.

The equipment used for reproduction of classified information (photocopiers, fax machines, computer systems, etc.) must be physically protected in order to limit their use to authorized persons only. The maintenance of this equipment shall be carried out in such conditions so as to ensure the security of classified information which has been reproduced, in compliance with the recommendations of this directive. The same applies to their scrapping, which must ensure that the memories of these devices are destroyed.

Article 49: Total reproduction

At the *Secret Défense* level, the total reproduction of classified information or materials is only possible with prior authorization from the originating authority. The custodian of the information or materials, who wishes to reproduce them, must send a justified request to this authority. If the authority consents to the reproduction[64], it specifies the numbers to be allocated to additional copies and shall indicate this reproduction on the copy in its possession.

In case of emergency and in exceptional circumstances, the custodian can be dispensed of this procedure provided the following conditions are met:

1) the number of reproductions is kept to the strict minimum;
2) regulatory marking is carried out by allocating to each copy an individual number composed of two fractions:
   - the first having as numerator the number of the copy in the series of reproductions and as denominator the total number of reproductions;

   - the second being the individual number of the copy, as allocated by the document originating authority;

3) bear if necessary, on the reproduced copy, the purpose for which it was made or draw up a separate list of recipients;
4) promptly report to the originating authority the number of reproductions, the reproduction numbers and purpose of the copies. The originating authority indicates these reproductions on the copy in its possession.

At the *Confidentiel Défense* level, the reproduction can be made by the holding authorities, under their responsibility, provided a logging system is used to keep track of the number and recipients of the reproduced copies.

Article 50: Partial reproduction

Extracts of classified documents are themselves classified at the level appropriate to their content. If an extract of a classified document does not justify a classification, its importance must remain limited so as not to compromise, if disclosed, the information from which it was extracted. The distribution of unclassified sequential extracts of classified information is prohibited.

[64] Model 12/ IGI 1300 in annex.

Extracts of *Confidentiel Défense* or *Secret Défense* classified information can be reproduced by their custodian under conditions fixed by article 49 of this directive.

When extracts of documents containing classified information are transferred to another medium, even when these extracts are themselves classified, the reference to the classification is transferred onto the new medium, in accordance with the requirements of this directive.

Section 3: Inventory

Article 51: The inventory procedure

Classified documents are subject to constant monitoring so as to ensure their traceability and that the authorized holders take them into account.

To this end, each minister recommends the procedure for inventory and monitoring of *Confidentiel Défense* and *Secret Défense* classified documents held in all departments and agencies within his department.

A counter-inventory is made at every staff turnover, the previous holder and his replacement both signing the minutes.

The inventory period is utilized to reduce the workload of the management of classified documents. Dates of expiry of validity are checked for downgrading or declassification: the re-evaluation of the level of protection of classified documents and if necessary, their destruction must be carried out.

At the *Confidentiel Défense* level, it is recommended to carry out an annual inventory. This inventory is to be carried out under the responsibility of each holder or by a specialized office. If it is carried out, a report should be drafted. Failing that, an annual verification count must be done according to procedures defined by the ministerial directives in order to verify the physical presence of the documents.

At the *Secret Défense* level, the annual inventory, which is mandatory, is carried out by the secret protection offices, liaising with the holders. The HFDS collates the minutes of the inventory and transmits to the SGDSN a summary, at the most on March 31 each year, in the annual evaluation report mentioned earlier.

The minutes of the annual inventory, prepared by each secret protection office, mentions references and identification of each *Secret Défense* classified information medium, and is accompanied, otherwise[65], by one of the following administrative documents:
- a receipt from the new holder;
- minutes of destruction;
- minutes of remittance in an archive repository.

[65] These documents will only be attached to the inventory if they concern transportation of documents that took place since the production of the minutes of the previous annual inventory.

Section 4: Protection of classified equipment

Article 52: General provisions and classifications

Protection of classified equipment involves the implementation of security measures at all stages of production (program, analysis, planning, manufacturing or construction, test, etc.) as well as during utilization, maintenance, repair and transport until decommissioning and destruction.

The responsible authority (the program director until the delivery or holding authority during utilization) determines the equipment to be protected and the classification level to retain, which can be different from that covering the documents (manuals, maps, etc.) which concern them.

It is important to eliminate any possibility of ground or aerial view and the use of technical means of detection and identification. An effective way of ensuring protection of *Secret Défense* level classified equipment consists in storing them in an area complying with the protection rules defined by this directive. The area in question must be set up in a protected zone in order to be able to criminalize the violation of the prohibition to enter.

When the equipment is in service or exposed to the view outside a protected area, the authorities in charge see to it that adequate measures are taken to protect the classified equipment and their components.

Article 53: Protection of classified equipment during transportation

Distribution and transportation of classified equipment requires special security measures: protection against being seen as far as possible and permanent guards during transportation.

The routes are chosen according to the degree of security that they confer. Depending on the type of equipment to be protected and from the moment the transported equipment is on the list maintained by the Ministry of Defence, the special provisions should be referred to[66].

For the other classified equipment, the authority that requested the transportation is responsible for the following tasks:

- packaging of equipment;
- selection of routes and stop over points, in agreement with the concerned civil or military authorities;
- organization of a convoy or escort and technical provisions in case of breakdown or accident.

The transportation of classified equipment is carried out by national means, except in cases where this is absolutely impossible or cases of joint operations. Otherwise, it must be

[66] Inter-ministerial directive no. 3100/SGDN/ACD/PS/DR dated June 25, 1980 on the safety of transportation of certain sensitive equipment made in civil liability and inter-ministerial instruction no. 312/SGDN/ANSDR dated August 21, 1981 on nuclear safety in the field of Defence.

conveyed and all arrangements made so that security is ensured without interruption throughout the entire duration of the transportation.

Chapter 3:
Distribution and carriage of classified information or materials

Section 1: The distribution and dispatch of classified information or materials

Article 54: Distribution

When circulating classified information or materials, the dispatching authority draws up a list of recipients and ensures that they are granted security clearance at the required classification level.

At the *Secret Défense* level, the number and reference of the materials allocated to each recipient as well as the numbers of copies retained by the originating service is identified in the mailing list (at least two copies, of which an original intended eventually for the archives).

The list of recipients, when it is in itself a secret, is not attached to each dispatch of the information medium copies.

Article 55: Electronic distribution, dispatch and receipt of classified information or materials

Electronic distribution, dispatch and receipt of classified information are governed by the provisions in Title V.

Article 56: Dispatch and receipt of classified information or materials

The dispatch of classified information or materials is subject to a specific procedure by which to monitor and ensure the physical integrity of the document through a special conditioning.

The dispatch authorities are:
- at the *Secret Défense* level, the secret protection office;
- at the *Confidentiel Défense* level, the security cleared personnel, in accordance with the principle of need to know.

The originating authority, after marking and logging of each information medium, performs the following operations:

1) Dispatch

- Conditioning

Classified information or materials are dispatched in a double envelope, strong enough to ensure maximum physical integrity of the information materials:

- the plastic-coated outer envelope indicates the sending service, the address of the recipient (without explicit mention which may draw attention to the classified nature of the content) and the monitoring reference. It does not, in any case, bear mention of the classification level of the information or material that it contains. At the *Secret Défense* level, each envelope is numbered;
- the inner security envelope is opaque and of good quality, if possible the cloth lined or reinforced type, and must prevent discrete opening or re-sealing. It bears the stamp of the classification level, reference of information materials being transmitted, the seal of the sending authority, the name and function of the recipient as well as reference to the department or agency to which it is assigned.

    - Monitoring of dispatch

A dispatch slip, without classification stamp or indication of the purpose of the information sent is placed in the internal security envelope, whose number it bears. It contains three detachable sheets A, B and B'[67] signed by the head of the sending authority or a person designated by him.

The A and B sheets are destined to the recipient, who retains the first as proof and sends back the second as acknowledgement of receipt. The colored B' sheet is kept by the dispatcher until sheet B is received, for which it is then substituted.

2) Receipt

Reception formalities are handled by the secret protection office of the recipient body or, at the *Confidentiel Défense* level, by the recipient of the dispatch.

It is necessary:

- to check the integrity of the packaging in order to detect a possible compromise;
- to log or to get the classified information or materials logged, in accordance with the provisions of article 45;
- to sign and to send back sheet B of the dispatch slip as acknowledgement of receipt.

On receipt of *Secret Défense* classified documents, the secret protection office sends them to the recipient.

Section 2: Carriage

Article 57: The carriage of classified information or materials on the national territory

The procedures for transmitting classified information materials must be capable of meeting deadlines compatible with the degree of urgency and ensure the best protection of the transmitted materials.

The carriage of classified materials over national territory is carried out as below:

1) Within the same building

[67] Models 14/ IGI 1300, 14 bis/ IGI 1300 and 14 ter/ IGI 1300 respectively in the annex.

In order to avoid their observation, classified information or materials are transported internally in an envelope, either:

- by the holder himself;
- by another cleared person;
- by a courier or by an authorized staff of the internal courier service.

The position of classified information and materials must be continuously monitored, particularly in the classified documents logging system.

At the *Secret Défense* level, a report at the secret protection office must be made.

This rule can sometimes be relaxed for a brief and temporary communication of classified information or materials. The holder of classified information materials, responsible for their carriage, is accountable. He must check their position and reintegrate them as soon as the operational requirements allow it.

2) With change of buildings or geographical area

At the *Secret Défense* level, the carriage can be made :

- by an authorized courier or by any person cleared at the required level: the classified information or materials are placed in a bag or suitcase that can be locked, devoid of any remarkable external features; the holder may not, under any circumstance, part with it until he has delivered it to the receiving secret protection office;
- by military means: under conditions set by the instructions of the Ministry of Defence.

In the absence of any courier or any security cleared personnel available within a certain time period not compatible with the degree of urgency that must be duly justified, civil postal services are authorised within the national territory, under the imperative condition of resorting to postal operators proposing protected carriage, such as registered mail having a declared value or recorded delivery mail with acknowledgment of receipt.

At the *Confidentiel Défense* level, the carriage can be made:

- by an authorized courier or by any person cleared at the required level: the classified information or materials are placed in a bag or suitcase that can be locked, devoid of any remarkable external features; the holder may not, under any circumstance, part with it until he has delivered it to the recipient;
- by military means: under conditions set by the instructions of the Ministry of Defence;
- by civil postal services within the national territory, under the imperative condition of resorting to postal operators proposing protected carriage, such as registered mail having a declared value or recorded delivery mail with acknowledgment of receipt.

The crucial reliability of postal operators responsible for carrying classified documents depends particularly on their capacity to meet the requirements imposed by this directive.

The postal operator may entrust the performance of a task to a subcontractor but it retains full responsibility for the execution.

Only those postal operators can be approached if they:
- have an establishment on the national territory;
- are granted a Facility security clearance;
- have a security program catering for valuable articles by means of a signature service including an ongoing monitoring and logging allowing to identify at all times, the person responsible for guarding the concerned articles, either through a signature and clocking-in register, or by an electronic monitoring and logging system.
- obtain and provide the sender a proof of delivery on signature and clocking-in register or a receipt showing the package numbers;
- ensure that the delivery will be made within a maximum of 24 hours, or before a given date and time.

The sender verifies the projected date and time of delivery and immediately informs the recipient department by a standard fax or email, indicating the courier depot office and the information medium references, excluding their purpose and secret nature. On receiving the courier, the secret protection office or the recipient acknowledges receipt. In case of abnormal delay, there is suspicion of compromise and the secret protection office or the recipient department implements the provisions of Article 67.

Verifications[68] are made with the postal operators in collaboration with specialized services to ensure that the conditions of storage and delivery of classified information or materials are met.

Article 58: Overseas carriage of classified information or materials

Classified information or materials sent overseas or passing through a foreign country should be permanently protected to prevent their compromise during transportation and particularly during stopovers.

Only the following means are authorized:
- specialized military courier;
- diplomatic pouch and courier mail;
- courier certificate.

The postal option can be authorized for *Confidentiel Défense* level information materials, under the conditions mentioned in article 57 by using the “international registered” priority service for dispatch towards countries of the European Union or NATO.

For information exchanged under an agreement or an international program, provisions of applicable regulations should be consulted.

1) Specialized military courier

[68] In accordance with the provisions of title VI.

Classified information or materials at the *Secret Défense* level are normally transported via diplomatic pouch or eventually by specialized military courier.

For military organizations, the courier service is the central administration mail office (BCAC). In case of exceptional emergency, it is possible under certain conditions to receive, aside from the diplomatic pouch, a "courier letter" delivered by the Ministry of Foreign Affairs[69].

2) Diplomatic pouch and courier letter

Upon delivery of the dispatches, no later than the eve of departure of the pouch to the diplomatic pouch division of the Ministry of Foreign Affairs, a visible seal must be affixed on the outer envelope or on a label fixed to the package, mandatorily containing the mention "By accompanied suitcase-satchel".

Transportation is mandatorily done by an authorized courier or by a cleared person provided that the "satchel" does not exceed 20 kg. Otherwise, it is necessary to provide special measures in accordance to the instructions of the Ministry of Foreign Affairs. A "courier letter" certifies the quality of the carrier so as to avoid scrutiny of the consignment by customs or the relevant police department.

The April 18, 1961 Vienna convention on diplomatic relations prohibits any demand by foreign authorities to submit the consignment to them and stipulates that "the diplomatic pouch shall not be opened or detained". The courier need only present his "courier letter" and seek, if necessary, assistance from the nearest diplomatic or consular officer. If however the relevant authorities of the host State request that the bag may be opened in their presence, the courier has the right to refuse and return with the pouch to the State of origin.

3) Courier certificate

When an international security agreement or regulation makes provision for it, it is possible to make the carriage through an authorized courier, under conditions laid down in article 57. The courier is then equipped with a courier certificate for one or several journeys[70] issued by the NSA or the delegated security authorities. The courier is reminded that he is committed, throughout the journey, to keep in his possession or under his direct surveillance[71], the package containing classified documents, equipment or components.

Chapter 4:
Destruction and archiving of classified information or materials

Section 1: Destruction of classified information or materials

[69] Diplomatic pouch division.
[70] Models 09/IGI 1300 (single journey) and 09bis/ IGI 1300 (multi-journey) in the annex.
[71] This type of transportation does not benefit from the protection granted to the diplomatic pouch according to the April 18, 1961 Vienna Convention (article 27); the package transported can be opened by foreign authorities.

Article 59: The common procedure

When classified information or materials become obsolete or unnecessary, they can be destroyed with the agreement of the archive administration[72] for an original document. Destruction can be done only by securitycleared persons. Preparatory materials that are no longer applicable are destroyed without any particular formality.

Destruction of such documents is carried out in such a way as to make it impossible to even partially reconstruct any information contained on the storage materials.

Destruction techniques are adapted to the number and type of information materials to be destroyed. The main means of destruction are burning, incineration, grinding, shredding and power surges[73]. When classified documents have to be transported for incineration, they must imperatively have first been shredded and mixed.

After the operation, destruction minutes[74] are drawn. These minutes of destruction reports bear the signature of the holding authority and, for *Secret Défense* documents, that of a witness holding a PSC at *Secret Défense* level.

At the *Secret Défense* level, the holding authority of the document informs the classifying authority in writing that, unless it otherwise wishes, it will destroy the information medium. If there is no response within two months, the holding authority shall destroy the information medium and report to the classifying authority by sending it a copy of the minutes[75]. A copy of the minutes shall also be forwarded to the secret protection office.

Article 60: Emergency evacuation and destruction

In the face of exceptional circumstances and in case of immediate threat requiring the evacuation of buildings by staff or the destruction of classified information or materials, emergency evacuation and destruction plans are established by each department or agency holding classified information or materials. These plans provide procedures to access premises and classified information or materials, in all circumstances.

The terms of practical implementation of these plans are on cards which are available at all times to involved parties of each holding department or agency.

They specify:

---

[72] Article L212-2 of the Heritage Code.

[73] Burning consists in exposing the entire medium or the utilization zone to a temperature of more than 1000° C with a blowtorch; incineration is complete combustion reducing the medium to ashes, intended to prevent any dispersion of fragments; grinding consists in reducing the medium to pulp so that the residual pieces do not exceed 2 mm in diameter; shredding consists in reducing the medium to strips of less than 0.8 mm wide and 13 mm long; electrical surge consists in destroying power-supply circuits of the material by a positive overvoltage immaterialtely followed by a negative overvoltage (which does not, however, destroy the circuits containing information).

[74] Model 13/ IGI 1300 in annex.

[75] In case of dissolution of the service from which the authority which carried out the classification emanates, the copy of the destruction minutes is sent to HFDS of the relevant ministry.

- the list and location of classified information or materials to be destroyed or evacuated;
- measures applicable to the information system;
- the list and location of the means of destruction and evacuation to be used;
- authorities empowered to issue the order for destruction or evacuation.

The operation thus established must be tested by simulations, which, for the *Secret Défense* and *Confidentiel Défense* levels, are carried out at intervals, not exceeding three years, defined by each ministry.

Section 2: Archiving

Article 61: General archiving principles for classified information or materials

Any authority holding classified information or materials, either produced or received, is under the obligation to ensure its conservation and protection in accordance to legal or regulatory provisions and to operational regulations of the archiving service to which it is attached.

The Heritage Code defines archives as all documents, regardless of their date and place of conservation, their forme and their storage medium, either produced or received from any individual or corporation and by any public or private service or body, in the year of their activity[76]. It establishes a system of conservation and for consultation of archives applicable to all public or private archives.

Article 62: Transfer of classified information or materials to the archives

Classified information or materials are subjected to general provisions of the Heritage Code related to archives. On the expiry of their current period of use, they are sorted for separating documents intended to be kept from documents lacking administrative utility, historical or scientific interest and which are intended for elimination[77]. On this occasion, their classification level is revised each time as required.

The following provisions are applied to documents which, on the expiry of their current period of use, remain classified:

1) Destruction

Classified information or materials are destroyed under conditions described in article 59 of this directive, in compliance with the provisions of the Heritage Code.

2) Transfer to archive repositories

Once they are no longer routinely used, classified information or materials of administrative and historical interest are transferred, at intervals specified by each minister, to the following archive repositories:

[76] Article L211-1 of the Heritage Code.
[77] Article L212-2 of the Heritage Code.

- the defence history services, for the Ministry of Defence and services which are attached to it, be it for administrative matters as for the management of archives;
- the archives of the Ministry of Foreign and European Affairs, for matters relevant to it;
- the French heritage management authorities, national archives and public archive services of local and regional authorities, for all civil administrations and civilian agencies managing public archives (e.g. the Prefecture of Police).

Only these departments are equipped and empowered to receive classified information or materials up to the *Secret Défense* level. Information or materials at *Très Secret Défense* level can only be transferred after a mandatory and prior downgrading or declassification procedure.

Article 63: Communication to the public of classified information or materials transferred to the archives

Public disclosure of classified information or materials that have been transferred to the archive departments comes under the combined provisions of the Criminal Code[78], Heritage Code[79], the aforementioned law of July 17, 1978 on improving relations between the administration and the public[80], the December 3, 1979 decree related to Defence archives[81] and finally the December 1, 1980 decree[82] on the rules of the archives of the Ministry of Foreign Affairs.

A classified document transferred to public archives is, on the condition of having been first declassified, in principle, communicable as of right upon expiry of the fifty year period from its date of issue or that of the most recently classified document included in the file. This period, under certain circumstances, is increased to seventy five or hundred years[83]. A document may be incommunicable, whatever be the delay. Thus, in no way can an archive be communicated which may result in the risk of circulating information related to weapons of mass destruction[84].

Whatever be the duration of incommunicability allocated to the classified document, its communication is only possible after the declassification of the document. When the service keeping archives receives a request for communication of a document covered by national defence secret, it must send this request to the authority issuing the concerned document. This authority verifies the duration of incommunicability allocated to the document. If all time limits have expired, the originating authority proceeds with the declassification. The document may only then be disclosed.

[78] Article 413-10 and the following articles of the Criminal Code, related to compromise.
[79] Article L213-1 and L. 213-3 of the Heritage Code.
[80] Aforementioned Law no. 78-753 of July 17, 1978.
[81] Decree no. 79-1035.
[82] Decree no. 80-975.
[83] Article L. 213-2 (3°, 4° and 5°) of the Heritage Code (**annex 1**).
[84] Article L. 231-2 (II) of the Heritage Code.

A person wishing to consult a classified archive before the expiry of the applicable period of incommunicability must seek an exemption[85]. The service keeping the archives receiving the exemption request sends this request to the originating authority. This authority must always enquire upon the opportunity of declassifying the document. If keeping classification is justified, disclosure is not possible and the exemption is denied.

Chapter 5:
Additional marks on the limitation of the scope of distribution

Article 64: General principle

Classified information and materials which need to be subjected to specific distribution restrictions due to their contents, must, in addition to the possible mention of their classification level, bear a special mark specifying the services, States or international organizations that can access them[86]. This mark, affixed by the originator, has the effect of limiting the scope of distribution of this information and draws attention to the strict need to know. The eventual security measures relevant to the classification level are applied and classified information or materials are routed in such a manner so as to ensure compliance of the distribution scope thus defined.

Article 65: Determination and application of "*Spécial France"*

The *« Spécial France »* (*"Specific to France"*) mark is not a classification level. It is used for information or materials, whether classified or not, that the originating authority deems necessary to be disclosed to French nationals only and are not to be communicated, under any circumstances, fully or partially, to a foreign State or to one of its nationals, to an international organization or to company registered under foreign law, even if there is a security agreement with this State or this organization. The *« Spécial France »* mark can apply only to certain parts of a document.

When information marked *« Spécial France »* is classified, it must, in addition to being in accordance with the security measures fit for their degree of protection, be transmitted only to French individuals or legal entities duly security cleared and having a need to know.

The blue colored *« Spécial France »* stamp is affixed on top of the page, immediately to the right or below the information classification stamp and, for non-paper information materials, in accordance with the provisions of article 44 of this directive.

Routing of the classified information or materials is carried out by national courier offices and through national channels. If necessary, the *« Spécial France »* mention is indicated on the inner security envelope.

[85] Exemption from the rules for communicability of archive documents, considered in article L. 213-3 of the Heritage Code and decree no. 79-1035 of December 3, 1979 (article 7).
[86] Article R 2311-4 of the Defence Code.

« Spécial France » information is never mentioned on inventories or directories prescribed by security agreements or regulations.

These documents may leave the national frontiers by the diplomatic pouch[87], which constitutes a protected national circuit, ensuring the protection and compartmentalization of the transmitted information and involving the implementation, at all stages of routing, of security measures appropriate to the eventually set degree of classification. The same is applied to sending by specialized military courier or, in case of emergency, to the courier letter delivered by the Ministry of Foreign Affairs[88].

The rules applicable to information and physical materials are equally valid for electronic documents which can only be sent electronically via a specific national transmission channel offering all the aforementioned security and partitioning guarantees.

Chapter 6:
The compromise of a national defence secret

Compromising a national defence secret consists in revealing all or part of it, to someone who is not authorized to know. If deliberate compromises are rare, those due to negligence of the holder or by illegal access are common. Rivalry between States and economic competition between corporations fuel the active search for classified or strategic information and require that the protection of classified information or materials remains a key concern of any holding person or agency.

Article 66: Scope of the compromise

The appropriation, delivery or disclosure to uncleared persons or persons not having any need to know, of any element constituting a national defence secret constitute activities against the interests of the nation, and are considered as particularly dangerous. The articles 413-9 to 413-12 of the Criminal Code deal with breaches of national defence secret[89].

Disclosure or allowing the possible disclosure of a national defence secret (i.e. rendering it possible for one or several unauthorized persons to access it) constitutes the offence of compromise.

Any person holding elements covered by the national defence secret is responsible for them. It is his duty to prevent the communication of these elements to an unauthorized person, under penalty of him being prosecuted for the compromise.

For classified information, physical acts which result in the breach of national defence secret, can take three notices[90] :

---

[87] Article 27 of the 1961Vienna Convention.
[88] Article 58 of this directive.
[89] These provisions are not the only ones protecting the secret, articles dealing with treason and espionage also refer to them in an indirect manner (articles 411-6 for communicating a secret to a foreign power, 411-7 for collecting intelligence meant to be transmitted to a foreign power, 411-8 for carrying out an activity aimed at delivering intelligence to a foreign power).
[90] Article 413-10 and 413-11 of the Criminal Code.

- a positive act, consisting in destroying, stealing or reproducing a secret that one possesses;
- a passive attitude, consisting in allowing destruction, diversion, reproduction or disclosure of a secret, either by another holder or by a third party;
- a negligent or imprudent attitude, consisting in ignoring administrative instructions and regulations and thereby undermining the protection of classified information by exposing it to the risk of being revealed.

The person committing the violation may be a qualified person[91] or a third party[92]. A person is qualified when, by his status, occupation, function or mission, whether temporary or permanent, is authorized to access classified information and needs to know it. Any person who is prohibited from accessing the secret is considered as third party. Unlike the qualified person, the common third party may not be criminally charged for having a passive or negligent attitude.

Protection under criminal law is limited to information or materials subject to a classification measure. As long as this classification endures, regardless of its age or relevance, the offence of compromise retains its full application. A person holding a PSC is not released from his obligations when his PSC ends[93].

These provisions are applicable to acts committed to the detriment [94]:

- of countries having signed the North Atlantic Treaty;
- of the North Atlantic Treaty Organization.

They are also applied to information exchanged[95] :

- under a security agreement, duly approved and ratified between France and one or more foreign States or an international organization;
- between France and an institution or body of the European Union and classified under the security regulations of the latter, published in the Official Journal of the European Union.

The secret status is independent of the sometimes high number of people who know its content.

The violation for compromise is constituted even if disclosure is not made but simply made possible.

The sanction for an attempt at compromise is the same as for actual commission of the crime[96].

[91] Article 413-10 and 413-10-1 of the Criminal Code.
[92] Article 413-11 and 413-11-1 of the Criminal Code.
[93] Thus, for example, a person cannot testify before a court by revealing classified elements, unless these have been declassified beforehand.
[94] Article 414-8 of the Criminal Code.
[95] Article 414-9 of the Criminal Code.
[96] Article 413-12 of the Criminal Code.

Compromise of classified information is an offence. The particular nature of the breach causes important procedural peculiarities in the opening prosecution, jurisdiction and applicable sanction.

Besides criminal sanctions, the perpetrator of an act, committed deliberately or not, which compromises a national defence secret, incurs the withdrawal of his security clearance and will be subject to disciplinary sanctions which can seriously affect the course of his career.

Legal entities are criminally responsible for compromises attributed to them and incur, in addition to a fine, prohibition to carry on the activity in the fiscal year or during which the offence was committed[97].

Article 67: Procedure to be followed in case of compromise

Speed and discretion of intervention are of utmost importance in order to limit the consequences of the disclosure of compromised classified information or materials.

Any discovery of a potential compromise is reported immediately to the hierarchical authority and to the head of security of the concerned organization. In case there is a proven compromise or a mere suspicion, they must be directly and promptly reported to:

- either the competent department of the Ministry of Interior[98], in charge of centralizing the cases and for conducting an inquiry under the control of the judiciary;
- or the relevant department of the Ministry of Defence[99], which in turn notifies the relevant department of the Ministry of Interior;
- the HFDS of the concerned ministry who notifies himself the SGDSN.

In matters regarding Information Technology, disappearances, thefts, accidental losses of classified equipment or attacks against information systems are the subject of an information systems report of loss or attack, addressed without delay:

- directly to the HFDS of the concerned ministry;
- through the hierarchical channel of the concerned ministry, to the originating authority of the classified information and to SGDSN, so as to inform them about possible consequences of the compromise;
- to the concerned investigating service, if it is not itself the issuer of the minutes.

The head of the service immediately takes the adequate measures to prevent repetition of such occurrences, in collaboration with the security officer.

Not reporting such acts, which facilitate the disclosure of classified information, leads to administrative or professional sanctions.

---

[97] Articles 121-2 and 414-7 of the Criminal Code.
[98] Central Directorate of Interior Intelligence (DCRI - *Direction centrale du renseignement intérieur*).
[99] The Directorate for Defence Protection and Security (DPSD - *Direction de la protection et de la sécurité de défense*) or the General Directorate for External Security (DGSE - D*irection générale de la sécurité extérieure*) for its domain of competence.

The Ministry of Interior, in addition to the information mandatorily given on a case by case basis, provides the SGDSN with an annual review of the cases reported and the progress of any procedure or action taken on each account.

The annual evaluation report of secret protection prepared each year by the HFDS[100] indicates the number of reported or suspected cases of compromise as well as actions taken.

When the compromise concerns foreign classified information, the French NSA promptly informs the foreign NSA. When an DSA is concerned, it promptly informs the foreign NSA as well as the French NSA. When *Secret Défense* level information is compromised, the DSA reports to the French NSA, which in turn will itself forward the information to its foreign counterpart.

Chapter 7:
The access to classified information by magistrates

The primary judicial role of the magistrate with regard to national defence secret is to punish the reported shortcomings in its protection. However, the magistrate can himself be confronted to this secret, during his investigations, by the authority responsible for classifying a document whose disclosure is refused to the magistrate. Indeed, neither the magistrates nor the judicial police officers are authorized to know the elements under cover of secret.

Now if denying access to a magistrate constitutes the offence of obstructing justice[101], granting access exposes one to the criminal sanctions applicable to compromise. In order to resolve this paradox, and ensuring preservation of the national defence secret, while promoting the course of justice and avoiding any obstruction to the smooth running of proceedings, the conditions under which the magistrates can access classified information, which is instrumental in finding the truth, are clearly defined.

Article 68: The means of access to classified information by magistrates

To have elements of classified information relevant to the investigations that he is conducting, the magistrate has three possibilities: the search inquiry, the audition and the judicial summons.

1) The search inquiry

A search inquiry for the purpose of obtaining classified elements involves, in most cases, the magistrate entering the premises where such documents are kept. Thus, the search inquiry is dealt within the provisions dealing with granting access to sites holding national defence secret[102] .

2) The hearing

[100] Article 12 of this directive.
[101] Article 434-4 of the Criminal Code.
[102] Article 81 of this directive.

No administrative authority may authorize any of its agents to speak about classified information unless it has not been previously declassified. An person holding a PSC, who cannot be released from his obligations to protect the secret, can, in no case, be heard by a court on elements that are still classified, under pain of incurring penalties applicable to the compromise.

3) The judicial summons

The judicial summons is the most frequently used means by courts in matters of classified information. The magistrate sends to the administrative authority responsible for the classification, that is to the competent minister, a judiciary summons for transmission of elements instrumental in finding the truth.

Two situations can arise:

- either the magistrate has identified the classified element(s) that he requires and sends a declassification request directly to the classifying authority;
- or the magistrate wishes to be informed of a number of elements that he cannot accurately identify; he then requests the concerned administration to search for these elements, sort them and communicate the unclassified elements, the classified ones needing first to be the subject of a declassification request.

Article 69: The procedure for declassifying classified information

The declassification of classified information, sought by motion, can be decided after consulting the Consultative Commission on National Defense Secret.

1) Request for declassification of information

A French court may, within the context of proceedings pending before it, request declassification of elements protected by national defence secret [103]. This justified request is sent to the administrative authority which has classified the document, which in turn promptly refers to the Consultative Commission on National Defense Secret (CCSDN).

The CCSDN, which is an independent administrative authority[104], shall issue an advice, shedding light, for the classifying authority, on the advisability of declassifying and communicating the information designated by the court, to the exclusion of information whose classification rules are not under the jurisdiction of French authorities only[105]. For elements classified by foreign authorities or international organisations such as NATO or the European Union, it is the responsibility of the magistrate to consult the concerned authority or organisation. He may, if he whishes, ask the SGDSN, national security authority, for further information on the procedures.

[103] Article L2312-4 of the Defence Code.
[104] Created by a July 8, 1998 law, this independent consultative body is dealt with in the articles L 2311-1 to 2311-8 of the Defence Code.
[105] Article L.2312-1 of the Defence Code.

The reason stated by the requesting magistrate allows the Commission to validate on the one hand the validity of the entitlement to jurisdiction by making sure that the elements for which declassification is requested effectively concern the proceedings, and on the other hand, to sort the requested classified documents so as to determine which can lead to finding the truth.

2) The decision of the Consultative Commission on National Defense Secret

The Commission has access to all classified elements. In order to attain its objective, it is authorized to open, if required, the seals of classified elements which are submitted to it. It mentions it in the minutes of the session[106].

The CCSDN issues an opinion within two months of referral. This opinion takes into account the objectives of the judiciary in regards to public interests, that the presumption of innocence and the rights of the defence are respected, that international commitments of France as well as the necessity to preserve defence capabilities and the security of personnel are respected. The opinion can be favorable, partially favorable or unfavorable to declassification. The opinion is forwarded by CCSDN to the competent minister in his capacity as the classifying authority[107].

3) The decision of the classifying authority

The decision of the Commission is advisory. Therefore the minister has discretion to order declassification despite an unfavorable opinion or to refuse declassification despite a favorable opinion. Within a period of fifteen days inclusive of receipt of the opinion of the CCSDN[108], the competent minister shall notify his decision, which does not have to be justified, accompanied by the recommendation of the opinion, to the concerned court. The recommendation of the opinion given by CCSDN is published in the Official Gazette of the French Republic[109].

Each declassified element is accompanied by an express indication of declassification specifying the date of the minister's decision. The element can then be transferred to the file of proceedings to be examined by the magistrate and submitted to the different parties which will be able to carry out an adversarial hearing. Erroneous transfer of a classified document to a judicial file can result in criminal penalties.

[106] Article L2312-5 of the Defence Code.
[107] Article L2312-7 of the Defence Code.
[108] Or at the expiry of the period of two months given to CCSDN to formulate its opinion.
[109] Article L2312-8 of the Defence Code.

TITLE IV:
PROTECTION OF SITES

→ Security rules for sites are implemented to protect classified information or materials against any internal or external threat that can affect their availability, integrity, confidentiality and also to prevent access by any unauthorised person.

→ Physical protection measures applied to an information depend on its classification level;

→ Every physical protection system must be based on a risk assessment ;

→ A protection system is satisfactory when it sufficiently delays intrusion so as to allow the setting up of intervention means before the elements covered by national defence secret are compromised;

→ The basic security screening of physical or legal entities are foreseen for the execution of sensitive contracts within sites holding national defence secrets;

→ Access by a magistrate to sites holding national defence secrets is allowed under clearly defined conditions and involving the intervention of the CCSDN.

Chapter 1:
Principles of physical sites protection

Article 70: General principles

The physical protection is a set of security measures intended to guarantee the integrity of buildings and premises specifically dedicated to classified information or materials, as well as the reliability of furniture in which they are kept, in order to avoid any loss, degradation or compromise. It also aims to facilitate the identification of the author or the authors of a possible intrusion.

The degree of physical security applicable to sites for ensuring their protection, depends on the classification level of documents which they protect, their volume and the threats to which they are exposed.

The global protection system and technical solution retained, are based on the outcomes of the assessment of threats and restrictions inherent to the site environment, as well as the work methods and management of classified information or materials (for example, in accordance with the circulation of these information or materials in the site and the number of individuals having access to it). The vulnerabilities linked to the information systems shall also be taken into account.

This set of protective measures consists of four combined or separated elements in accordance with their classification level:

- one or several protective devices (barriers);
- one or several detection and alarm devices;
- intervention means based on procedures and established instructions;
- one or several deterrent devices (indications).

Thus, a satisfactory security system aims, by delaying the intrusion (no barrier is impossible to clear), and allows the implementation of intervention means, alerted and guided by the detection devices before the classified information or materials are compromised.

To be effective, a physical protection system must rely on an accurate risks analysis of risks, and:

- be multifaceted, that is, in line with the concept of defence in depth, including several successive devices, additional, of different nature, associated or combined to one or several alarm-devices relying themselves on different principles;
- be homogenous, that is guarantee the same efficiency in all respects, the intrusion always operating in less resistant sites, and the value of a system equivalent to that of its weakest element;
- be dissuasive, that is contribute to reduce the risk of an intrusion attempt;
- be controlled, that is be tested frequently in order to verify its operational state;
- be traceable, that is providing any means that can bring a historical functioning of various components.

In order to avoid intrusion of an unauthorisedperson, who always represents a threat to classified information or materials which are stored, inside a site or a protected premises, physical protection must necessarily include an access control system[110].

The access control consists of a material means to ensure a person's right as to whether he can access the site or information. Therefore the aim is:

- Filtering the traffic flows, individuals and vehicles wishing to enter or exit a site, building or premises;
- Checking individuals or vehicles in the protected areas;
- Preventing or limiting movement of unauthorised individuals.

Access control consists of different levels of mechanism:

- Authorised access ;
- Identification and/or authentication of the person;
- Processing and tracking later the identification of somebody upon entry or exit.

Physicaly securing energy access, technical premises and means of communication, is also part of the physical protection of classified information or materials.

[110] **Annex 4.**

Article. 71: Physical security protection

The types of physical protection measures, their articulation, according to the type of barrier, and the specific measures at higher classification levels, are given in detail in **annexes 5 to 7.**

The physical protection system of any classified information or materials consists of several "barriers", inclusive and successive:

- the surrounding building and/or the building itself;
- the premises containing the furniture;
- the furniture in which the classified information or materials is stored.

The level of protection of the entire system depends on the level of protection ensured by the measures applied to each of these "barriers". To set a minimum threshold of physical protection, it is therefore necessary to classify each barrier according to the degree of resistance that it opposes to intrusion attempts. These classes are given in detail in **annex 6.** The physical protection classes specified therein, according to the classification levels of materials to be protected, are minimal thresholds to be followed strictly.

The minimum class of furniture to be used for ensuring the conservation of classified information or materials is defined according to the class of other barriers in accordance with the table in **annex 6**.

On a foreign territory, and taking into account its specific environment, organisations protecting classified information or materials shall, except in the event of external operations, use the protective measures described in this Directive.. Besides, and considering their specific environment, the premises where classified information or materials are stored may be subject to additional security measures, such measures being the results of a precise risk analysis led by the person responsible for the site concerned.

The protection rules of an international organisation could be retained for a French representation physically situated within an entity related to this organisation, or applying, according to the security agreements in force, measures that are consistentwith the aforesaid rules.

In circumstances where the detention of classified information is required, but where appropriate physical protection measures cannot be set up, compensatory measures are taken in order to preserve the same level of protection. These alternative measures should be preceded by a specific risk analysis, carried out by the person in charge of the concerned site, and be validated by the competent investigating service. The level of protection must at any event be sufficient, to allow the taking into account of the actual time of intervention before the intrusion.

Article 72*:* Consultation of investigating services for the physical protection of *Secret Défense* documents

The handling and storage, within premises, of classified information or materials at the *Secret Défense* level and above can only intervene, except in force majeure cases, after consultation with the investigating services about the capacity of these premises to receive such documents.
Due to the diversity of protective devices available on the market and the evolving techniques used, the concerned authorities may, if necessary, consult the competent investigating services of the Ministries of Defence and Interior, on the efficiency of materials and protection systems they want to install, or in order to check the validity of the materials and systems in place.
The investigating services particularly ensure that the risk analysis and physical protection measures, whether regulatory or compensatory, have taken into account the actual time elapsed between the detection of the intrusion, the resistance of mechanical means and the possibility of an intervention.

Chapter 2:
The protected areas

Article. 73: Definition

The aim of the protected area is to ensure to the sites interesting national defence, whether they are services, establishments, public or private companies, a legal protection against intrusions, complementary to the physical protection mentioned before. They are established according to the protection need determined by the competent minister.

The protected area is defined in article 413-7 of the Criminal Code. It consists of premises with defined and enclosed areas, where traffic is prohibited and access is subjected to authorisation in order to protect installations, materials, research secret, studies or manufacturing or classified information or materials that are found there. Boundary lines are visible and cannot be crossed through inadvertence.

The procedure for creating protected areas is defined in articles R. 413-1 to R. 413-5 of Criminal Code.
Measures to restrict access are taken up by the responsible authority. All accesses should be permanently controlled so that any access inside a protected area cannot be done through ignorance. To that effect, numerous notice boards are placed at adequate spots.
Authorisation to access a protected area is given by the Head of the service, building or company, under supervision and control of the authority who had considered the creation of the protected area.

By virtue of aforesaid criminal provisions, any person who enter a protected area without authorisation is liable to be prosecuted.

Chapter 3: The restricted areas

Article. 74: Creation of restricted areas

The aim of the creation of restricted areas is to grant a reinforced protection to information and materials, as well as to information systems classified at the level *Secret Défense*.

Each Minister must ensure that restricted areas are created, by decision of the authorities in charge of the storage of classified information, in all departments and organizations which usually work out, process, receive or possess information or classified materials at *Secret Défense* level. Moreover, thereation of restricted areas, even temporary, is recommended in the departments or organisations dealing occasionally with classified information or materials at that level.

A restricted area cannot be created outside a protected area. It can be included in a protected area or is similar to it.

Security measures applicable to restricted areas are defined in **annex 7**.

Chapter 4:
Sites temporarily holding secrets: Protection of meetings and conference rooms

Article. 75: The preparation and organisation of meetings and conferences

The organising authority shall ensure the protection of classified information or materials exchanged during a meeting, conference, training or presentation of materials.

The premises planned for the session during which classified information and materials are processed shall be:

- safe from directly or indirectly hearing interceptions (soundproofing, absence of microphone) and unauthorised camera;
- accessible only to authorised individuals (possible creation of a temporary protected area).

The technical control of sites is carried out regularly by the security service.

The organising authority specifies, in the invitations or convocations to a meeting, conference, training or presentation of materials, the classification level of classified information or materials which will be communicated, in order to allow the designation of individuals holding a PSC at the required level and having a need-to-know. The limits and the degree of accuracy to be brought to the communication, during conferences or presentations of materials, must be determined in advance by the officer in charge.

The authorities receiving the invitation, sent in time to the organising authority, the names and tasks of individuals authorised to represent them as well as their level of PSC. The organising authority then makes a list of all individuals attending the meeting, in whatsoever capacity: auditors, lecturers, assistants, technicians in charge of screenings or trials, etc.

Article. 76: Protection of classified information or materials during meetings and conferences

The organising authority verifies the identity and PSC level of each participant present, if necessary through security certificates[111]. It ensures that during the meeting, nobody holds devices allowing the intercepting, rebroadcasting and recording of information such as, for example, a mobile phone, a personal data assistant (PDA) or laptop.

The organising authority can prohibit any note taking or any recording of speeches by the auditors. It ensures that communication is limited to the purpose of the meeting in pursuance of the strict principles of partitioning of classified information, particularly for levels *Très Secret Défense* and *Secret défense.*

In some facilities allocated to the requirements of defence and national security, radio jamming equipment can be used for rendering inoperative, both for transmission and for reception, electronic communication devices of all types (mobile phones and laptops for example)[112].

Article. 77: Security measures at the end of a meeting or conference

In case of communication of *Très Secret Défense* or *Secret Défense* information, the organiser writes down, in a short report to be possibly classified, information spheres that have been displayed, the measures taken to ensure their protection, as well as, the list of participants, mentioning the proof of their PSC.

The organising authority of the meeting proceeds at the end of the session:

- to the retrieval and security of classified information or materials possibly made available to the auditors (documents, graphs, plans, films, tapes, etc.);
- to the destruction of provisional and preparatory materials.

Auditors and participants assume full responsibility for the protection of their work documents and notes, which are classified to the level corresponding to the information collected. These documents are destroyed under their care when they are no longer useful.

The transmission of notes taken by the participants, or of their reports of the meeting, is carried out by the methods provided in articles 57 and 58 of the present directive.

A control list of tasks to be carried out during the preparation, during and at the end of the meeting figures in **annex 8**.

[111] Model 05/IGI 1300 in annex.
[112] Article L. 33-3 of the postal and electronic communication code.

Chapter 5:
Access by unqualified individuals to sites holding national defence secrets

The necessity for performing a duty, whether it is a sensitive contract or the need to intervene on emergency, or an inspection task, can require the access by unqualified individuals to sites holding elements concealed by national defence secret.

Article 78: Access by unqualified individuals to sites holding national defence secrets

1) The term "sensitive contract" includes any contract or deal, regardless of its legal status or denomination, with the exception of jobs contracts, where performance is made to the benefit of an organisation or within a site holding classified information or materials in which a public or private co-contractor of the administration, takes precautionary measures, including jobs contracts of its employees, intended to ensure that the conditions for performing the task do not compromise security or essential interests of the State.
Basic security screening of the legal entity may be solicited by the contracting authority, on the basis of elements provided as part of the contract. This basic security screening is concluded by a notice. Arestricted notice may lead to the elimination of the application of the concerned company. The notice given by the investigating service is consigned in a shuttle form[113] sent to the contracting authority or the adjudicator.

Sensitive contracts include a clause on protection of secret compliant with the standard article figuring in **Annex 10**. The contracting authority may complete or adjust the standard article depending on the specifications of the said contract, without however going against the article.

It may prescribe this standard article, completed or adapted this way, in the sensitive subcontracts.

2) In the case of a sensitive contract bearing on carriage of classified information or materials, on security services of sites holding elements under national defence secrets, whatsoever they may be, as well as, on the maintenance in such areas, only the individuals belonging to the concerned company and who have previously been subject to a basic security screnning defined in Article 32 have the right to execute this contract.

3) The employment contracts of individuals executing a sensitive contract include a clause on protection of secret as presented in **annex 09**. When an employee performing an ordinary employment contract, is subjected to the conditions applicable to sensitive contracts, an amendment in accordance with these provisions is included in his employment contract.

The parties to the employment contract may complete or amend the article previously mentioned, according to the specifications of the said sensitive contract, without being contrary to it.

[113] Model 17/IGI 1300.

4) The individuals intervening in matters of assistance, for security or fire control, acting in cases of real emergency, are allowed to carry out the operations required in such situation, without being subject to normal formalities. If, in exceptional circumstances, one of these individuals by any chance accesses a national defence secret, he is liable, in case of disclosure, to the penalties provided in Article 413-11 of the Criminal Code.

Article. 79: Access by unqualified individuals on account of a control mission

Some individuals, in their particular capacity, and for the practice of the assignment conferred by law, may have to enter sites holding secrets, without having the capacity or necessity to access these secrets. This is particularly the case for individuals responsible for visits or inspections under the labour laws or even international inspections conducted pursuant to an agreement[114].

These individuals must be authorised by the responsible authority of the site, to enter areas in which classified information or materials is processed, and are previously subject to an identification check and control of their capacity.

In terms of social legislation, companies bound by a contract as defined in Title VI of this directive[115] should seek to reconcile the priority of protecting national defence secret with the need to apply the labour law[116] rules.

In principle, no company should be a barrier to the tasks of inspection, investigation or control conducted by the medical inspections team, investigators, inspectors, prevention engineers and civil servants who hold, for the execution of their assignments[117], the right to enter in all premises where employees work[118], the possibility to analyse any sample[119], and books, records and documents relevant to the fulfilment of their mission should be made available to them[120]. However, when the company holds elements protected by national defence secret, and in accordance with the previous provisions, only the responsible authority of the site can allow them to enter areas where classified information or materials is processed, and this, after identification check and control of the capacity of those officials[121].

However, although these individuals undertake not to reveal manufacture secrets or operation methods that might be revealed to them on this occasion[122], unless being prosecuted on the

[114] In this hypothesis, specific procedures are set up, particularly concerning inspections by formalities provided for by the international agreement for the prohibition of chemical weapons, signed in Paris on January 13, 1993.
[115] The following provisions do not apply to the State, or to the local authorities or to their public administrations (articles L. 8113- 8 and L. 8114-3 of the labour code).
[116] Articles L. 8112-1 to L. 8123-4 of the labour code. The peace of social relationships, the security of the employees and the fight against illegal employment can contribute to the protection of national defence secret.
[117] Articles L. 8112-1 of the labour code for the inspectors, L. 8113-11 for the supervisors, L. 8123-1 for the medical inspectors, L. 8123-4 for prevention engineers.
[118] Articles L. 8113-3 to L. 8113-5 and L. 8123-3 and 4 of the labour code.
[119] Articles L. 8113-3 to L. 8113-5 of the labour code.
[120] Articles L. 8113-4 and L. 8123-4 of the labour code.
[121] Article L. 8114-1 and 2 of the labour code: the refusal by the responsible of the site to lend himself to these operations is a crime of obstruction.
[122] Articles L.8113-10 and L. 8123-5 of the labour code.

basis of breach of professional secrets[123], they are not authorised, unless they have been duly security cleared and can prove their need to know for the fulfilment of their mission, to access or to be acquainted with classified information or materials, such access remaining subject to compliance with rules set by the present directive.

In general, the rules on protection of national defence secret apply to any inspection or control provided for by laws or regulations.

If, in exceptional circumstances, one of these participants accesses a national defence secret, he is bound not to disclose it, or to be liable to penalties in the provisions of Article 413-11 of the Criminal Code. In this persepective, all these individuals are duly informed of their duties by their employment authority.

Chapter 6: Access by magistrates to sites holding elements covered by national defence secret

Article. 80: Magistrate and protection of national defence secret

Bringing together the two requirements that represent the search of criminal offenders and protection of national defence secret, the creation of sites having special protection is accompanied by provisions which clearly definethe procedure by which a magistrate may enter into them legally[124]. These provisions, applicable to the sites holding the secrets, are hardly issued due to the non existence of the legal proceedings[125].
With the aim of making these provisions known, the responsible authority for the site or the delegated authority, prepare instructions on how to behave in case of a search, to the intention ofto the personnel of the site. These instructions refer to a directive or a ministerial circular, and aim to facilitate the development of the operation.

Article. 81: Access by a magistrate to sites holding national defence secrets

1) Consultation of the list delimiting sites holding national defence secrets

The list of sites holding elements set by national defence secrets, is established by order of the Prime Minister, but is not published. It specifies, for each site, the concerned organisation, the rooms clearly identified and the establishment of the site where the classified information or materials are stored. The HFDS are required to regularly update the list related to their ministry.

[123] Article 226-13 of Criminal Code.
[124] Article 56-4 of the Code of Criminal Procedure.
[125] Article 56-4 (IV) of the Code of Criminal Procedure.

The list is sent to the Consultative Commission on National Defense Secret (CCSDN) and the Minister of Justice. The latter organises a safe access to this list allowing each magistrate who is considering a search to verify whether the concerned site appear therein [126].

2) Access procedure

A magistrate may, when he considers this action necessary for the proper conduct of the proceedings that he instructs, carry out a search on a specifically identified site holding classified elements, provided he is accompanied by the chairman of the Consultative Commission on National Defense Secret (CCSDN), of a representative member of the Board or a delegate, duly security cleared[127].

The magistrate who intends to proceed with such an operation must first send in writing to the chairman of the CCSDN the information relevant for the fulfilment of his mission. The President (or his delegate) goes to the sites immediately. From the beginning of the search, the magistrate informs the President of the CCSDN, as well as the head of the establishment, his delegate or the officer in charge of the site, of the nature of the offence which is subject to investigations, the reasons justifying the operation, its purpose and the targeted premises.

Only the President of the CCSDN or his representative (member of the commission or delegate), assisted by any cleared person thereto, may, without risk of compromise, examine the classified documents and, in accordance with the subject of the search of the magistrate, sort out the classified elements and select those which can be useful to the court.

The magistrate can only seize, among the classified elements, the documents relating to the offences under investigation. If the necessity of the investigation justifies that the original classified elements are seized, copies are left to their holders.

Each classified document seized is, after inventory by the President of the CCSDN, placed under seal. The seals are handed over to the President of the Commission who becomes their custodian. The minutes of meeting recording transactions carried out and making an inventory of the seized classified documents is prepared but is not attached to the record of the proceedings. It is presented to the President of the Commission.

The declassification of concerned documents is then processed according to the procedure described in Article 69[128].

Article.82: Specific cases

1) Criminal Concealment

The act of concealing[129], in the sites identified as holding national defence secrets, proceedings, objects, documents, information, information networks, data processing or files

[126] Articles 56-4 of the Code of Criminal Procedure and R2311-9-1 of the Defence Code.
[127] Article 56-4 of the Code of Criminal Procedure and R. 2312-1 of the Defence Code.
[128] Articles L2312-4 to L. 2312-8 of the Defence Code.
[129] Article 56-4 al. 4 of the Code of Criminal Procedure.

that are not classified and trying to take undue advantage of the protection enclosed in national defence secret, put at risk its author to sanctions for the offence of obstructing justice[130].

2) Incidental discovery of a classified element

When during a search in a site non identified as holding national defence secrets, one or more classified elements are incidentally discovered, the magistrate, present on the sites or having been immediately notified by the police officer, informs the President of the CCSDN. Classified elements are sealed without their contents being disclosed, by the magistrate or police officer who discovered them, then are handed over or passed on, in accordance with the rules protecting national defence secret, to the President of the CCSDN for safekeeping[131]. The minutes recording the operations relating to these classified elements is not attached to the legal proceedings file but is sent to the president of the CCSDN.

The declassification and communication of elements thus placed under seal are submitted to the standard procedure previously described. The CCSDN sends the seals, with his opinion, to the originating authority.

[130] Article 434-4 of Criminal Code, which provides for and restrains as characterising the criminal obstruction of justice lets it obstruct the manifestation of the truth, particularly by the destruction, removal, concealment or alteration of a public or private document facilitating the discovery of a crime or a misdemeanour, the search of proof or the conviction of the guilty.

[131] Article 56-4 (II) of the Code of Criminal Procedure.

TITLE V:
SECURITY MEASURES RELATED TO INFORMATION SYSTEMS

→ The rules of this directive and the specific implementing instructions issued by the National Information Systems Security Agency (ANSSI - *Agence nationale de la sécurité des systèmes d'information*) are applied to information systems dealing with classified information;
→ SSI *(Information Systems Security)* concerns all the parties having a responsibility in the implementation of these principles and measures: IT services for logical security and the other aspects of computer security, business managers for access rights to information, and those responsible for the physical security of the premises;
→ The functional security chain of information systems, placed under the authority of the HFDS in the ministries, or an equivalent security structure in organizations not covered by a ministerial department, is responsible for specifying, applying to itself, and inspecting the necessary security measures. The latter must have as its objectives availability, confidentiality and integrity, while remaining coherent with the purpose of the information and systems concerned;
→ The accreditation is the formal act by which the responsible authority certifies, after assessing the risks, that the protection of the information and the systems are ensured at the required level.

Article. 83: Scope of application

This title specifies the measures to be applied to protect classified information in computerized information processing systems.

These measures apply to any information system intended to process classified information, whether they are placed under the responsibility of a government ministry (central or decentralized administrative service), an organization-dependant institution, a public or private organization that has a defence or national security contract, or more generally any public or private individual who processes such information.

Directives and technical guidelines supplement as necessary the general measures outlined in this directive.

Chapter 1:
The organization of responsibilities relating to the information systems

Article. 84: Interministerial bodies responsible for the security of information systems

1) The General Secretariat for Defence and National Security (SGDSN)

The SGDSN proposes and implements government policy on the security of information systems[132], especially for systems handling information covered by national defence secret. It ensures that the President of the Republic and the Government have at their disposal the means of electronic communication needed for defence and national security. It is also responsible for ensuring the security of these means of communication. For this purpose, it has at its disposal a nationally competent service, the National Information Systems Security Agency(ANSSI)

2) The National Information Systems Security Agency (ANSSI)

The ANSSI is the national authority for defence and security of information systems[133]. It assists the General Secretary for defence and national security in accomplishing his duties in the field of information systems security.

3) The strategic committee of information systems security

The committee proposes strategic orientations for information systems security to the Prime Minister and monitors their implementation[134].
It is chaired by the General Secretary for Defence and National Security. Its secretariat is provided by the ANSSI.

Article. 85: The ministerial departments

Each minister is responsible for information systems security for the departments and organizations under his charge. He establishes a network of responsibilities, called "functional chain" of information systems security, responsible for enforcing the regulations, implementing measures and monitoring their application.
The organization of this chain of responsibilities, described in this chapter, can be customized to each government department in accordance to its specific constraints.

On the issue of information systems security, and under the responsibility of the minister, the HFDS drives the security policy for information systems and monitors its implementation[135]. He/she ensures the deployment, in his/her ministry more particularly, of the governmental secured means of electronic communication. He/she names an information systems security civil servant (FSSI) to assist him/her in this area.

The HFDS is more specifically responsible for:
- communicating inter-ministerial directives related to information systems security to all concerned personnel and specifying the implementation modalities;
- developing specific directives for his ministry by defining, for each type of computer system, the necessary protective measures;
- supervising the implementation of these directives and the effectiveness of the prescribed measures;

[132] Articles R. 1132 - 3 of the Defence Code.
[133] July 7, 2009 Decree no. 2009-834, article 3.
[134] July 7, 2009 Decree no. 2009-834, article 7.
[135] Article R. 1143-5 of the Defence Code.

- identifying the information systems protection needs and ensure they are met;
- specifying the inspections and checks to verify the effective implementation of directives and guidelines, dealing with information systems security;
- organizing staff awareness and more particularly that of qualified authorities and information systems security personnel, as well as supervising the training of personnel.

Article. 86: Qualified authorities and security agents

1) The qualified authority in information systems security (AQSSI)

Qualified authorities are responsible for information systems security at the level of a service or branch of a ministry or at the level of an organization or a ministry-dependant institution.

The qualified authorities are designated by the Minister for the department and agencies under his charge. Their responsibilities cannot be delegated.

The qualified authority, in association with the HFDS and the FSSI of the government department to which it reports, is particularly responsible for:

- defining an information systems security policy adapted to the service, department, establishment or agency, based on the security objectives that it sets, or, for the systems processing classified information, the security objectives fixed by this directive;
- ensuring that the regulatory provisions and, if required, contractual provisions on information systems security are implemented;
- ensuring implementation of instructions and internal directives;
- ensuring that the internal security verifications are regularly carried out;
- organizing personnel awareness campaigns and training in security issues, particularly regarding information systems ;
- ensuring the implementation of regulatory procedures prescribed for the accreditation of systems, approval of security devices and also for the management of controled information systems security articles(ACSSI)[136];
- designating security accreditation authorities for systems under its responsibility.

In the case of an organization that does not depend on a ministry, namely a private organization, it is the responsibility of the director of the organization to assign, to a person within the organization, the function of qualified authority, as described in this article.

2) The information systems security agent, manager or officer (ASSI, RSSI, OSSI)

The qualified authorities can be assisted by one or more information systems security agents, managers or officers (ASSI, RSSI, OSSI)[137]. They specify the scope of the duties and hierarchical dependence of the latter during their nominations. This scope may be a service, a department or a whole organization, one or more information systems, or a facility.

[136] Article 93 of this directive.
[137] Designated as ASSI in the rest of the directive.

These agents mainly carry out the operational duties of information systems security. They can particularly be responsible for:

- being the privileged point of contact of system users regarding security issues;
- ensuring the training and awareness programs for managers, IT staff and users regarding information systems security;
- maintaining a list of personnel having access to the information systems;
- ensuring the continuous monitoring of the activities of external personnel called in to work on the information systems;
- ensuring the implementation of the prescribed security rules by the operating staff and users;
- ensuring their awareness of security measures and informing them of any modifications in the conditions of utilization of the system;
- ensuring the carrying out of the prescribed protective measures, establishing specific instructions and supervising their implementation ;
- ensuring the management, accounting-for and following-up of the ACSSI in the scope of their responsibilities, and periodically carrying out their inventory;
- establishing security procedures relative to the conservation, storage and destruction of the ACSSI ;
- periodically verifying the installation and operation of security devices;
- ensuring compliance with operational security procedures specific to the information system;
- supervising maintenance operations;
- reporting any irregularities noted or any security incident.

Article. 87: The system security administrator

For each information system dealing with classified information, the authority responsible for the use of the system designates a security administrator to implement the operational security measures. To this end, the administrator is particularly responsible, in relation with the concerned ASSI, for:

- the installation of software security patches and protective software;
- the management of system access and authentication measures;
- the management of user accounts and access rights;
- the taking into account of security alerts and security logs.

The administrator reports any vulnerability in the system that he detects, any security incident and any difficulty in implementing security measures to the ASSI.

The security administrator, whenever it is possible, should not be the system administrator. He must be security cleared to the level of classified information processed by the system and at least at the *Secret Défense* level.

Chapter 2:
The protection of information systems

Article. 88: General principles of information systems protection

The general objective of information system protection is to guarantee the integrity, authenticity, confidentiality and availability of the information processed by the system. The protection of an information system is based on principles pertaining to the organizational and technical resources, complemented by defence in-depth principles. These principles must be strictly adhered to when the system is likely to process classified information.

1) Organization-related principles

These principles include:

- **taking security into account:** information system security must be taken into account in all phases of the system lifecycle under the control of the accreditation authority, particularly during system design and specification studies, throughout its operation and during its decommissioning;
- **information system security policy**: a security policy defining the technical and organizational principles and requirements of the security system must be established and approved by the accreditation authority. This policy is based on a risk management, taking into account threats to the system and information, and the vulnerabilities identified in the system;
- **accreditation of the system**: prior to their commissioning, all systems must be accredited[138] by a designated authority in accordance with Article 90;
- **the organization of the chain of responsibilities**: the persons who have responsibilities regarding information systems security must clearly be identified, security cleared to the required level and informed of threats to the system and to information;
- **system security control during the operational phase**: the implementation of security measures and compliance with the conditions linked to the accreditation are controlled throughout the utilization of the information system, especially by carrying out regular security audits;
- **security incident management**: procedures for detecting and dealing with security incidents likely to affect information system security must be implemented. The incidents encountered and means deployed for resolving them are reported to the accreditation authority. The ANSSI is informed of incidents and their technical characteristics affecting the information systems processing classified information.

2) Principles related to technical resources

These principles include:

- **technical protection of the system**: the information system must be designed so as to protect information being processed and to ensure its integrity and availability. It must also ensure the confidentiality of sensitive information related to its design and security settings;

[138] Article R2311-6-1 of the Defence Code.

- **management of sensitive components of the system**: management of ACSSI and other sensitive components of the information system must be done, and allow traceability throughout their lifecycle, in accordance with Article 91;
- **physical protection of the system**: the means of physical protection of an information system **Annexe**must be applied;
- **management and control of system access**: the information system must be designed and managed so as to allow access[139] only to persons having the required level of security clearance and on a need to know basis;
- **approval of security devices**: security devices approved by the ANSSI in accordance with Article 89 of this chapter must be used[140].

3) Defence in-depth principles

The protection of an information system requires the use of a range of security techniques, so as to reduce risks when a particular security component is compromised or fails. This defence in-depth is divided into five major areas:

- **warn**: avoid the presence or appearance of security vulnerabilities;
- **block**: prevent attacks from reaching system security components;
- **contain**: limit the consequences of a system security component compromise;
- **detect**: to be able to identify incidents and compromises occurring on the information system, so as to be able to react to them;
- **fix**: have the resources to bring the system back into operation and in secure conditions, following an incident or compromise.

Article. 89: Approval of security devices

Security devices are hardware or software resources designed to protect information processed by the system or to protect the system itself. These devices can be designed for general use or specifically for a particular system.

These devices implement different types of security functions and mechanisms, namely:

- encryption functions, encoding the information stored or sent over the networks and ensuring their signature, authentication or cryptographic key management;
- functions controlling access to information, such as authentication, filtering, logical partitioning between the security levels or the marking of information;
- functions or mechanisms meant to protect the device itself, such as logging and tracking of access to the device, or prevention or detection of unauthorized physical or logical intrusions, furthermore guaranteeing the protection of sensitive data stored or their erasure if need be, and more generally any function or mechanism meant to guarantee the integrity and availability of the device;
- functions securing administration and management of the device;
- functions protecting the transmission of radio signals, particularly against interferences;
- functions or mechanisms limiting emissions of compromising signals.

[139] Article R2311-7-1 of the Defence Code.
[140] Article R2311-6-1 of the Defence Code.

A security device installed in an information system that processes classified information must be approved by ANSSI when it is used as a complement to organizational security measures, as an essential means of protection against unauthorized access to classified information or to the system.

Exceptionally, depending on the risk analysis which is made and on the specific conditions of use, the accreditation authority may decide not to employ an approved device. This decision must be specifically justified from the viewpoint of consequential risks and argued in the system accreditation decision.

The approval is usually requested by the authority responsible for the design of the security device, or failing that by the authority responsible for using the system. It is issued following a security assessment of the device, performed by one or more laboratories approved by the ANSSI. This evaluation aims to verify the consistency of the security objectives, as identified in the security target, in view of threats, and assess the effectiveness of functions and security mechanisms. Based on the results of the evaluation, the ANSSI may issue an approval that attests the ability of the device to protect classified information at a specific level, under the identified conditions of use. At the end of its validity period, the approval must be subject to renewal which may require re-evaluating the device. Due to an evolution of the threats or the discovery of new vulnerabilities, an approval may be withdrawn before expiry.

To ensure the smooth running of the approval or renewal process, the requesting authority needs to set up an approval commission which comprises, in addition to the authority itself, the ANSSI, the concerned assessment laboratories and, where appropriate, the authority using the system.

Article. 90: Security accreditation

1) The accreditation process

It is necessary to implement a process, called “accreditation”, to identify, achieve and maintain an acceptable level of security risk to the considered information system, given the required need for protection. This process is based on a comprehensive security risk management of the entire information system throughout its life cycle.

The security accreditation of a system is exhaustive in that it includes within its scope anything that can have an impact on system security, be it technical or organizational. In particular, utmost attention of must be brought to:

- interconnections with other systems;
- removable media;
- remote access by “nomad” users;
- maintenance, utilization and remote management operations on the system, particularly when they are carried out by external service providers.

Any information system processing classified information must be subject to accreditation, consisting in obtaining from an accreditation authority a statement claiming that the

considered information system is capable of processing classified information at the classification level considered in accordance to the security objectives pursued, and that this authority accepts the residual security risks. When the system uses security devices approved by ANSSI, the accreditation authority must take into account the conditions attached to these approvals.

2) accreditation authority and commission

The accreditation is given by an authority appointed in the following conditions:

- in cases where the information system processes *Très Secret Défense* classified information, the SGDSN is the accreditation authority;
- in cases where the information system belongs to an administration, service, organization or facility under the responsibility of a ministry, the concerned qualified authority names the accreditation authority;
- in cases where the information system is under the responsibility of several ministries, a single accreditation authority is named by the concerned ministries;
- in other cases, particularly when the information system belongs to a private organization, the designation of the accreditation authority is the responsibility of the organizations concerned by the information system.

The accreditation authority must be chosen at a hierarchical level sufficient to endorse the responsibility relating to the accreditation decision, and in particular to accept the residual risks. It is in principle the authority responsible for the system utilization. It can also be the qualified authority.

The accreditation authority puts in place an accreditation commission meant to assist and prepare the accreditation decision. Such a commission includes representatives of the users of the system, and system operation and security responsible parties. Being the National information system security authority, the ANSSI may be a part of any accreditation commission. It is a de facto member when the SGDSN is the accreditation authority.

3) The accreditation decision

The accreditation decision is taken after examination of the accreditation file. This namely includes:

- a risk analysis;
- the system security policy;
- the security operation procedures;
- the management of residual risks;
- the results of tests and audits conducted in order to verify the compliance of the system to the security policy and operational procedures;
- if required, the approval of the security devices.

The decision of accreditation must occur before system commissioning. However, in exceptional cases, when operational emergency requires it, a provisional commissioning can be done, without waiting for the accreditation of the system, taking into account the progress

of the accreditation procedure and the residual security risks. In this case, the final commissioning will occur subsequently, when the security accreditation has been obtained.

The accreditation decision is obtained for a maximum duration of:

- five years for a *Confidentiel Défense* level information system*;*
- two years for a *Secret Défense* or *Très Secret Défense* level information system.

The ANSSI is the recipient of all accreditation decisions on information systems processing classified information. It may request the corresponding accreditation files.

4) The verification and renewal of accreditation

The accreditation authority determines the conditions of maintaining the security accreditation during the information system lifecycle. It regularly verifies that the system indeed operates under the approved conditions, especially after maintenance in operational phases.

The accreditation authority reviews the need for accreditation renewal before the scheduled completion, particularly when:

- the conditions of use of the system have been modified;
- new functionalities or applications have been installed;
- the system has been interconnected with new systems;
- problems in applying the security measures or accreditation maintenance conditions have been reported, for example during a security audit;
- system risks have evolved;
- new vulnerabilities have been discovered;
- the system has experienced a security incident.

Article. 91: controled information systems security articles (ACSSI)

Some resources, such as security devices or their components, and some information relative to these resources (algorithm specifications, design documents, encryption keys, evaluation reports, etc.) may require the implementation of specific management to ensure their traceability throughout their life cycle. These resources and information, whether classified or not, need to be accessible at any time and especially in cases of suspected or actual compromise.

These resources and information are called "controled information systems security articles" (ACSSI). They carry a specific mark identifying them, in addition to their classification, wherever applicable.

The decision to classify a resource or information as ACSSI is taken by the ANSSI on the basis of an opinion given by the approval commission of the concerned security device. In the case where the security device is not subject to approval, the accreditation authority of an information system using such security device may decide, after consultation of the

accreditation commission, to classify as ACSSI this device or its components or the related information.

The ACSSI management principles have the following objectives:

- to train, raise awareness and give responsibility to the holders of such resources and information;
- to ensure these resources and information are accounted for, and ensuring the inventory at a central or local level, so as to be accessed at any moment if required;
- to manage their distribution;
- to periodically check their localization and status;
- to inform the functional chain of any suspected or actual compromise after such events as loss, theft, or disappearance, even if they are temporary;
- to ensure their destruction.

Article. 92: Specific information systems

1) Processing of "*Spécial France*" information

Information systems capable of processing information marked "*Spécial France*"[141] must also be subject to specific security measures to ensure that foreign users who have a legitimate need to access the system do not have access to any information which is authorised only to French users.

2) International exchanges

When classified information is transmitted through the information systems under the responsibility of foreign states or international organizations, protective measures must be determined by agreement or by security regulations with these partners, which guarantee to this information a level of protection at least equivalent to that provided in this directive.

The protection of information systems processing classified information which are entrusted to France by foreign states or international organizations is ensured in accordance with agreements and security regulations established with these partners. If required, these agreements and regulations are subject to additional directives for applying these measures in France. In the absence of such agreements or regulations, the provisions of this directive apply to these systems.

[141] In accordance with article R 2311-4 of the Defence Code.

TITLE VI:
THE PROTECTION OF SECRET IN CONTRACTS

→ in the same manner as physical individuals, private legal entities must be granted security clearance for the execution of classified works;
→ The storage by a contractor of classified information or materials is conditioned by the physical aptitude of premises to receive the classified information or materials.

Article. 93: General security principles

The security of classified information or materials in contracts, interpreted as per Article 2 of the present directive, is guaranteed by the inclusion of provisions meeting these present requirements and defining the duties of contractors. Any sub-contracting[142] contract of a deal requiring access to classified information or materials abides by the rules of the present directive, including in the pre-contractual phase.

Any contract that involves access to classified information or materials includes clauses on protection of the secret specifying the duties of contractors as defined in **Annex 9**. The holder of such a contract undertakes, under contractual and criminal liability, to ensure the protection of classified information or materials that he will have to handle or to know under this contract by taking into account the special provisions stipulated in a security aspects letter in relation to the contract.

The physical aptitude to hold classified information or materials is conditioned by compliance with laws and regulations on protection of national defence secret. The contract holder whose purpose involves the storage of classified information or materials is required to implement in his establishment or establishments the security measures required for ensuring protection of national defence secret pursuant to Article 71. With respect to any person he employs, whom he receives or with whom he is associated, the contract holder shall take all appropriate measures to control, failing which, restrict access to parts of its facilities in which protection of classified information or materials warrants it.

[142] For purposes of Act no. 75-1334 of December 31, 1975 relative to subcontracting.

Chapter 1:
Security measures in the negotiation and award of contracts

Section 1: Pre-contractual phase

Article 94: Duties of the contracting authority

From the beginning of a procedure for the award of a contract or whether there has been a public call for tender to the competition, the contracting authority has to inform prospective candidates of the deadline to provide documentation necessary for the security clearance and, if the contract requires the storage of classified information or materials, the documents needed to carry out the assessment of physical aptitude of the company to store classified information or materials. This time period cannot be less than fifteen days from the date of the notification issued by the contracting authority. For this purpose, the contracting authority communicates all the necessary notices or procedures on how to obtain them and, where appropriate, the competent service for processing the file.

Candidates for contracts requiring storage of classified information or materials are informed of the physical standards to be met and duties generated by the storage of classified information or materials and the fact that the start of classified work is suspended when the aptitude is evaluated, which can, if necessary, intervene after the notification of the contract.

When the file is incomplete, the contracting authority informs the bidders of the missing documents that should be provided before the deadline expiry.

The contracting authority informs the security clearance authority of selected applicants and transmits to it the security aspects letter project. The security clearance authority transmits the security clearance request file to the investigating service upon receipt of this information.

Article. 95: Duties of the bidder

Any candidate, physical individual or legal entity, to a contract, whatever be his nationality, the form or legal status of the company, must hold a security clearance under the conditions defined in this present title. For this purpose, as part of his application, the physical person or legal entity bidder must submit an application for security clearance or a valid security certificate as evidence of his security clearance. Subject to the provisions of Article 97 of the present directive, this security clearance file should comply with **Annex 11**.

In support of his application for a contract whose execution involves the storage of classified information or materials, the company, regardless of nationality, must, in addition, agree to submit an aptitude file for each place situated on the French territory where it is projecting to carry out classified works. This file is meant to evaluate the ability of those places to ensure the protection of elements covered by national defence secret.

If the file(s) mentioned in paragraphs 1 and 2 of the present Article has or have not been provided or completed within the deadline, the bidder is deemed to have waived the request of security clearance to classified information and materials for the contract in issue.

Article. 96: Communication of classified information in pre-contractual phase

Since taking cognizance of classified information is necessary in the pre-contractual phase, and particularly for the development and submission of the bid, the personnel security clearance of individuals is possible without the company who employs them itself being security cleared, provided that the clearance procedure concerning it has been started. For this purpose, the bidder must select among his personnel, at the latest when his application has been selected as a bid, one or several individuals who will access the classified information or materials on a strict need to know basis for the development of the bid.

If the selected individuals pursuant to this present section do not have security clearance or if the security clearance decision concerning them is not appropriate to the needs of the contract, the bidder related to them simultaneously deposits a request for security clearance for each of them. This request is heard and is subjected to a provisional security clearance decision or a refusal decision issued under the conditions and time limits specified in Title II (chapter 2) of the present directive. The provisional security clearances granted pursuant to the procedure defined in the present section shall not prejudice the security clearance of the legal entity to execute the said contract.

The contracting authority defines the list of individuals authorised to have access to classified information and materials as part of the development of the bid and fixes the places and modus operandi of the elements covered by national defence secret. These sites must provide the protection guarantees inherent in the level of classified information processed as defined in Article 71.

Unsuccessful applicants storing classified information and materials are required to return them to the sender upon notification of the rejection of their bid and according to the modalities defined by the contracting authority.

Article. 97: Case of foreign companies

Every company registered under foreign laws applying for a contract is obliged, in support to its application, to produce a certificate justifying its security clearance or the procedure in progress undertaken to this purpose. This certificate is issued by a security clearance authority of the State it belongs to when this State has concluded a bilateral or multilateral security agreement covering exchange of classified information or materials with France.

The security clearance authority may approach the General Secretariat for Defence and National Security, as National Security Authority, or the Designated Security Authority mentioned in the security agreement for the purpose of requesting the National Security Authority of the State of the nationality of the applicant firm to conduct the appropriate clearance of this company.

No applying company registered under foreign laws can be accepted when the execution of the contract entered into, under this title, implies the storage or exchange of classified information or materials marked "*Special France*".[143]

Article. 98: The case of French companies bidding in an international framework

French companies bidding for a contract requiring access to classified information outside the country and for which security clearance is required, must address, if they do not already hold security clearance, their security clearance file either to the General Secretariat for Defence and National Security as the National Security Authority, or to the Designated Security Authority specified in the security agreement applicable between France and the countries on whose behalf they are bidding. A company already cleared addresses to its security clearance authority for a possible extension of the field of security clearance. The security clearance authority shall, if necessary, transmit the elements to the national security authority for the issuance of an appropriate certificate of security clearance.

Section 2: The security clearance procedure

Article.99 : Prior investigation

To evaluate if a company does not present vulnerabilities for defence and national security, investigations led by the investigating service focus particularly on the real holders of the management and control power as well as on the shareholder(s). The national security authority of the State of the nationality of the officers or shareholders may be consulted. The direction taken by the vulnerability investigation does not affect in any way the reputation of the concerned company or that of its managers.

At the completion of investigations, the investigating service issues a security notice that is communicated only to the security clearance authority. The conclusions of the security notice are of three types:

- "no objection notice", when the instruction has not revealed any element of vulnerability constituting a risk for the security of classified information or materials nor for that of the legal entity;
- "restricted notice", when the legal entity presents certain vulnerabilities including direct or indirect risks for the security of classified information or materials to which it would have access, but that the specific security measures taken by the security officer would allow to control;
- "unfavourable notice", where specific information shows that the legal entity presents vulnerabilities which put on the secret such risks that no security measure seems sufficient to neutralise.

The security notice is issued for a given level of security clearance. The "no objection" notice is valid for the specified level as well as for lower levels. For restrictive or unfavourable notices, the investigating services give their opinion on a case by case basis, on the opportunity to grant security clearance for lower level[s].

[143] In accordance with the provisions of article 65 of this directive.

The restrictive or unfavourable notices are not classified. They are accompanied by a confidential file indicating the reasons for the notice. This file, which is classified fully or in part, clarify the elements of vulnerability detected in the course of the investigations. These elements can only be brought to the knowledge of the clearance authority. Since it cannot be copied, the confidential file is returned after communication and without delay to the investigating service which despatched it, for storage purposes.

However, to allow recognition of security clearances between clearance authorities, the security notice as well as any elements relating to the security clearance of the concerned legal entity may be transferred between the security clearance authorities. Unless there is change in the situation of fact or law of the company, the duration of validity of the security notice issued is fixed in accordance with the provisions of Article 24.

Article.100: The facility security clearance

The security clearance of the contractor is an explicit decision which is issued by the security clearance authority on the basis of the security notice issued by investigating services designated in Article 24.

The security clearance authority takes its decision in the light of the security notice issued before the date of the contract award, without being bound by that notice. In a justified emergency and after referral by the investigating service, the security clearance authority takes as a last resort, if it deems it necessary, its decision in light of other useful elements in its possession.

The decision of refusing to grant security clearance is notified to the representative of the legal entity under the conditions defined in Article 26. A refusal decision does not prejudge the conclusion of contracts of any kind not involving the implementation of measures for the protection of national defence secret.

The security clearance decisions issued on the occasion of award of a contract requiring the knowledge of classified information or its storage have a time limit of validity fixed by the security clearance authority and, if possible, a validity domain. The validity duration of the security clearance decision may be distinct from that of the security notice without being greater.

Article.101: Validity period of the facility security clearances

The security clearance granted to a company by a ministry during a contract requiring access to or storage of classified information or materials remains valid for any other consultation with a contracting authority within the same ministry, at the time of another contract, within the time limits and the validity domain of this security clearance and unless the situation changes in fact or in law of the company in question.

The security clearance in the course of validity previously issued by another ministerial department, for which a certificate may be established, is extended again to the new contract unless there is a change in law or fact of the bidder. The security clearance authority, if

necessary after reviewing the files sent at its request by the authority having previously cleared the bidder, may take a security clearance decision related to the domain ofthe new contract if the previous security clearance has been limited to a particular domain.

If the security clearance decision expires during the execution of a contract governed by these provisions, an application for renewal must be filed with the security clearance authority, within six months and no later than one month before the expiry date. The validity of the decision is then extended under the conditions defined in Article 31.

Any change affecting the holder, legal entity or individual, of a security clearance,occurring after the decision, must be reported to the security clearance authority to enable it to reconsider its decision.

Article.102: Confidentiality of the facility security clearance

The legal entity having been granted a security clearance decision cannot publicly disclose details of the decision or rely on, or disclose information to third parties referring to classified work unless specific authorisation fromthe referring contracting authority.

Article.103: Personnel security clearances

The sole persons authorised to know classified information or materials on behalf of a security cleared company are the individuals belonging to this company who have been subject to a prior security clearance decision issued in accordance with the conditions of Article 24. Unless otherwise stipulated, this security clearance level may not exceed that of the security clearance of the company.

The approval as defined in Article 33 may be used for timely access to classified information at a higher level than the one of the facility security clearance.

The employment contracts of public or private persons mentioned in the first line includes a confidentiality clause for the protection of the secret in accordance with the standard article contained in **Annex 9 (4)**. In case of change in assignments leading the employee to work under the conditions defined in the first line, the employment contract is subject to a written agreement in accordance with these provisions. The parties to the employment contract may complete or adapt the standard article according to the specifications of the said contract without going against it.

Section 3: Contracting phase

Article.104: Conditions for Contract signing

The contracting authority may not sign any contract requiring knowledge of classified information before receiving the facility or personnel security clearance certificate from the selected applicant, made, except in the case of an emergency procedure, on the basis of the security notice of the investigating service.

When the contract requires storage of classified information, the final confirmation of the aptitude, on the basis of the file established in accordance with the prescriptions of the annex 13, shall have been sent to the contracting authority before the classified work begins but can be communicated to the company after notification of the contract. In this case, and according to the timetable established in connection with the investigating service and the contracting authority, the start date of the contract is specified at the time of notification under the following conditions:

1) An initial test of aptitude on measures taken by the security cleared company for ensuring the security of classified information or materials is made by the investigating service in the concerned establishments, prior to any start of classified work. At the end of this control, the technical notice issued by the investigating service is sent to the contracting authority and notified to the contractor. Upon receipt of this notice, and without reservation, the manager of the company issues a certificate[144] certifying compliance with standards of premises or facilities concerned.

2) If the technical notice reports deficiencies in the security system implemented within the company, the holder is required to undertake to implement all measures necessary for compliance of the facility within a period defined in connection with the investigating service and contracting authority and consistent with the start date of the classified works.

3) At the end of compliance work and not later than the date of expiry of the period stipulated in the notification, the aptitude certificate mentioned in paragraph 1 of this article[145] is sent by the manager of the company to the contracting authority who informs the investigating service of it and may seek to initiate a control.

4) If the certificate is not received within the pre-defined deadline or if deficiencies are found during controls by the investigating service, a formal notice to comply with the requirements of Article 71 is made. The failure to execute work involves the responsibility of the holder.

If the holder has a premise suitable for processing classified information or materials that has been subject to an aptitude notice in the context of a previous contract, he shall inform the concerned contracting authority of this notice as well as the certificate of no change in the conditions that led to the issuance of the aptitude notice[146].

Chapter 2:-
Security measures relating to the execution of contracts

[144] Annex 12, model A.
[145] Annex 12, model B.
[146] Annex 12, model A.

Section 1: Security structure

Article.105: The in-charge of the security policy of the company

Under his personal contractual and criminal liability and that of the legal entity, the company's head who is the contract holder is required to implement regulatory requirements for the security of classified information or materials. As such, a security policy to ensure implementation of the protection of classified information or materials within the company, failing which, in its various branches must be established. For the development and implementation of the security policy, the representative of the legal entity appoints one or more individuals as security officer. The individuals thus selected must have sufficient seniority in the company and have all the means necessary to fulfil the missions assigned to them. To this end, they are attached in the exercise of their security mission to the company head and act on their behalf and under the latter’s authority.

The security officer shall be subject to approval by the security clearance authority. To be approved, the security officer must have prior security clearance. This approval may be granted for a probationary period of maximum twelve months. At the end of this probationary period, unless explicitly decided otherwise, the approval is deemed confirmed. The approval may be withdrawn at any time by the security clearance authority, especially when its holder ceases to have security clearance. In this case, the head of the company holding the concerned contract shall propose a new holder under the same conditions and with the least possible time.

As per the needs of protection of the secret in each establishment of the company, the company head possessing a contract involving the storage of classified elements may designate one or more deputies to the security officer who is then known as Central Officer of the Company. His deputies are called Establishment Security Officers.

Since information systems hold and process classified information, the company head must also appoint a security officer assigned to the security of information systems to strengthen the security structure. This function can be exercised by the security officer or under his authority.

The provisions of this present section are applicable to any deputy of a security officer.

The company head may, where appropriate, designate security correspondents in physical or operational divisions of the company to consolidate the activities of the security officer within these subdivisions. Placed, for this mission, under the operational control of a security officer, these security correspondents are not subject to the approval required above.

Article. 106: Role and duties of the security officer

Under the authority of the company head, the security officer is responsible for the general security organisation of the establishment, especially relationships, as part of its function,

with the investigating service, the security clearance authorities and the contracting authorities.

1) In this, he will in particular ensure:

- the application of the security rules stated in different texts within the establishment;
- the management of security clearance files of the establishment personnel on a need to know basis; he is also responsible for the security clearance requests of possible subcontractors. He is responsible for informing the investigating service of the vulnerabilities appearing of which he is made aware after the security clearance decision, and informing to the security clearance authority any change in the status of the legal entity;
- the updating of a register of members of personnel holding security clearance and to whom access is authorised, within the framework of the contract and subsequent sub-contracts. This register gives the issue and end of validity dates as well as the level of these security clearances;
- providing, at the request of the investigating service, information on all the persons who have been called to have access to classified information;
- increase awareness among and training of personnel;
- indicating actual or suspected compromises of the secret, in the conditions defined in Article 67;
- the management and updating of the security aspects letters of contracts of public or private law;
- updating of the security file.

2) within the framework of the contracts involving the storage of classified information or materials, he is moreover responsible for:

- permanent supervision of the management and protection of classified information or materials;
- management and follow-up of ACSSI;
- management of authorisation requests for the access to areas with restricted access and management of basic security screening for access by external personnel to the establishment;
- application of international rules for foreign nationals' visits to the establishment under his charge;
- application of international rules for visits abroad for his establishment's personnel;
- sensitisation to the security provisions to be complied with in the establishment by different participants;
- compliance with the regulatory provisions of access, handling, conservation, copy, and destruction of classified information.

Section 2: Security aspects letter

Article.107: Content of the security aspects letter

Every contract contains a security aspects letter that lists the security instructions related to the contract. When its content justifies it, it can be classified in whole or in part. It may be

modified during execution of the contract at the behest of the contracting authority or on a proposal by the contract holder.

The contracting authority approves the security aspects letter of the contract and the security aspects letters of any possible sub-contracts. The follow-up of the security aspects letters of the sub- contracts is carried out by the primary contractor under his responsibility and under the control of the referenced contracting authority. The modalities of this control can be defined in specific terms or in the security aspects letter of the principal contract.

The security aspects letter covers the requirements listed in **Annex 13**. These can be adapted by the contracting authority in liaison with the holder without going against it.

Article. 108: Case of sub-contracting

Any contract requiring the storage of classified information or materials, giving rise to at least one sub-contract itself requiring access to classified information or materials, must include in its security aspects letter the list of concerned subcontractors, the works they have carried out, and their expected dates of start and end of execution as well as classified information and materials whose knowledge is necessary for their execution. The modification of the security aspects letter may be done subsequently, subject to the agreement of the referred contracting authority.

Section 3: Follow-up of the execution

Article. 109: Duties of the holder

During the execution of the contract, the holder is required to implement the security measures required to protect classified information. In particular, for the purpose of storage of classified information or materials, he controls the access to his installations and has to submit to periodic aptitude checks throughout the contractual period. He has to inform the security clearance authority and the investigating service of any change of fact or law in the situation of the company or personnel involved in the execution of the contract.

Article.110: Specific duties of primary contractors

The primary contractors must guarantee, in addition, the application by their subcontractors of security conditions no less stringent than those provided in the contract. The primary contractors must request authorisation from the referred contracting authority for communicating classified information to subcontractors. Under the modalities agreed by the parties, this authorisation may cover all or part of the classified information, on a need to know basis, in accordance with the extent of services defined by the sub-contract.

The classified information or materials relating to the contract cannot be communicated to the sub-contractor before such sub-contractors, as well as their employees who have a need–to-know, have been subject to a security clearance decision. The possible storage of classified

information and materials by sub-contractors can only be done under contracts with security aspects letter approved by the referred contracting authority.

Article.111: Security and aptitude checks

Aptitude checks and inspections may be expedited periodically in the company premises, pursuant to Article 8, to verify the application of this directive during the execution of each contract.

Under the authority of the company head, the premises of the holding company shall be refurbished in compliance with regulations in force when they no longer present sufficient guarantees for the security of classified information or materials. During the refurbishment works of these premises, the company takes all measures to ensure the security of classified information or materials. After each compliance, a check giving rise to a new aptitude notice of concerned premises may be made by the investigating service as per the procedure specified in article 104. Any refusal of compliance or delay to comply may be considered a breach of contractual commitments for protection of the secret and lead to the imposition of sanctions mentioned under the contract, without prejudice to any possible criminal penalties.

Article.112: Specific measures at the term of the contract

When classified work is completed, the contractor holder must inform within one month time, the contracting authority, which specifies the destination to give to the classified information or materials he had in his possession till now. The security aspects letter mentioned is closed. To this end, modalities for archiving classified information or materials are defined by the referred contracting authority in conjunction with the concerned services.

The security aspects letter of a contract that has generated one or more sub-contracts can only be closed after the closure of all the subcontracting security aspects letters.

When, after the closure of a security aspects letter, the company still stores classified information or materials, it should be subject to a valid security clearance decision and a follow-up by an investigating service, even though this company would not be a holder of any other contract giving access to elements covered by national defence secret.

GLOSSARY

Accountability: ability to identify the initiator of an action.
Alert procedure: step initiated by the security clearance authority of the person to be security cleared in order to make him aware of his vulnerabilities discovered during the administrative inquiry.
Approval: decision taken at the issue of a standard security clearance procedure to the advantage of a person who occasionally has to be aware of classified information or materials at the *Tres Sécret Défence* level of different special classifications, *Sécret Défence* level or *Confidentiel Défense* level.
***Approval of a security product*:** formal recognition that the evaluated security product can protect information to the level as specified in the defined employment conditions.
Aptitude: capacity of a company to process or store classified information or materials. This capacity, evaluated by an investigating service, is based on the control of all physical security measures implemented by the holder of the contract for one or several establishments and including, if necessary, the security of information systems.
Archiving: operation consisting of depositing to an archiving service, information materials, which are of no usual use. The materials which still needs to be classified cannot be archived, except, on certain conditions and in services security cleared to receive them. A classified materials at level *Très Secret Défense* cannot in any case be archived.
Authenticity*:* characteristic of an information or its processing which guarantees his identity, source and eventually its purpose.
Authority qualified in relations to information system security: responsible for the security of information systems in the central administration and decentralised services of the State, in the public service placed under the authority of a minister as well as in the organisations and facilities under his charge.
***Availability*:** characteristic of an information or a process to be usable on request by a person or by a system.
Awareness: instruction frequently given to persons who hold a security clearance or liable to be security cleared and meant to make them realize the protection of national defence secret stakes, legal and administrative sanctions encountered and the necessity of applying the prescribed security measures.
Basic security screening: simplified administrative inquiry, meant to ensure the integrity of a person and solicited by the security clearance authority, the contracting authority or the person responsible for a site in order to authorise his access to a facility or to ensure, during transport, the safeguarding of classified information or materials.
Bidder: any legal entity applying to a contract. In the case specifically identified in this instruction, the bidder can be an individual.
Classified information or materials: procedure, object, document, information, information network, computer data or file presenting a character of national defence secret (art.413-9 of the Criminal Code).
Classified materials: object, equipment, facility, system or substance presenting a character of national defence secret and which requires appropriate protection at Très *Secret Défense*, *Secret Défense* or *Confidentiel Défense level.*
Classified work: services, whatever the type, requiring access to classified information or materials.
Commitment of responsibility: document in two sections signed by the holder of a security clearance during the taking up and termination of his functions. The commitment has the aim of reminding this person the criminal responsibility he runs due to his security clearance. The signature of the central inset of the commitment of responsibility by the concerned person means that he has has been aquainted with the decision.
Compromise: take cognizance, certain or possible, to a classified information or materials by one or more unqualified persons.
Confidentiality: restricted natureof an information or process to which access is limited only to persons admitted to be acquainted for requirements of service, or to authorised entities or processes.
Contracting authority: any public or private person, including in cases of contracts with sub-contractors, and who has applied to a supplier or a service provider for the execution of a contract or a deal. When the deal is governed by the provisions of the public markets code, the term “contracting authority” designates the power

adjudicator. When a deal governed by the provisions of the public markets code leads to subcontracting contracts, the power adjudicator at its source is called “contracting authority of reference”.

Courier security decision: authorisation given, not for getting knowledge of classified information or materials, but for ensuring, during the transport, the guarding of classified information or materials. For this reason, this decision is delivered, not at the end of the security clearance procedure, but after a basic security screening carried out by the investigating services of the Ministries of Defence and Interior.

Data*:* any representation of information in a conventional form meant to facilitate its processing.

Declassification: deletion of the classification of classified information or materials at any level whatsoever.

Defence security civil servant (FSD): person assisting the HFDS and controlling under him particularly the execution of the measures of protection of classified information or materials.

Designated Security Authority (DSA): authority responsible before the National Security Authority (NSA) and responsible for informing the companies of the national policy in a specific domain, particularly industrial, as well as to give directions and provide help for applying it.

Downgrading: modification, by lowering,the classification level of classified information or materials.

Emergency plan: document set by an organisation holding classified information or materials, foreseeing, in case of exceptional circumstances, the evacuation or destruction arrangements of the information materials.

Facility security clearance (FSC): decision given at the end of a procedure allowing the evaluation of the guarantees offered by the private legal entity and of the interest shown by its managers to the protection of national defence secret and to the aspects linked to the security of classified information or materials.

Foreign company: any bidder to a contract whose headquarters is not located in France.

Holder: any person assigned to a contract. When the contract is a public deal with sub-contracting, the holder of this deal is called “primary contractor”.

Identification: note figuring on an information aid and specifying the number of the sample as well as its record number.

Information: any knowledge or element of knowledge susceptible to be represented in a form adapted to a communication, record or process.

Information system: set of IT methods having the aim of developing, processing, storing, routing, presenting or destructing information.

Information system security agent: person responsible for the management and follow-up of security measures of information system found on the site or sites where he assumes responsibilities, particularly in the management and follow-up of items requiring individual accounting.

Information systems security civil servant (FSSI)*:* person charged with bearing the interministerial regulation to the knowledge of organisations and enterprises, developing the regulation of his ministry by defining for each type of information system the necessary protection measures and controlling in his own department the application of this regulation and the efficiency of the recommended measures.

Integrity: property ensuring that an information or a process has not been modified or destructed in an unauthorised way.

Investigating service: State service responsible for investigating the persons prior to a personnel security clearance decision or in the framework of a basic security screening, of evaluating the aptitude of premises and checking the security measures. These services give their conclusions in the form of a security notice.

Jobs catalogue: in an organisation, list of jobs that can require access to classified information or materials. The catalogue is made on the single criteria of the need-to-know.

Marking: operation consisting of affixing on a classified material the marks specifying its level of classification, copy number, record number,page number for a paper document and if required, the exclusively national recipient.

Material: any material means, whatsoever be its form and physical characteristics, allowing receiving, conserving or restoring the information or data.

National Security Authority (NSA): government organisation in charge of relations with other States and international structures in the field of personnel security clearances and protection of classified information or materials. In France, the National Security Authority is the General Secretariat for defence and national security.

Need to know: absolute necessity to take cognizance of an information within the limits of a determined function, for the proper execution of a specific assignment.

Non-repudiation: impossibility of negating the participation in the processing of information.
Person responsible for classification: authority originating information and attributing them, in accordance with their content, an appropriate classification level.
Person in charge of the company: person representing a legal entity for a contract and has the power to commit thereof.
Personal notice: notice meant to receive information required for a personnel security clearance. It must be filled by the concerned person himself and constitutes a major element of the personnel security clearance file. It is used by the authority responsible for giving the decision and by the investigating services.
Personnel security clearance decision: administrative act authorising, at the end of the security clearance process, the holder, in accordance with his need to know, to have access to classified information or materials at a given level. The person granted clearance is informed of the granting thereof but is never given the decision to grant clearance.
Personnel security clearance file: file constituted in view of a personnel security clearance. It includes the personnel security clearance request established by the applicant authority and attesting the need to know, the individual notice filled in by the concerned person and a recent identity photograph.
Primary contractor: is thus named the contractor that, in the framework of a public deal, has concluded the contract with the public entity, contract owner, and who entrusts, under his responsibility, all or part of the execution of this contract to one or more subcontractors.
Protected area: area created by order of the concerned ministers and subject to a prohibition of access without authorisation, criminally liable in case of infraction (articles 413-7 and R. 413-1 to R. 413-5 of the Criminal Code).
Provisional security clearance decision: an exceptional and temporary decision taken in view of a provisional security notice and allowing a person to have access to classified information or materials. This clearance terminates upon delivery of the final decision and not later than six months after being granted.
Qualified person: Qualified, under article 413-10 of the Criminal Code, is the person who, by his status, profession, funtion, or mission, temporary or permanent, is authorised to have access to classified information and has the need to know it

Refusal of personnel security clearance: decision taken by the employment authority, in view of the security notice or any other element received concerning a person, to deny a security clearance to this person. Its motivation is governed by law n° 79-587 of July 11, 1979 on the motivation of administrative acts.

Renewal of personal security clearance: procedure triggered at the end of validity of a security notice concerning a person already security cleared to obtain an updated notice. This new notice will allow giving a personnel security clearance decision in favour of the person who still presents the need to know.
Restricted area: premises or place which is subject to specific material protection measures and whose access is regulated and subordinated to special conditions.
Secret protection office: office located in a restricted area and whose existence is mandatory for proceeding with the development, marking, storage, routing, recording, follow-up and destruction of *Secret Défense* classified information or materials.
Security accreditation: declaration by the accreditation authority, in view of the accreditation file, that the information system considered is apt to process the information at a given classification level in accordance with the targeted security objectives, and that residual security risks are accepted and controlled. The security accreditation remains valid while the information system (SI) operates under conditions approved by the accreditation authority.
Security administrator: person responsible for the implementation of maintenance, supervision, and development of security measures to be applied to any information system containing classified information or materials at the *Secret Défence* or *Confidentiel Défence* levels.
Security agreement: intergovernmental agreement entered into by at least two States or within a multinational alliance and aiming at the protection of classified information and materials. These agreements consist of mutual identification and recognition of national security authorities, the correspondence of the classification levels, mutual recognition of personnel security clearances, methods of transmission and protection of classified information and materials.

***Security certificate**:* document attesting that a person has been duly security cleared for the processing of classified information or materials at a specified level.
Security clearance authority: competent authority for soliciting a security clearance investigation or a basic security screening and issue the decision.
Security clearance procedure: procedure aimed at ensuring that a person can, without risk for national defence or its own security, know of classified information or materials in the exercise of his functions.
Security network: set of manual, material and organisational means which allow the secure routing of information or materials classified at a determined level (and below it) between a group of security cleared correspondents.
Security notice: outcomes issued by an investigating service at the issue of investigations related to a person and aimed at detecting and evaluating the vulnerabilities of this person. The security notice is an aid to the personnel security clearance decision, but it does not link the authority responsible for the decision.
Security officer: named by the Head of the employer service, he is the HFDS and the investigating service correspondent. He has the assignment, under the orders of his employment authority and in accordance with the arrangements of each structure, of fixing the security rules and instructions to be implemented concerning the persons and classified information or materials, and monitoring their application. He participates in the instruction and awareness campaign of the personnel in matter of the protection of the secret. He is responsible for the management of personnel security clearances and, in conjunction with the investigating services, for the monitoring of access to protected areas. He manages the secret protection office.
His missions are to be distinguished from those given to the security officer in a company holding a contract, who is designated by the company head after approval of the contracting authority.
Senior defence and security civil servant (HFDS): person in charge of assisting the minister in exercising his attributions in matters of defence security and protection of secret. He is, in certain ministries, called the corresponding senior security and defence civil servant (HFCDS) or senior defence civil servant (HFD).
Sites holding classified elements: premises in which are held classified information or materials, whatsoever be the level.
Special classification: category of classified information or materials at the level *Très Secret Défense* and responding to the necessity of partitioning. The special classifications are organised in security networks constituted of Top secret registries. The personnel security clearance at level *Très Secret Défense* are stated for one or more special classifications expressly named.
Spécial France: mark found on the information materials and specifying their exclusive national destination.
Stamp: mark found on an information materials specifying the classification level and, if required, its exclusive national use. The stamp possesses definite characteristics (dimensions, aspect).
System administrator: person responsible for clarification, operating, maintenance, control and development of information system.
Top Secret registry: office where *Très Secret Défense* information or materials are issued, received, handled and stored.
Upgrading: modification by raising the classification level of classified information or materials.

Vulnerability: act related to the situation of a person and which weaken the guarantees that he presents for the protection of classified information or materials. It is a weakness which can lead to various pressures and which should be taken into account for giving with or without restriction, for refusing or for withdrawing access to classified information or materials.
Warning procedure: step initiated by the security clearance authority aimed at sensitising the security officer of the employer service of a person on the existence of elements that can present a risk of vulnerability of the person to be security cleared.
Withdrawal of a personnel security clearance: decision taken by the employment authority, in view of the new vulnerability elements, of deleting the security clearance of a person.

ANNEXE
Table of Annexes

ANNEX 1:

REFERENCE TEXTS

CRIMINAL CODE

Legislative part

Article 121-2
Legal entities, excluding the State, are criminally liable, as per the sections of articles 121-4 to 121-7, for crimes committed, on their behalf, by their organisations or representatives.

However, local authorities and their associates are criminally liable only for offences committed in the pursuit of activities which may be subject to public service delegation agreements.

The criminal liability of legal entities does not exclude individuals who are perpetrators or accomplices to the same acts, subject to the provisions of the fourth line of Article 121-3.

Article 226-13
The revelation of secret information by a person who is the trustee by nomination or by profession, either due to an office or a temporary mission, shall be punishable by one year imprisonment and a fine of 15,000 Euros.

Article 411-6
The fact of delivering or making available to a foreign power, a foreign company or organisation or foreign-owned entity or to their agents information, processes, objects, documents, computer files or files whose use, disclosure or assembly are likely to affect the fundamental interests of the nation shall be punishable by fifteen years' imprisonment and a fine of 225,000 Euros.

Article 411-7
The fact of collecting or assembling, for purpose of delivery to a foreign power, a foreign company or organisation or foreign-owned entity or to their agents information, processes, objects, documents, computer files or files whose use, disclosure or grouping are likely to affect the fundamental national interests shall be punishable by ten years' imprisonment and a fine of 150,000 Euros.

Article 411-8
Exercising, on behalf of a foreign power, a foreign company or organisation or foreign-owned entity or to their agents, an activity aimed at obtaining or delivering devices, information, processes, objects, documents, computer files or files whose use, disclosure or

grouping are likely to affect the fundamental national interests shall be punishable by ten years' imprisonment and a fine of 150,000 Euros.

Article 413-7
A penalty of six months imprisonment and a fine of 7,500 Euros shall be imposed, in the services, institutions or legal entities, public or private, of interest to national defence, for entering, without authorisation, inside the enclosed sites and premises where free movement is prohibited and limited to ensure the protection of facilities, materials or the confidentiality of researches, studies or manufacture.

An order of the State Council determines, on one hand, the conditions under which is carried out the demarcation of land and premises referred to in the preceding paragraph and, on the other hand, the conditions under which the permission to enter same can be issued.

Article 413-9
Possess a character of national defence secret under this present section, the processes, objects, documents, information, computer networks, computer data or files concerning national defence which have been the subject of classification measures meant to restrict their distribution or access to them.

May be subject to such measures the processes, objects, documents, information, computer networks, computer data or files whose disclosure or access to which is likely to harm national defence or could lead to the revelation of a national defence secret.

The classification levels of procedures, objects, documents, information, computer networks, computer files or files presenting a character of national defence secret and the authorities in charge of defining the conditions under which their protection is organized are determined by order of the State Council.

Article 413-10
A penalty of seven years imprisonment and a fine of 100,000 Euros shall be imposed, on any person holding, by office or profession, either due to a function or a temporary or permanent assignment, a process, object, document, information, computer network, computer data or file holding a character of national defence secret, for either destroying, diverting, removing or reproducing it, or for giving access to it to an unqualified person or for informing the public or an unqualified person.

The same penalties shall be imposed on the holding person who has allowed access to, destroy, divert, remove, reproduce or disclose the process, object, document, information, computer network, computer data or file referred to in the precedent paragraph.

Where the trustee acted recklessly or negligently, the offense is punishable by three years imprisonment and a fine of 45,000 Euros.

Article 413-11
A penalty of five years imprisonment and a fine of 75,000 Euros shall be imposed on any person not referred to in article 413-10 for:

1. Ensuring possession, access to, or knowing a process, object, document, information, computer network, or computer data or file of national defence secret;

2. Destroying, removing or reproducing, in any manner whatsoever, such a process, object, document, information, computer network, computer data or file;

3. Informing the public or an unqualified person of such a process, object, document, information, computer network, computer data or file.

Article 413-12
The attempt of the crimes referred to in the first paragraph of Article 413-10 and Article 413-11 is punishable by same penalties.

Article 414-7
The legal entities declared criminally liable, under the conditions provided in article 121-2, of the offences defined in this title are liable, in addition to the fine in the manner provided for in article 131-38, to the penalties provided by article 131-39.

The prohibition mentioned in s.2 of article 131-39 concerns the activity in the course of or at the time at which the offence was committed.

Article 414-8
The provisions of articles 411-1 to 411-11 and 413-1 to 413-12 are applicable to the acts mentioned in these provisions which are committed against:

1. the signatory powers of the North Atlantic Treaty;

2. the organisation of the North Atlantic Treaty.

Article 414-9
The provisions of articles 411-6 to 411-11 and 413-9 to 413-12 are applicable:

1. For information exchanged under a security agreement on the protection of classified information between France and foreign States or international organisations, duly approved and published;

2. For information exchanged between France and an institution or body of the European Union and classified in accordance with security regulations of the latter which are subject to publication in the Official Gazette of the European Union.

Article 434-4
A penalty of three years imprisonment and a fine of 45,000 Euros shall be imposed, on attempts to hinder the coming out of the truth:

1. to change the status of the place of a crime or a misdemeanour by alteration, forgery or erasure of traces or clues, or by providing, the displacement or removal of any objects;

2. to destroy, remove, conceal or alter a public or private document or object to facilitate the discovery of a crime or misdemeanour, the search for evidence or conviction of the guilty.

When the facts mentioned in this present article are committed by a person who, by his office, is expected to contribute to the manifestation of the truth, the penalty is increased to five years imprisonment and a fine of 75,000 Euros.

Regulatory part

Article R 413-1
Protected areas which are enclosed locations and premises mentioned in article 413-7 are demarcated in accordance with the conditions provided for in this section.

Article R. 413-2
The need for protection is determined by the minister in charge of facilities, equipment or researches, studies, manufacturing of a secret nature concerned.

The authorities responsible for services, facilities or legal entities concerned may receive by order delegation to determine this need of protection.

Article R 413-3
When the main activity of the service, facility or company under the minister has determined the need for protection, establishment and boundaries of protected areas are fixed by order of this minister.

Where the main activity of the service, facility or company is another minister, the establishment and boundaries of protected areas are fixed by the joint order of this minister and the minister who determined the need for protection.

The authorities responsible for these services, facilities or legal entities may receive by delegation order for taking the orders provided for by this present article.

Article R 413-4
The order creating a protected area is notified to the service, facility or company head. It thus takes, under the control of the authority that has determined the need for protection, all the

necessary arrangements to make visible the limits of the area and the prohibitions to which it is subjected.

A copy of the order is sent, for their information and possibly for the purposes of the application of the provisions that concern them, to the Minister of the Interior and to the competent local prefects.

Article R. 413-5
The authorisation to enter the protected area is given by the service, facility or company head, according to the directives and under the control of the minister who determined the need for protection.

However, when the area was established to protect the researches, studies or manufacturing that must be kept secret in the interests of national defence, the authorisation is issued by the minister who determined the need for protection.

In any case, the authorisation is issued in writing. It can be withdrawn at any time in the same manner.

CODE OF CRIMINAL PROCEDURE

Article 56-4
I. - Where a search is considered in a specifically identified site, holding the elements covered by national defence secret, the search may be conducted by a magistrate in the presence of chairman of the Consultative Commission on National Defense Secret. The latter can be represented by a member of the Commission or by delegates, duly security cleared to national defence secret, named in a manner according to the methods determined by order of the State Council. The President or his representative may be assisted by any person cleared for that purpose.

The list of sites referred to in the first paragraph is accurately determined and limited by order of the Prime Minister. This list, regularly updated, is communicated to the Consultative Commission on National Defense Secret as well as the minister of justice, who makes it accessible to magistrates in a secure way. The magistrate verifies if the site in which he wishes to conduct a search figures on this list.

The demarcation conditions of the places holding the elements covered by national defence secret are determined by order in the State Council.

The fact of concealing in the places referred to in the preceding paragraph processes, objects, documents, information, computer networks, computer data or unclassified files, in trying to make them benefit from the protection afforded to national defence secrets, exposes its author to the criminalties provided for in article 434-4 of the Criminal Code.

The search may be conducted only pursuant to a written decision of the magistrate who advises the chairman of the Consultative Commission on National Defense Secret of the information necessary to fulfil its mission. The chairman of the Commission or his representative goes to the scene immediately. At the beginning of the search, the magistrate shall inform the chairman of the commission or his representative, as well as the facility head or his delegate, or the person in charge of the site, of the nature of the offence or offences on

which the investigations are based, the reasons justifying the search, its aim and the sites targeted by this search.

Only the chairman of the Consultative Commission on National Defense Secret, and his representative and, if need be, persons who assist him, can gain knowledge of classified materials found at the scene. The magistrate can only seize, among the classified items, those relating to infringements on which the investigations depend. If the necessities of the investigation warrant that classified materials are seized in original, the copies are left with their holder.

Each classified item seized is, after the inventory of the chairman of the Consultative Commission, placed under seal. The seals are delivered to the chairman of the Consultative Commission on National Defense Secret of which he becomes the custodian. The operations on seized classified items and the inventory of these items are subject to a report that is not attached to the case file and which is kept by the chairman of the Consultative Commission .

The declassification and communication of elements mentioned in the inventory come under the procedure provided for by articles L. 2312-4 and following of the Defence Code.

II .- When during a search, a site turns out tohold elements covered by national defence secret, the magistrate present at the scene, or immediately notified by the police officer, informs the chairman of the Consultative Commission on National Defense Secret. The classified materials are placed under seal, without knowing about them, by the magistrate or police officer who discovered them, then are delivered or sent by any means in compliance with the regulations applicable to national Defence secrets, to the chairman of the commission in order for him to ensure its custody. The operations related to classified elements are subject to a report that is not attached to the case file. The declassification and communication of elements thus placed under seal come under the procedure laid down in articles L.2312-4 and following of the Defence Code.

III.-The provisions of this article shall be made under penalty of nullity.

DEFENCE CODE

Legislative part

Article L1111-1
The National Security Strategy aims to identify all the threats and risks that could affect the life of the Nation, particularly as regards protection of population, territorial integrity and continuation of the institutions of the Republic, and to determine the responses that public authorities must make.

All public policies contribute to national security.

The defence policy aims to ensure the territorial integrity and protecting the population against armed aggression. It contributes to the fight against other threats that could jeopardize national security. It provides compliance with alliances, treaties and international agreements and participates, in the framework of the European treaties into force, in the general European Security and Defence Policy.

Article L2311-1
The rules related to the definition of information covered by the provisions of this chapter are defined by article 413-9 of the Criminal Code.

Article L2312-1
The Consultative Commission on National Defense Secret is an independent administrative authority. It is responsible for giving an opinion on the declassification and communication of information subject to a classification under the provisions of article 413-9 of the Criminal Code, excluding information whose classification rules do not fall under the sole French authorities.

The opinion of the Consultative Commission on National Defense Secret is made following the request from a French court.

Article L2312-2
The Consultative Commission on National Defense Secret consists of five members:

1. A chairman, vice- chairman acting in his place in case of absence or incapacity and one member appointed by the President of the Republic from a list of six members of the State Council, the Supreme Court or the Court of Audits, established jointly by Vice-chairman of the State Council, the first President of the Supreme Court and the first President of the Court of Auditors;

2. A deputy, appointed for the duration of the legislature by the President of the National Assembly;

3. One senator, appointed after each partial renewal of the Senate by the President of the Senate.

The mandate of members of the commission is not renewable.

The mandate of the non-parliamentary members of the commission is six years.

Unless they resign, the offices of the commission member cannot be terminated except in case of impediments stated by the same. Members of the commission appointed to replace those whose mandate ended before its normal term shall be appointed for the remaining duration of the said mandate. Notwithstanding the fifth paragraph, when the nomination occurred less than two years before the expiry of the term of their predecessor, they may be renewed as a member of the commission.

Article L2312-3
The funding necessary to the commission to perform its mission are registered on the agenda of the mission “Department of Government action” related to the protection of fundamental rights and liberties.

The chairman is the organizer of expenses of the commission. He appoints the officers of the commission.

Article L2312-4
A French court in the context of pending court proceeding before it may request the declassification and communication of information, protected under national defence secret, to the administrative authority in charge of the classification.

This request is justified.

The administrative authority immediately refers the matter to the Consultative Commission on National Defense Secret without delay.

Article L2312-5
The chairman of the commission may conduct any necessary investigation.

The commission members are authorised to know about any classified information as part of their assignment.

They are required to respect national defence secret protected under articles 413-9 and following the Criminal Code for actions, acts or information which they know by reason of their duties.

To fulfil its mission, the commission, or on delegation of the same, its chairman is authorised, notwithstanding the provisions of articles 56 and 97 of the Code of Criminal Procedure to proceed with the opening of sealed classified elements received by him. The commission shall indicate this in its minutes of the session. The documents are returned to the administrative authority by the commission during the sending of its opinion.

The commission shall establish its internal rules.

Article L2312-6
Ministers, public authorities, public officials cannot oppose the action of the commission for any reason whatsoever and shall take all necessary steps to facilitate it.

Article L2312-7
The commission shall issue a notice within two months of its referral. This notice considers the public service assignments of justice, respect for the presumption of innocence and the rights of defence, respect for international commitments of France and the need to preserve defence capability and security of personnel.

In case of an equal share of votes, the chairman has the casting vote.

The meaning of the notice may be favourable, favourable to a partial declassification or unfavourable.

The notice of the commission is sent to the administrative authority that made the classification.

Article L2312-8

Within fifteen calendar days after receipt of the notice from the commission, or the expiry of two months mentioned in article L2312-7, the administrative authority shall notify its decision, with the meaning of the notice, to the court that requested the declassification and communication of classified information.

The meaning of the notice of the commission is published in the Official Journal of the French Republic.

Article L. 4121-2
The opinions or beliefs, particularly philosophical, religious or political, are free.

But they can however only be expressed outside the service and with the reserve required by the military. This rule applies to all means of expression. It does not prevent the free exercise of religion on military sites and aboard ships of the fleet.

Independent of the provisions of the Criminal Code relating to the violation of national defence secret and professional secret, the military must exercise caution for all acts, information or documents of which they have knowledge in the exercise or during the exercise of their functions. Apart from the cases expressly provided by law, the military cannot be absolved of this obligation by an express decision of the authority on which they depend.

The use of means of communication and information, of any kind whatsoever, may be restricted or prohibited for ensuring the protection of military personnel in operation, the execution of their mission or the security of military activities.

Regulatory part

Article R*1132-1
The General Secretariatfor defence and national security constitutes a service of the Prime Minister.

Article R*1132-2
The General Secretary for Defence and National Security ensures the secretariat of the council of defence and national security. According to the directives of the President of the Republic and the Prime Minister, he leads, in conjunction with the ministerial departments concerned, the work preparatory to meetings. He prepares records of the decisions, notifies the decisions taken and monitors their execution.
Article R*1132-3
The General Secretary for defence and national security assists the Prime Minister in the exercise of his responsibilities in defence and national security. Accordingly:

1. He leads and coordinates interministerial work related to the defence and national security policy and to public policies that contribute to it;

2. In connection with the ministerial departments concerned, it follows the evolution of international crises and conflicts that may affect the interests of France's defence and national security and examines the dispositions which are susceptible to be taken. It is associated with the preparation and conduct of negotiations or international meetings with implications on defence and national security and is kept informed of their results;

3. He proposes, distributes, enforces and monitors the measures necessary for the protection of national defence secret. It prepares the interministerial regulation on defence and national security, ensuring the distribution and monitoring of the implementation;

4. In support of the national intelligence coordinator, he participates in the adaptation of the legal framework within which the action of intelligence services is registered and in the planning of their means and ensures the organisation of interministerial intelligence analysis and summary groups;

5. He develops the interministerial planning of defence and national security, ensures its implementation and conducts the inter-ministerial exercises implementing it. He coordinates the preparation and implementation of national defence and security measures incumbent to various ministerial departments and ensures the coordination of civilian and military resources available in the event of a major crisis;

6. He ensures that the President of the Republic and the Government have the means of electronic communications and command necessary for defence and national security and ensures the operation;

7. He proposes to the Prime Minister and implements the government policy on security of information systems. For this purpose, he has at his disposal a service of national competence, called “National Information Systems Security Agency”;

8. He ensures the consistency of the actions undertaken in scientific research and technological projects policies related to defence and national security and contributes to the protection of national strategic interests in this domain.

Article R1143-1
For the exercise of their responsibilities in defence and security:

1. The Minister of Defence and the Minister of Foreign Affairs designate, for their respective ministries, a senior correspondent for defence and security civil servant, by order, and the conditions according to which they fulfil their assignments;

2. The minister of Interior is assisted by a senior defence civil servant;

3. The other ministers are assisted by a senior defence and security civil servant.

Article R1143-2
The senior officials referred to in Article R1143-1 report directly to the minister. For the conduct of their assignment, they have authority over all departments and services of the ministry.

They need to have a specialised defence service, or defence and security service.

They may assist several ministers and have one or more senior deputy officials.

They are in permanent liaison with the general secretary for defence and national security and with their counterparts in other ministries.

Article R. 1143-5
The senior officials referred to in Article R. 1143-1 run and coordinate within the ministry concerned, the policy of defence, vigilance, prevention of crisis and emergencies. They monitor the preparation of application measures. To this end:

1. They ensure the distribution of plans, employment rules and governmental orders on defence and security and coordinate the development of ministerial plans and application instructions;

2. They ensure the knowledge and proper application of the defence and security planning within the ministerial department responsible for them, through sensitisation and training and by inter-ministerial exercises and ministerial implementation of plans;

3. They are responsible for the organisation and operational maintenance of the ministerial device in an emergency; they particularly ensure the establishment and proper functioning of a permanent device monitoring and warning system;

4. They ensure the development and implementation of security policies in the areas of activity within their ministry, especially when they are recognised as vital ;

5. They advise the minister on the protection measures of goods and people within their ministry; they may be responsible for implementing these measures;

6. They ensure the protection of the scientific and technological heritage;

7. They ensure the deployment in their ministry of secure means of governmental electronic communication and emergency tools; they ensure their proper functioning;

8. They coordinate the security policy of information systems and monitor its implementation thereof;

9. They can participate, in the framework set by their minister and under the auspices of the General Secretariat for Defence and National Security, to implement the national policy of economic intelligence.

Article R1143-6
The senior officials referred to in Article R1143-1 are responsible, within the government ministry responsible for them, for the application of provisions relating to defence security and defence to the protection of secret provided in Articles R.2311-1 and the following Defence Code related to the protection of national defence secret.

In the organisations attached to the same ministerial department, these senior officials are responsible for the distribution of the provisions relating to defence security and protection of secret and monitor their application.

Article R1143-8
The senior officials referred to in Article R1143-1 send annually to their minister and the General Secretary for defence and national security a report on their activities.

The General Secretary for defence and national security submits the summary of these reports to the President of the Republic and the Prime Minister.

Article R2311-1
The processes, objects, documents, information, computer networks, computer data or files related to national defence secret are referred to in this chapter as “classified information and materials”.

Article R2311-2
Classified information and materials are subject to a classification including three levels:

1. Très Secret Défense;

2. Secret Défense;

3. Confidentiel Défense.

Article R2311-3
The Très Secret Défense level is reserved for information and materials concerning the government's priorities on defence and national security and the disclosure of which is likely to affect national defence very seriously.

The Secret Défense level is reserved for information and materials whose disclosure is likely to cause serious damage to national defence.

The Confidentiel Défense level is reserved for information and materials, whose disclosure is likely to harm national defence or could lead to the discovery of a national defence secret classified at Très Secret Défense or Secret Défense level.

Article R2311-4
The classified information and materials bear the mention of their classification level.

Classified information and materials that should not be disclosed, in whole or in part, due to their content except to certain international organisations or to certain States or their nationals, bear, in addition to the mention of their classification level, a specific mention specifying the states, their nationals or the international organisations, that can have access to them.

Classified information and materials which should never be disclosed wholly or partially to international organisations, foreign States or their nationals bear in addition to the mention of their classification level, the particular mention “Spécial France”.

The modifications of the classification level and the declassification, as well as amendments and deletions of specific mentions, are decided by the authorities who carried out the classification.

Article R2311-5
The Prime Minister determines the criteria and modalities of organising the protection of classified information and materials at the Très Secret Défense level.

For the information and materials classified at the Très Secret Défense level, the Prime Minister defines special classifications to which they are subject, and which correspond to different government priorities.

Under the conditions set by the Prime Minister, every minister, whatsoever his function be, determines the information and materials that should be classified at this level.

Article R2311-6
Under the conditions set by the Prime Minister, the information and materials classified at the Secret Défense or Confidentiel Défense levels, as well as the organisational arrangements for their protection, are determined by each minister for the administrations and organisations of his government ministry.

Article R. 2311-6-1
The information systems containing classified information are subject to, prior to their employment, a security accreditation at a level at least equal to the classification level of this information.

The protection of these information systems must, under the conditions set by order of the Prime Minister, especially in view of threats to the availability and integrity of these systems and the confidentiality and integrity of the information they contain, be ensured by the devices, hardware or software, approved by the National Information Systems Security Agency.

The authority responsible for the use of the information system attests the system's ability to ensure particularly, at the required level, the availability and integrity of the system as well as the confidentiality and integrity of information that the latter contains. This certificate is considered as a security accreditation. An order of Prime Minister sets the conditions for implementing these provisions.

Article R. 2311-7
No person is qualified to know the classified information or materials if he has not previously been subject to a security clearance decision and if he does not need, according to the approval of the employment authority under which he is placed, especially in view of the jobs catalogue warranting a security clearance established by this authority, to know them for the exerciseof his duties or the fulfilment of his assignment.

Article R2311-7-1
No person is qualified to access an information system or its devices, hardware or software, of protection, when this access allows knowledge of the classified information contained therein or modify the protection devices of this information, if he has not previously been subject to a security clearance decision and if he does not need, according to the approval of the authority responsible for the system work, to access it for the exercise of his duties or the fulfillment of his assignment.

Article R2311-7-2
The security clearances mentioned in articles R2311-7 and R2311-7-1 can be issued to individuals as well as legal entities.

Article R2311-8

The security clearance decision specifies the classification level of classified information and materials which the holder can know as well as the work that it concerns. It comes after a procedure defined by the Prime Minister.

It is taken by the Prime Minister for Très Secret Défense level and indicates particularly the special categories to which the security cleared person has access.

For Secret Défense and Confidentiel Défense classification levels, the security clearance decision is taken by each minister for the ministry under his charge.

Article R2311-8-1
Each minister may, by order, delegate to the prefect locally competent the signature of security clearance decisions to know information covered by national defence secret for personnel of his ministerial department and placed under the authority of the prefect and the persons employed in organisations related to his assignments.

Article R2311-9
The Defence Minister or the command is authorised to restrict the use of the communication and information methods, whatsoever, for ensuring the protection of military operations, the execution of the mission or the safety of military activities.

The possession and use of cameras, film, telephone, data communication or records as well as transmitters or receivers or television broadcasting in the enclosures and the military establishments or in the country, in the cantonments and vehicles, and on board the fleet ships and aircrafts, may be subject to prior authorisation.

The publication or sale of films, photographs or recordings taken in the enclosures, military establishments, ships and aircraft fleet, or during operations, manoeuvres or any other military activity is subject to prior authorisation of the commander of the administrative training.

Article R2311-9-1
The list of sites holding elements covered by national defence secrets mentioned in the second paragraph of Article 56-4 of the Code of Criminal Procedure, is established by order of Prime Minister on the proposal of the concerned ministers.

The list designates the sites involved in conditions such as to allow their accurate identification by the Consultative Commission of national defence secret and the magistrates. It may include categories of premises, classified by government ministry, when this designation is sufficient to the identification of the sites or, otherwise, of individual locations. It is regularly updated.

The list is sent to the Minister of Justice and the Chairman of the Consultative Commission of national defence secret. The Minister of Justice implements, under the conditions defined by order of the Prime Minister, secure access to the list, such as to preserve the confidentiality thereof and allowing each magistrate to verify whether the site in which he wishes conduct a search figures on this list.

Article R2311-10
Under the authority of the Prime Minister, the General Secretary for defence and national security is responsible for studying, prescribing and coordinating at interministerial level the measures to ensure the protection of national defence secret. He is qualified as national security authority for national defence secret, for the implementation of international agreements and treaties providing for such authority.

The General Secretary for Defence and National Security ensures the implementation of the measures mentioned in the first paragraph. He has the authority to control them. He has the possibility to referral at all times, through the ministers concerned, the services that contribute to crime prevention.

The defence security assignments specified above do not affect the responsibilities of ministers in this matter.

Article R2311-10-1
The General Secretary for Defence and National Security may, in his capacity as National Security Authority for national defence secret, name in particular domains, especially in the industrial field, on proposal of the Ministers concerned, a Designated Security Authority.

Article R2311-11
The General Secretary for Defence and National Security, in accordance with the provisions of Article R2311-10, prescribes, coordinates and monitors the implementation of measures to ensure the protection of secret in relations between France and foreign countries.

He ensures, under international agreements, the security of classified information entrusted to France.

He defines measures to protect information and materials held by France, which have been classified by a foreign State or international organisation and which do not bear mention of a classification level equivalent to those defined in article R. 2311 2.

He sets out measures to ensure the protection of national information entrusted to foreign states or international organisations.

Article D*2311-12
For the exercise of his duties mentioned in Articles R2311-10 and R2311-11, the General Secretary for defence and national security has at his disposal a defence security service.

Article R2312-1
The chairman of the Consultative Commission of national defence secret can be represented by a member of the commission or a delegate chosen from a list provided by the commission during the searches conducted by a magistrate, under I of article of 56-4 of the Code of Criminal Procedure. In this case, he shall designate such a representative upon receipt of the decision of the magistrate.

The General Secretary and former members of the Consultative Commission of national defence secret may be on the list, as well as people presenting guarantees with regards to both the constitutional objectives of the search for criminal offenders and safeguarding the fundamental interests of the nation, and not exercising the functions that could lead them to know the legal proceedings at the start of the search. The people on the list shall be security cleared to national defence secrets for the accomplishment of their mission.

The choice of the representative must ensure his actual presence in the place searched considered by the magistrate, throughout the expected duration thereof.

Article R2312-2
The magistrate and the representative appointed by the chairman of the Consultative Commission of national defence secret are, by all means, immediately informed of the appointment made by the President.

Article R2313-1
The rules relating to the archiving services of the Ministry of Defence are defined by Decree No. 79-1035 of December 3, 1979 on the archives of the defence and under Article 4 of Decree No. 79-1037 of December 3, 1979 on the aptitude of public archiving services and the cooperation between the administrations for the collection, storage and communication of public records.

HERITAGE CODE

Article L211-1
The archives are the set of documents, regardless of their date, place of storage, their notice and media, created or received by any person or company or by any public or private organisation in the exercise of their activity.

Article L212-2
At the expiry of their current period of use, the public archives other than those mentioned in Article L212-3 shall be selected to separate the documents to be conserved from the documents lacking administrative value or historical or scientific interest, for disposal.

The list of documents or categories of documents for disposal as well as the conditions of their disposal is determined by agreement between the authority which issued or received and the archives administration.

Article L213-1
Public archives are, subject to the provisions of Article L213-2, legally communicable.

Access to these archives is exercised under the conditions set for the administrative documents under Article 4 of Law No. 78-753 of July 17, 1978 laying down various measures to improve relations between the administration and the public and various administrative, social and fiscal provisions.

Article L. 213-2
Notwithstanding the provisions of Article L213-1:

I. - Public records are automatically legally communicable at the expiry of a period of:

1. Twenty-five years from the date of the document or the most recent document included in the file:

a) For the documents whose communication violates the secret of the government and the responsible executive authorities discussions, the conduct of foreign relations, currency and public credit, commercial and industrial confidentiality, research by the relevant departments of tax and customs offenses or the confidentiality of statistics except when relevant data are collected through questionnaires relating to personal facts and behaviour mentioned in 4 and 5;

b) For the documents mentioned at 1° of I of Article 6 of Law No. 78-753 of July 17, 1978, with the exception of documents produced under a contract for services performed for one or more persons determined when these documents enter, because of their content, the scope of 3° or 4° of this I;

2. Twenty-five years after the date of death of the concerned person, for documents whose disclosure violates patient privilege. If the date of death is unknown, the time is one hundred and twenty years from the date of birth of the person concerned;

3. Fifty years from the date of the document or the most recent document included in the file, for documents whose disclosure violates national defence secret, the fundamental interests of the State in the conduct of external policy, state security, public safety, the safety of persons or the protection of privacy, except for the documents mentioned in 4° and 5°. The same deadline applies to documents that have a value judgement or opinion on an individual, named or easily identifiable, or who reveals the behaviour of a person under circumstances likely to cause prejudice to him.

The same deadline applies to documents relating to the construction, equipping and operation of structures, buildings or parts of buildings used for detention of persons or usually receiving detained persons. This period is counted from the end of the assignment to use these structures, buildings, or parts of buildings in question;

4. Sixty-five years from the date of the document or the most recent document included in the file, or a period of twenty-five years from the date of death to a person if the latter period is shorter:

a) For documents whose disclosure violates the confidentiality of statistics where relevant data are collected through questionnaires relating to private facts and behaviour;
b) For documents relating to investigations conducted by legal police services;
c) For documents relating to cases before the courts, subject to special provisions relating to judgments, and enforcement of judgments;
d) For the minutes and directories of public officers or ministers;
e) For records of birth and marriage of the civil state, from the date of their completion;

5. One hundred years from the date of the document or the most recent document included in the file, or twenty-five years from the date of death of a person where the latter period is shorter, for the documents referred to in 4° relating to a minor.

Similar limits apply to documents covered or having been covered by national defence secrets whose disclosure is likely to endanger the safety of persons named or easily recognisable. It is the same for documents relating to investigations conducted by police services, matters brought before the courts, subject to special provisions relating to judgments, and execution of court decisions which affect the intimate communication of the sexual life of people.

II .- Those public archives cannot be consulted whose disclosure would lead to the dissemination of information to design, manufacture, use or locate nuclear, biological, chemical or other weapons which have direct or indirect destruction effects of a similar level.

II .- The administration of archives can also, after approval by the authority which has authored the documents, decide on the anticipated opening of the funds or part of the funds from public records.

Article L213-3
I. - Authorisation to consult public archives prior to the expiry of the deadline established in I of Article L213-2 may be granted to persons who request it where the interest which is attached to the consultation of these documents does not lead to an excessive undermining of the interests that the law has contemplated to protect. Subject to, in respect of the minutes and registers of notaries, Article 23 of the law of 25 Ventôse year XI containing the organization of the notary, the authorisation is granted by the administration of archives to those who made the request after approval by the authority which has made the documents.

The response time to a consultation request may not exceed two months from the registration of the application.

II .- The archives administration may also, after approval by the authority which has made the documents, decide on the anticipated opening of the funds or part of the funds from public records.

Article L. 213-4
The payment of public records from the President of the Republic, the Prime Minister and other Cabinet members may be accompanied by the signature between the paying party and the government archives of a protocol related to processing, conservation, evaluation or communication conditions of the funds paid, during the period provided for in Article L213-2. The provisions of this Protocol may also apply to public records from the personal collaborators of the signatory authority.

For the application of Article L213-3, the agreement of the paying party required for authorising the consultation or the anticipated opening of the fund is given by the signatory of the protocol.

The protocol is automatically terminated legally in case of death of the signatory and, in any event, at the date of expiry of the period provided for in Article L213-2.

The public archive documents made prior to the publication of Law No. 2008-696 of July 15, 2008 related to the archives that was still governed by the protocols then signed. However, the provisions of these protocols relating to the agent designated by the signatory shall cease to apply twenty-five years after the death of the signatory.

Article L. 213-5
Every government holding public or private, archives is required to give reasons for any opposition to a request for the communication of the document archives.

Article L. 213-6
The public archive services which receive the private archives as a gift, bequest, transfer or deposit is required to comply with the stipulations of the donor, the author's legacy, the transferor or applicant for the conservation and communication of such records.

Article L. 213-7
The provisions of Articles L213-1 to L213-3, L213-5, L213-6 and L213-8 are displayed clearly in premises open to the public from the public archive services.

Article 26 of law no. 83-634 of July 13, 1983 concerning rights and duties of officials:

The officials are bound by professional privilege under the rules established in the Criminal Code.

The officials must exercise professional discretion for all the facts, information or documents they have knowledge of in the course of exercise or in connection with the exercise of their duties. Apart from the cases expressly stipulated by the regulations in force, particularly regarding freedom of access to administrative documents, the officials cannot be released from the obligation of professional discretion by the express decision of the authority upon which they depend.

ANNEX 2:
Classification guide:
Recommendations for the development of the specific ministerial directive relating to the protection of the secret

The onus is on each minister, according to his mandate, to define in a specific directive:

a) the conditions of use of classification levels *Secret Défense* and *Confidentiel Défense*. He particularly fixes:

- The application scope of each level of *Secret Défense* and *Confidentiel Défense* and establishes the classification of information or categories of information that will have to be covered by the secret;
- The objective criteria to be considered in assessing the secret nature of information (for example, importance in the defence and national security policy and organisation, the concerned domain, the nature of the source ...);
- The authorities responsible for the classification.

b) The information or categories of information which must be classified *Très secret*:

- either in the special classifications which divide this level;
- either in a new category within one of the existing special classifications;
- or in a new special classification after exceptional creation request to the Prime Minister.

The following elements can be taken as a reference for the classification at the most appropriate level. They are for illustrative purposes only and do not constitute a exhaustive list.

1) The ***Très Secret Défense*** level is reserved for information or materials relating to government priorities in defence and national security matters and whose unauthorised disclosure is likely to affect national defence very seriously.

The compromise of such information would lead to:

- a direct threat to the internal stability of France or of allies or friendly countries;
- a very serious prejudice against relations with allies or friendly governments;
- a very serious prejudice against operational efficiency, including in the framework of combined operations, security of national armies, maintenance of the efficiency of basic security or information operations for the nation;
- a serious prejudice against French economy;
- the risk of loss of a large number of human lives.

2) The ***Secret Défense*** level is reserved for information or materials whose disclosure is likely to seriously affect national defence.

The compromise of such information could:

- lead to international tensions;
- seriously harm relations with allies or friendly governments;
- seriously harm the operational efficiency of security or information actions;

- cause prejudice against materials, important to the financial, monetary, economic or commercial interests of France;
- directly threaten human lives, seriously harm public order, security or liberty of people.

3) The ***Confidentiel Défense*** level is reserved for information or materials whose disclosure is likely to affect national defence or can lead to the discovery of a national defence secret.

The compromise of such information would:

- harm important diplomatic relations (official protests or sanctions);
- represent a serious obstacle to the development and functioning of the main policies of France;
- harm the operational efficiency, including in the framework of combined operations, security of national armed forces, maintenance of the efficiency of security and information operations;
- lead to the termination or strong disturbance of activities linked to the continuity of national life;
- go against the financial, monetary, economic or commercial interests of France;
- substantially compromise the financial viability of large organizations ;
- create an obstacle to enquiries related to serious crimes or facilitates the commitment of these crimes;
- cause injury or harm to security and liberty of the people.

It is reminded that the decision to classify an information is an important act due to the restrictions that are induced in the matter of protection and to the legal consequences that it can generate. An over-classification results in an inflation of protected documents, devalues the concept of secret and is accompanied by additional costs. Conversely, an under-classification does not guarantee sufficient protection to the information.

ANNEX 3:
Rules of protection for information or materials bearing the mark *Diffusion Restreinte*

The mark *Diffusion Restreinte (DR)* is not a classification level, but a mark of protection. Its main objective is to make the user aware of the necessary discretion he must exercise in the manipulation of information covered by this mark.

1) Holder of** Diffusion Restreinte **information

The application of this mark reveals the need to avoid the disclosure, in the public domain, of information whose grouping or operation could:

- lead to the discovery of classified information ;
- undermine the security or public order, reputation of institutions, private life of their members;
- harm the economic or financial interests of private legal entities or public facilities.

Should particularly receive at least the mark *Diffusion Restreinte*:

- the documents defining, generally, the aims, options, criteria of choice retained in different domains of national military activity or operational or technical security and which cannot be classified;
- the documents related to public order (event reports…);
- the unclassified documents whose distribution should be limited and controlled in accordance with the provisions of a security agreement signed with a foreign country;
- the operation documents whose confidentiality has only a limited and temporary interest;
- the documents or information issued from a ministry which wishes to limit or monitor the distribution.

The mark *Diffusion Restreinte* is not meant to protect personal information, but this possibility is not excluded (for example, report on the morale of a group, report of an event …).

***2) Condition of use of the mark** Diffusion Restreinte*

It is up to each authority of the State Administration, facilities' head or service head, to decide if the distribution of information should be restricted or not.

Any signatory to a document containing information responding to the criteria specified above is responsible for the assignment of the mark *Diffusion Restreinte.*

The *Diffusion Restreinte* information should be communicated only to persons who need to know it for service, that is, within the limits of their assignments:

- the civil and military personnel of ministries;
- the designated personnel of a company holding a public deal passed by an organisation relating to a ministry: these personnel should be informed of

the discretion rules to be applied vis-à-vis information and their contractual responsibilities.

Generally, a *Diffusion Restreinte* document issued by a ministry can only be communicated to persons belonging to this ministry and to organs having a need- to-know and with whom they are entering into a relationship.

3) Development and marking

The development of *Diffusion Restreinte* documents can only be made in the premises or enclosures of public or private organisations offering sufficient security conditions banning access of unauthorised individuals to these documents.

The *Diffusion Restreinte* documents should be identified on the first page with the references of the issuing organisation, the date of issue and the record number.

It should bear the following marking:

- on each page, the *Diffusion Restreinte* stamp affixed in the middle of the top of the page;
- for the messages and other computer documents, the mark *Diffusion Restreinte* reminded at the start of each page;
- for the linked documents, the *Diffusion Restreinte* stamp affixed in the middle of the cover and the last page;

4) Shipment and circulation

The internal transmission of *Diffusion Restreinte* documents can be carried out:

- internally:
  - in a premises, enclosure or building related to a ministry, by any person of this ministry;
  - in a public or private organisation within the framework of a public deal, in an envelope or by person designated by the deal holder;
- externally:
  - in double envelope, the internal envelope bearing the mark *Diffusion Restreinte* and the document references, the external envelope only includes the addresses required for the transmission;
  - by post (civil or military) in metropolitan France, to the departments or overseas communities or abroad[147], by means guaranteeing the proper receipt of the document.

5) Storage, destruction and reproduction

The documents marked *Diffusion Restreinte* are registered at the departure and arrival according to the rules applied to any unclassified administrative document.

[147] For documents bearing the marking *Spécial France* these articles have to be combined with art. 65 of the present directive.

They should be stored in furniture which can be locked.

Their destruction takes place under the responsibility of the holders, without specific mention on the record documents of the mail.

Their reproduction should remain limited only to the requirements of the service.

6) Security of information systems

Information systems for processing, storage or transmission of *Diffusion Restreinte* information are subject to a security accreditation. A directive established by the ANSSI defines the rules applicable to the information systems at this level.When the urgency of their processing or transmission is more important than protecting their confidentiality, the *Diffusion Restreinte* information can, exceptionally, be processed or transmitted over systems that have not been the subject to a security accreditation at the *Diffusion Restreinte* level.

ANNEX 4:
Access control

The **access control** consists of verifying if a person requesting access to a site or an information has the right to do so.

As shown in article 70, its objectives are:
- of filtering the circulation flow, the individuals and vehicles entering or exiting a site, building or place;
- monitoring the individuals and vehicles in protected areas;
- to prevent or limit the movement of unauthorised individuals.

It is part of a global security system founded on its association with the internal, perimetric and peripheral protections.

It includes identification, processing and braking methods.

1) The **identification method** is the means enabling to receive the access rights of the individual and transmit them to a processing method.

2) The **processing method** is the means which validates, according to the rights given, the information provided by the monitoring methods in order to remove the obstacle and free movement.

The processing method covers three methods:
- action of a person;
- action of an automated system;
- combination of both.

3) The **braking method** is the device that obstructs the intrusion and enables to gain time required for intervention.

The access control rests on the following principles:
- the homogeneity (between the access control methods and other means of protection retained);
- the succession of filters (monitoring of buyers should be distributed in depth, in several layers);
- the proportionality to the threat (the checking should be adapted to potential attackers);
- the adaptation to buyers (it should be accepted by the current users).

The technical solutions retained depend on the requirements:
- what will be the use of it? (accessing a building, an area, a premises)?
- who will be controlled (military, civil personnel, scientific, maintenance personnel, technicians)?
- against which threat should we protect ourselves? (internal threat, vandalism, espionage or information leak) ?

Before any concept choice, an audit is required in order to gain a sound knowledge of the site, which enables:

- identifying, localising, setting in hierarchy, the targets of a site and the areas to be controlled;
- analysing the flow of individuals, vehicles at each access point;
- stating the existing level of protection of areas (openings, walls, presence or absence of monitoring systems such as card readers, barriers to passage, the level of resistance of these barriers to intrusion, uniformity of these points…)
- identifying potential threats (involuntary intrusion of the curious, deliberate penetration of initiated and/or equipped persons, internal complicity …);
- taking account the restrictions (architectural, regulation (fire, protection of national defence secret…).

Examples of mechanical or electronic means used for access control: access gates, tripod turnstiles, barriers, sas, interphones, videophones, keyboard codes, badge readers, biometric readers…

ANNEX 5 :
The different types of physical protection measures

All the security measures relative to physical protection is intended to ensure the physical integrity of buildings and facilities specifically dedicated to classified information or information media as well as the reliability of any pieces of furniture in which they are kept, so as to prevent any loss, degradation or compromise.

It is reminded that the classification level of the information and materials ascertains the threats and vulnerabilities to take into account and defines the level of protective systems required.

The physical protection measures include technical or human resources and rely on a specific organization, in order to coordinate the latter. These include:

- **static measures** based on physical devices. They constitute the bulk of the means of protection (walls, fences, doors, armored cabinets...) and of detection (volumetric radar, opening sensor, seismic detector ...) and provide passive and active protection. It also includes the installation of hierarchical control access systems tailored according to the need to know principle (such as badges or biometric reader);

- **dynamic measures** involving human intervention (guards, patrolling, screening, on-site or off-site intervention personnel) which contributes to detection by surveillance activities and ensure appropriate response in case of intrusion ;

- new **technological measures** the implementation of which must be well mastered and tested by users; if necessary, they will be complemented by more traditional mechanical methods;

- new **technological devices** whose implementation shall be perfectly mastered and tested by the investigating services of the Ministries of Defence and Interior, validated by the users and which will, if necessary, be complemented by more traditional devices.

The physical protection measures are subject to close monitoring and to any updates necessary to maintain the effectivenessof the whole security system.

ANNEX 6:
Physical protection barriers
and their division into classes

Barriers are divided into classes indicating their degree of resistance to an intrusion attempt. Each barrier is divided into four classes, from the less reliable to the most robust. Access control and an intervention procedure are required for all classes.

1. ***Classes of building and/or site:***

Class 4: - protected enclosure (fence of more than 2.15 m in height, or in the case where the walls of the building is the enclosure, protection of all openings less than 5.50 m above ground level)

- but no permanent guards.

Class 3: class 4 protection

+ permanent guards conducting patrols on the premises and site

or detection device / alarms connected to an external intervention entity (police station, police headquarters, security company).

Class 2: class 3 protection

+ detection devices / alarms (lighting system, remote monitoring, video surveillance, perimetric or peripheral detection)

+ Permanent presence of guards.

Class 1: class 2 protection

+ detection devices / alarms for the premises (volumetric or peripheral detection) or furniture (localized detection)

+ access logging (log and video surveillance).

Electronic filtering devices alone cannot ensure the integrity of access to buildings and / or site. They must mandatorily be complemented by mechanical lockout systems activated outside normal building occupancy hours.

2. ***Classes of the premises***

Walls, ceilings and floors of the premises must provide sufficient resilience.

Class d: premise with door having an ordinary mechanical lock, equipped with a safety latch with key which is protected, if possible, and unprotected windows.

Class c: premise with door having a high security lock (multipoint), equipped with a safety latch with key which is protected and windows which are protected when they are located within 5.5 m of access point (ground, roof, cornice, downspouts, promontory).
Protection of windows must be ensured:
- either by steel bars, 2 cm in diameter at least and 11 cm apart at most;

- or by a burglar-proof glazing. Windows must then be fitted with an opening-limitation device in order to prevent intrusion.
Class b: premise with reinforced door (solid wood or covered with sheets of steel) equipped with security bolts, high security mechanical lock with opening sensor or counter; other openings shall be protected as for class c.

Class a: vault whose door is at least equipped with security systems of Class b armored cabinets. The walls of the premises must have a resilience that is at least equivalent to that of 15 cm of concrete.

3. *Classes of the Furniture*

Armored furniture for conservation of classified information or information media fall into three classes and cannot be opened fraudulently without breaking and entering. They are hence designed so that any attempt to illegitimately open them leaves obvious marks. They will by default be equipped with a mechanical lock that meets the maximum security standards of their country of design.

Class C: cabinet which is considered to be armored, with one or two doors, with a metal frame at least 2 millimeters thick, equipped with a silent mechanical combination lock and having quiet operation which allows one to not need any keys. The doors must have a system protecting the pivot side prohibiting the removal of doors in case the hinges are cut, when the furniture is locked up. The bolts, inaccessible from the outside, must not allow for dismantling.

Class B: armored cabinet of identical structure as for class C
+ a strengthening of the structure of the area behind the vital organs[148] whose presence can be visually verified by removing the lock cover door (interior side of the door);
+ an indicator device, with mechanical and thermal trigger, definitely blocking the opening mechanisms during any illegitimate opening attempt;
+ a lock cover door seal (interior side of the door) allowing easy detection of any dismantling;
+ a lock to the combination changing device for the for the mechanical models, preventing access without a key;
+ a servomechanism, prohibiting the release of the bolts of the main door when the other door is not closed, in the case of there being not a single swing door;
+ a device that prevents the bolts from the front door, once released, to withdraw unless the combination is dialed again;
+ an opening counter that is not falsifiable and non-reusable, without a reset and which is protected by the lock cover;
+ a silent combination mechanical lock with quiet operation is recommended. The use of an electronic lock can be allowed if it is deemed necessary[149]. It must in that case be a high end lock[150], have an auditable memory, and eventually be programmed so as to be opened only in given time slots, include a system allowing a user to trigger an alarm towards a security service when the opening is made under threat.

[148] Locks, combinations, mechanisms ensuring the operation of the piece of furniture.
[149] The use of an electronic lock can be justified if single or multi-user audit functionalities, opening time slots defined by the user or users, alarm under threat or delayed openings are necessary.
[150] A lock that allows for setting opening and closing parameters. It must also allow to manage codes according to schedules and users.

The cabinet equipped with an electronic combination lock shall additionally include an easily switchable mechanical key. This key will be trapped in the lock so long as the combination bolts and the cabinet bolts are not extended, with the doors closed.

+ A system of steel wire rails on the main door ensuring a geographical distribution of the several horizontal and vertical bolts. If a handle operates the system, it must have such a breaking point so as to avoid excessive force on the railing.

The doors will be devoid of any property plate and of any decorative elements.

Class A: a safe which is shielded on all sides, with a minimum weight load of 500 kilograms or, alternatively, attached to the wall, to the floor or on a metal plate whose smallest dimension is larger than the largest dimension that of the largest exit in the room.

This cabinet shall contain all the class B security systems and in addition:

- one or more locks that can adapt to a new set of keys (known as mechanical locks with easily interchangeable keys[151]);
- at least one lock whose key remains trapped by the latch mechanism as long as the combination bolts and the furniture bolts are not extended with the door closed.

In general, the make and serial number of the piece of furniture are stamped on the outer shell in an apparent and unchangeable manner, as on all fixed and moving parts. The serial number and year of manufacture of each lock must be seen on them.

[151] Key lock that can be set to be opened by a new set of keys without disassembling the mechanism. This action must cancel the possibility of opening with the former set of keys.

Class combination tables

The following tables indicate the various possible combinations between the three barriers classes in order to obtain a minimum security level relating to each classification.

Table 1: Level Très Secret Défense

Class of the building or site	Class of the site			
	a	b	c	d
1	C	B	Prohibited	Prohibited
2	B	A	Prohibited	Prohibited
3	A	Prohibited	Prohibited	Prohibited
4	Prohibited	Prohibited	Prohibited	Prohibited

Table 2: Level Secret Défense

Class of the building or site	Class of the site			
	a	b	c	d
1	C	C	Prohibited	Prohibited
2	C	C	Prohibited	Prohibited
3	C	C	Prohibited	Prohibited
4	Prohibited	Prohibited	Prohibited	Prohibited

Table 3: Level Confidentiel Défense

Class of the building or site	Class of the site			
	a	b	c	d
1	C	C	C	C
2	C	C	C	C
3	C	C	C	B
4	C	C	B	Prohibited

ANNEX 7:
Measures applicable to restricted areas

As soon as documents having a classification level equal to or higher than *Secret Défense* are processed in the premises, special security measures must be implemented. These security measures define the restricted areas which are themselves compulsorily located in a protected area, as per the provisions of article 74 in this document.

The protection of classified information or information media is ensured by a tightening of the physical protection and access control measures, whose objective is to prevent:

- All access to this information by persons who have no need to access it, even if they are security cleared;
- Any entry, by viewing or listening, directly or indirectly, in sites where secrets are developed, processed, received or stored;
- Access to information systems classified at the *Secret Défense* level that could hinder or distort the systems operation, or fraudulently introduce, delete or modify data in these systems.

Processing or storage of classified information or materials in these premises can take place only after notification by the investigating services regarding the capacity of the premises to receive documents equivalent to or higher than *Secret Défense* level, except in cases where this is utterly impossible.

When services or organizations are required to process such documents occasionally, it is recommended that the security measures described here above be applied temporarily.

The sites containing classified elements at *Secret Défense* or higher level must satisfy the following standards:

- they must at least contain premises with a restricted number of openings, protected windows and strengthened doors with high security locks, and equipped if possible with an opening counter;
- this premises must contain an approved security cabinet;
- a constant monitoring of the site must be organized, based on at least one of the security systems described in **annex 5**.

If required, equivalent standards may be adopted by each minister in order to meet the requirements of situations specific to some premises.

- <u>Inspection of the premises</u>

For each site, a person in charge has to ensure that the scheduled security measures, especially the rules of access to the site, are applied.
During working hours, the premises must be inspected by the personnel employed there. Before any period of absence, they must ensure that the classified information or information media are secure and that the safes and offices are closed.

Outside the working hours, inspections are organized by the authorities in charge, so as to monitor:

- the functioning of detection devices;
- the closing of offices, safes, cabinets etc.;
- the emptying of dustbins and absence of any rough drafts or preparatory documents with classified information on them;
- the absence of classified information media outside the safes, except for media that cannot be hidden from direct view.

Security patrols are carried out regularly by guards who have undergone a security screening and have written instructions specifying their duties. These rounds are performed without the guards having to enter the restricted areas in the absence of personnel, unless required by the service (clear suspicions, special regulations, proven emergencies).

- Control of people and visitors in sites holding elements covered by national defence secret

Service people with access to sites holding elements covered by national defence secret at the *Secret Défense* level or above possess a visible badge.

The visitors are:

- provided with an individual authorisation from the authority in charge;
- provided with a temporary pass;
- accompanied throughout their visit by a security cleared person selected from the personnel of the site.

The maintenance personnel:

- must undergo a basic security screening;
- belong to a company that has previously met the requirements of a security investigation;
- wear a visible badge with photo;
- operate in the presence of site personnel.

ANNEX 8:
Guide of security measures applicable during meetings involving Classified Information

Before the meeting:

1. The organizer must determine the classification level of the meeting and request for the names of people who will attend the meeting so as to prepare the list of participants.
2. The organizer must ensure that the security officer receives the list of participants so as to check that their personnel security clearance (PSC) is valid and corresponds to the level of information or information media that are going to be dealt with.
3. The security officer ensures that the place where the meeting is to be held meets the security requirements of the classification level of the information to be addressed.

At the beginning of the meeting:

5. The security officer ensures that the identity of each participant is verified and complies with the list of participants previously validated by him.
6. The organizer informs the participants of the maximum classification level of the information to be addressed during the meeting and their corresponding security rules.
7. The organizer, assisted by the security officer, ensures that the security measures concerning mobile phones and other electronic devices are applied.

During the meeting:

8. The maximum classification level of the information discussed during the meeting must not exceed the PSC level of each participant as well as the protection capacities of the room where the meeting is held.
9. The organizer shall see to it that the communication of classified information is restricted to the purpose of the meeting.
10. During breaks, the participants are permitted to leave the meeting room if the security of the classified documents left behind is guaranteed.
11. Classified information must not be discussed outside the meeting room.
12. Any breach in security during the meeting must be reported to the organizer and the security officer, who shall inform the participants about it.

At the end of the meeting:

13. The organizer and the security officer are responsible for the collection, putting aside or destruction of classified documents once they cease to be useful.
14. The organizer writes the minutes of the meeting including the subjects discussed, the measures taken to ensure the protection of the classified information and the participants list.
15. When the participants are authorised to take notes during the meeting, the organizer informs them of their liability as regards the protection of secret.

ANNEX 9:
Contractual model clauses
for the protection of national defence secret

The following clauses are hereby included in the contracts under the present document. They can be adapted or completed by the contracting authority that cannot bypass them.

1. GENERAL SECRET PROTECTION CLAUSE

As part of the legislative and regulatory provisions regarding the protection of national defence secret, the contract holder undertakes to ensure the protection of classified information or information media that he may have knowledge of and/or possess under this contract, taking into account the special provisions specified in the security aspects letter of this present contract.

He acknowledges being informed of the following texts on his obligations regarding knowledge and possession of classified information covered by the national defence secret:

- the Criminal Code, especially the articles 413-9 to 414-9;
- the General Inter-ministerial Directive no.1300 related to the protection of national defence secret.

He agrees to comply with his obligations under the application of these provisions and those resulting from all the legislative and regulatory texts related to the protection of national defence secret.

Any violation or non-observance of security measures by the contract holder, even in cases resulting from carelessness or negligence, may lead to the termination of the contract to his detriment and withdrawal of the company's facility security clearance (FSC) to access classified information or material, without prejudice to the penalties prescribed by the provisions of Articles 413-9 to 413-12 of the Criminal Code.

2. ADDITIONAL STIPULATIONS PERTAINING TO CONTRACTS REQUIRING THE POSSESSION OF CLASSIFIED INFORMATION OR INFORMATION MEDIA BY THE CONTRACT HOLDER

- The work premises of the contract holder must offer all the guarantees to ensure the protection of national defence secret and can be subjected to inspections by the contracting authority.
- The contract holder agrees to report any modification that may bring changes to the guarantees in his premises for the protection of classified information or information media communicated as part of this present contract.
- On completion of the classified work, the contract holder has a time period of one month to inform the contracting authority about it. The latter (contracting party) shall then indicate the destination of the classified information or information media which have been until then in the possession of the contract holder. The contract holder agrees to adhere to this arrangement. In case of non-compliance with these provisions, the contract holder shall incur a penalty stipulated in the contract.

In the case of non-execution of work required by the investigating service in charge of verification of the physical aptitude of the premises in the conditions defined in the General Inter-ministerial Directive No.1300 pertaining to the protection of national defence secret, the contract holder's liability is engaged.

3. ADDITIONAL STIPULATIONS FOR RESEARCH OR STUDY CONTRACTS

- The contract holder acknowledges the contracting authority's power to search for classified information or information media related to the contract among the documents and materials in the contract holder's possession and to affix seals on the safes and premises in which the documents and materials recovered by the administration shall be gathered together for their protection.
- The entire classified information or material listed in the security aspect letter (SAL) must be returned in totality to the contracting authority.
- The working premises of the contract holder must have all the guarantees to ensure the protection of national defence secret and can be subjected to inspections.

4. STIPULATIONS FOR PROTECTION OF SECRET FOR THE EMPLOYMENT CONTRACT OF A SECURITY CLEARED PERSON

As part of the legislative and regulatory provisions regarding protection of the national defence secret, the holder of an employment contract agrees to comply with the measures prescribed to him to ensure, during the term of the said contract, the protection of classified information and information media that he may, upon a need to know principle, be required to know or possess, as per the conditions of his prior security clearance by the competent administrative authority and within the validity limits and secret level mentioned in the security clearance decision.

He acknowledges having taken cognizance of Articles 413-9 to 413-12 of the Criminal Code, of the General Inter-ministerial Directive No.1300 pertaining to the protection of national defence secret and arrangements made to ensure the protection of classified information or material.

5. STIPULATIONS FOR PROTECTION OF SECRET FOR THE EMPLOYMENT CONTRACT OF A PERSON NOT SECURITY CLEARED

As part of the legislative and regulatory provisions regarding protection of national defence secret, the holder of the work contract agrees to comply with the measures prescribed to him to ensure, during the term of the contract, the protection of classified information or information media that may be retained in the department for which the contract is executed and in any place in which the contract is executed.

He acknowledges having taken cognizance of Articles 413-9 to 413-12 of the Criminal Code and the provisions taken to ensure the protection of classified information or material.

ANNEX 10:
Model contractual clause for the protection of national defence secret for sensitive contracts

1. Within the framework of rules and regulations on the protection of national defence secret, the contract holder agrees to take all appropriate measures to ensure, during the execution of the contract, the absolute protection of all classified information or information media that may be held within the department for which the contract is carried out or in any location where the contract is carried out.

2. The contract holder acknowledges:
- having taken cognizance of articles 413-9 to 413-12 of the Criminal Code;
- that he does not have to know or possess any information covered by the national defence secret.

3. The contract holder acknowledges having made all of the personnel who are under his responsibility and who act on his behalf to perform services, sign an individual statement in which the aforementioned personnel certifies:
- having taken cognizance of Articles 413-9 to 413-12 of the Criminal Code;
- that they do not, under penalty of criminal prosecution, have to know or possess any information covered by the national defence secret.

4. The contract holder agrees that only persons who have submitted the abovementioned statement beforehand shall access the site where the services are carried out.

5. The contract holder undertakes to submit the individual statements mentioned above to the contracting authority prior to any of the concerned personnel accessing the sites where the services are carried out.

6. No concessions to the above provisions shall be acceptable by the contracting authority or required from it, including allowing for any unexpected, unforeseeable or urgent replacement of the contract holder’s personnel.

7. Non-compliance or failure to abide by these security measures by the contract holder, even in cases where they result from carelessness or negligence, may result in a contractual penalty, without prejudice to criminal penalties.

ANNEX 11:
LEGAL ENTITY SECURITY FORM [152]

PART TO BE FILLED IN BY THE CLEARANCE AUTHORITY

Company name	**Company Trade Registration no.**

Initial	**Re-examination**	**Renewal**	**Update**

Level of facility security clearance (FSC): **- Special remarks :**

Overview of the need for security clearance of the legal entity:

In particular:
Access to classified information or information media:
- *on the premises of the company to be security cleared:* *yes - no*
- *only at the premises of the client / contractor:* *yes - no*

Possession of classified documents / media:
- *on the premises of the company to be security cleared:* *yes - no*
- *only at the premises of the client / contractor:* *yes - no*

Public Contracting Authorities:

Contractor:

Security clearance authority: **Signature of the security clearance authority:**

[152] As in the case of the 94A individual form for individuals, the sole purpose of this form is to analyze vulnerabilities regards the protection of national Defence secret entrusted to a legal entity and not to make any judgments on the said company. The State informs the companies that the information collected is intended for specialized State agencies and is not disclosed to parties outside of these services. They are considered confidential and are treated accordingly.

DOCUMENTS TO BE PROVIDED WITH THE FORM

PART TO BE FILLED IN BY THE LEGAL ENTITY [153]

- **Recent complete Kbis.**
- **Up-to-date articles of association.**
- **Composition of the board of governors and governing bodies (supervisory board, executive, etc.)**
- **Functional organization of the company (including members who do not have the power to bind the company)**
- **Organizational chart positioning the company in the group.**
- **List of principal debts by origin (loans from banks, etc).**
- **Company presentation booklet.**
- **Latest balance sheet**
- **The representatives of the legal entity shall provide a list of other boards of directors on which they sit.**
- **A 94A individual form to be completed by each official manager of the legal entity.**
- **The detailed sheet supporting the need for security clearing the company (Appendix 1)**

Note: if this is a first request, attach the proposal letter of the security officer (SO) + his individual 94A form

Company representative in charge of monitoring the security clearance request of the company:[154]

Name:	**First name:**	**Phone number:**
Fax:	**email:**	

[153] Based on a declarative principle, this form commits the company and can jeopardize its involvement in a classified procurement contract in case of proven fraud during declaration. Once cleared, the legal entity is bound to report any significant change (management, capital stock, etc.) to its clearance authority and update this form and the provided documents.

[154] The investigation services of the concerned ministry reserves the right to request any additional information pertaining to the sections in this form.

CAPITAL STOCK [155]

1ST LEVEL

Name (and first name for individuals) of the shareholder(s)	Nationalities	In case of individuals Date and place of birth	In case of legal entities Company Trade Register No.	% held	Voting rights %

2ND LEVEL OF STOCK OWNERSHIP FOR ANY SHAREHOLDER HAVING 40% AND MORE OF SHARES OF THE 1ST LEVEL

Name (and first name for individuals) of the shareholder(s)	Nationalities	In case of individuals Date and place of birth	In case of legal entities Company Trade Register No.	% held	Voting rights %

3RD LEVEL OF THE STOCK OWNERSHIP FOR ANY PM SHAREHOLDER HAVING 40% AND MORE 2ND LEVEL SHARES

Name (and first name for individuals) of the shareholder(s)	Nationalities	In case of individuals Date and place of birth	In case of legal entities Company Trade Register No.	% held	Voting rights %

[155] For unlisted companies, please provide detailed stock ownership.

RISK MANAGEMENT

Insurances (identity of brokers intervening between the company and insurance companies)
Properties:
Liability:
Operational loss risks:

Has the "Risk Manager" position or equivalent been provided for in the company?	
Yes	**No**
If yes: Name: **First name:** **Date and place of birth:** **Tel:** **If not: how does the company manage risks?**	
Person in charge of information systems security:	
Yes	**No**
If yes: Name: **First name:** **Date and place of birth:** **Tel:**	

Standards		
Quality:	**Environment:**	**Others:**

Audit/Board meetings held at the company in the last 3 years	
Yes	**No**
If yes: please list by name	

INTERNATIONAL ENVIRONMENT

LOCATIONS ABROAD: SUBSIDIARIES, ESTABLISHMENTS, ETC.

Yes		No
If yes: please list (including addresses)		

TRADE LINKS WITH FOREIGN COUNTRIES

Does the company have export contracts?	Yes	No

If yes, with which countries and for which services?

Does the company have key suppliers abroad?	Yes	No

If yes, which ones?

Does the company interact with foreign companies or organizations?	Yes	No

If yes, fill in the infra table:

Country:
Domain: (Executives – Engineers – Technicians – Sales executives etc.):

Appendix 1
JUSTIFICATION SHEET FOR SECURITY CLEARANCE NEEDS OF THE COMPANY

If the space provided in the various cases below is insufficient to give detailed answers or all required information, complete this form from the annexuress for these answers and information, marking these annnexures with the case numbers for which they are prepared (see case 9).

Logo or memorandum of the company to be cleared:
Type of security clearance requirement: Contract with possession of classified information or material at the premises of the contract holder Contract without possession of classified information or material Put an X in the box corresponding to the requirement type justifying this description sheet.
1. Objective of the contract:
2. Description (as accurately and completely as possible) of the classified works to be entrusted to the company to be security cleared:
3. Sites: a) Sites of execution of the classified works: b) Sites of storage of the classified documents / materials: c) Duration of execution or storage:
4. Classified information or documents / material to be communicated to the company: a) maximum classification level: b) type of classified material: paper software, others (to be specified):
5. Does the company possess exclusive expertise to carry out the classified works? YES NO • if YES □ description of this expertise: • if NO □ does another company possess this expertise? YES □ reason for which it is not selected or not consulted: NO

6. Provisional date for contract notification or making the classified information or documents / material available:
7. If the contract is a sub-contracting contract, specify the following elements pertaining to the contract that it results from directly: a) objective: b) identification number and notification date: c) identification number and date of approval of the security aspects letter:
8. Consequences (operational, schedule-related, financial, technical etc.) if the company: a) is not security cleared on the provisional date mentioned in case 6: b) cannot be security cleared:
9. Annexures to this security clearance request: YES NO If YES, specify the number of the cases with an annexure:

I, undersigned (surname and first name):
…..……..…
(title or post):……..…….
……..……...
from (organisation or company requiring the security
clearance)……..…
…….……..
certify the reality of the need and accuracy of the justifications and information contained in this security clearance request.

Date and signature

Appendix 2

List of the constitutive elements of the facility aptitude file for the execution of a contract with storage of classified information or materials

1/ Documents to be provided by the company to be security cleared (information on the places of execution of classified works):

- valid abstract of the trade and companies register (model L bis) or copy of the commercial lease;
- functional organization chart and list of names;
- personal security notice 94/A (model 01 of the present directive) and letter of proposal for each likely security officer;
- detailed map of the facility;
- organization and means of protection and gardening of the facility;
- identification and description of the protection, current or envisaged, of the premises where the protected works are executed;
- information systems security file;
- list of subcontractors working within the facility, bringing out the service provider companies having a classified or a sensitive contract;
- letter from the company head, in which he commits to put in place, before the start of the protected works, the provisions necessary to guarantee the protection of classified information or materials entrusted to him.

2/ Document prepared by the contracting authority or the contractor (in addition to the definition and justification of the need-to-know):

- security aspects letter or draft security aspects letter.

ANNEX 12:
Models of
certificate of compliance
and
certificate of compliance with norms

Model A

CERTIFICATE OF COMPLIANCE
□ PHYSICAL
□ PHYSICAL AND ELECTRONIC

I, (name, first name and function of the person binding the corporation)

……
……

hereby certify that the premises where classified information and material will be received, handled, utilized, stored and transmitted within my company (name of the company) for the establishments mentioned below:

……
……
……..……
……

in the execution of the following contract(s):

……

within the legal and regulatory terms of protection for secrecy protection and in particular with respect to the Titles IV and V of the general inter-ministerial directive no.1300 on the protection of national defence secret.

The premises were verified by the investigating service on (date) and a technical notification was given (*state the references of the notifications*): ...……

Place Date

Signature

Model B

SECURITY STANDARDS UPDATE CERTIFICATE

□ PHYSICAL

□ PHYSICAL AND ELECTRONIC

I, (name, first name and function of the person binding the corporation)

……
……

hereby certify that the premises where classified information and material will be received, handled, developed, stored and transmitted within my company (name of the company) for the establishments mentioned below:

……
……

……

……

in the execution of the following contract(s):

……..

……

……

following the verification of the premises by the investigating service on the (date) resulting in a technical notification *(provide the references of the notification)* ……., have been updated and are within the legal and regulatory terms of protection for secret protection and in particular with respect to the Titles IV and V of the general inter-ministerial directive no.1300 on the protection of national defence secret.

Place Date

Signature

ANNEX 13:
Instructions related to the Security aspects letters

The Security Aspect Letter (SAL) covers the following:

- the commitment made by the contract holder to ensure that individuals needing access to classified information in the exercise of their functions have the appropriate security clearance;
- the commitment made by the contractor to ensure that all persons who have access to classified information or material are informed of their responsibility to protect the information in question as required by the relevant laws and regulations;
- the commitment to report any actual or supposed infringement of laws and regulations pertaining to the protection of classified information under the contract;
- the competent authorities in charge of coordinating the protection of classified information or material under the contract;
- the premises where the contract must be executed, the list of which may evolve;
- the list of classified information or material, their respective classification level and the protection conditions of each piece of information in accordance with the instructions in the general inter-ministerial directive no.1300 related to the protection of national defence secret and the procedure to communicate changes in the classification level;
- special security measures that must be taken in the execution of this contract to ensure the protection of classified information or material;
- modes of communication and means of electronic transmission;
- identification of subcontractors;
- the arrangements for communicating classified information to sub-contractors;
- the procedure for transmission of classified information;
- arrangements for the provisional management of classified information or material once the contract is completed.

A copy of the SAL is sent to the investigating service in charge of monitoring the company.

Models of notices, forms and administrative decisions

- Shuttle file between the contracting authority or the adjudicator and the investigating services relating to an opinion on a company for the execution of a sensitive contract (Model 17/IGI 1300)

PERSONAL AND CONFIDENTIAL

cerfa
N°14127*01

INDIVIDUAL SECURITY FORM (Model 94 A)

(Model 01/IGI 1300)

Identification photograph

full-face

less than 1 year old

ZONE RESERVED FOR THE APPLYING ORGANISATION

APPLYING ORGANISATION:

TYPE OF SECURITY CLEARANCE PROCEDURE REQUESTED (Tick one of the 3 boxes)

ADMISSION ☐ *RENEWAL* ☐ *REVISION* ☐

SECURITY CLEARANCE : TRES SECRET ☐ ***SECRET*** ☐ ***CONFIDENTIEL*** ☐

DECIDING AUTHORITY TO WHOM THE SECURITY NOTICE IS TO BE SENT :

STAMP OF THE OF THE APPLYING ORGANISATION AUTHORITY ***Date*** ***SIGNATURE OF THE AUTHORITY***

NAME, FUNCTION:

CANDIDATE REQUESTING SECURITY CLEARANCE

NAME (maiden name followed by name of spouse X... for married women) (IN CAPITAL LETTERS) *SEX* *M* ☐ *F* ☐ *DATE OF BIRTH*

FIRST NAMES (UNDERLINE THE USUAL FIRST NAME)	*NICKNAME OR ALIAS*		
PLACE OF BIRTH	*POSTAL CODE*	*COUNTRY*	
NATIONALITY(IES) ACQUIRED AT BIRTH	*CURRENTLY HELD NATIONALITY(IES)*		
YEAR OF ACQUIRING THE FRENCH NATIONALITY	*YEAR OF ARRIVAL in FRANCE*	*COUNTRY OF ORIGIN*	
COMPLETE ADDRESS OF THE CURRENT RESIDENCE (N °, STREET, TOWN) (1)	*POSTAL CODE*	*FROM*	*Phone ° numbers*
COMPLETE ADDRESS OF THE PREVIOUS RESIDENCE (IF THE ADDRESS IS LESS THAN 6 MONTHS OLD)	*POSTAL CODE*	*FROM:* *TO:*	
COMPLETE ADDRESS OF THE OCCASIONAL OR SECONDARY RESIDENCE (including abroad) (1)	*POSTAL CODE*	*FROM*	*email*

CURRENT PROFESSIONAL STATUS

CIVIL ☐	*POST - PROFESSION*	*MILITARY* ☐	*GRADE - POST*	*ARMY / ARMED CORPS OFBEBELONGING BELONGING*
MINISTRY OF ORIGIN	*MINISTRY OF EMPLOYMENT*			
ASSIGNED ORGANISATION				*FROM*
PROFESSIONAL ADDRESS				*PROFESSIONAL TELEPHONE NUMBER°* *E .MAIL -*

SUCCESSIVE JOBS IN THE LAST 5 YEARS (1)			
EMPLOYED BY INSTITUTION OR ORGANISATION (N°, STREET, TOWN) (COUNTRY IF ABROAD)	*JOB OR POST (e.g. : secretary, etc.)*	*PERIOD*	*POSTAL CODE*

LEVEL OF SECURITY CLEARANCE ALREADY OBTAINED: *DATE :*

(1) Use the "Additional information"space in page 4 if NECESSARY

LEVEL OF EDUCATION AND GENERAL KNOWLEDGE		
DEGREES OBTAINED OR EQUIVALENCES	*FOREIGN LANGUAGES*	*LEVEL OF KNOWLEDGE*

CURRENT MARITAL STATUS

Single	*Engaged to be married*	*Married*	*Widower/widow*	*Separated*	*Divorced*	*Engaged to be remarried*	*Remarried*	*common-law marriage*	*PACS*	*Other Situation**	*Number of children*
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

DATE AND PLACE OF WEDDING OR OF THE PRESENT SITUATION (*) OR DETAILS OF THE CURRENT SITUATION (be there common-law marriage or not)

ADMINISTRATIVE DOCUMENTS

NATIONAL IDENTITY CARD	*NUMBER*	*DATE OF DELIVERY*	*DELIVERING AUTHORITY*
PASSPORT(S) (Specify whether private, official or diplomatic)	*NUMBER*	*DATE OF DELIVERY*	*DELIVERING AUTHORITY*

TRIPS AND STAYS ABROAD DURING THE LAST 5 YEARS, STARTING BY THE MOST RECENT (1)

COUNTRY AND ADDRESS IN CASE OF STAY EXCEEDING 6 MONTHS	*YEARS*	MONTHS	*REASONS (professional / family / tourism)*

CHILDREN (1)

Surnames and first names	*Sex*	*Date of birth*	*Place of birth*	*Nationality*	*Different residence if any*

	FATHER OF THE CANDIDATE	MOTHER OF THE CANDIDATE
NAME - FIRST NAME (maiden name for the mother)		
DATE AND PLACE OF BIRTH (with postal code)		
NATIONALITY AT BIRTH / CURRENT NATIONALITY		
DATE OF ARRIVAL in FRANCE / COUNTRY OF ORIGIN		
YEAR OF ACQUIRING THE FRENCH NATIONALITY		
COMPLETE ADDRESS OF THE CURRENT RESIDENCE (WITH POSTAL CODE) OR LAST RESIDENCE IN CASE OF DEATH (AND DATE OF THE LATTER)		
NUMBER OF THE NATIONAL IDENTITYCARD OR PASSPORT		
NAME AND ADDRESS OF THE PREVIOUS EMPLOYER		

(1) Use the space “Additional information” in page 4 if required.

.

Spouse* :

*person mentioned in the previous page (in current family status)

NAME (maiden name followed by name of spouse X... for married women) (IN CAPITAL LETTERS)	SEX	M ☐	F ☐	DATE OF BIRTH

FIRST NAMES (UNDERLINE THE USUAL FIRST NAME)	NICKNAME OR ALIAS

PLACE OF BIRTH	POSTAL CODE	COUNTRY

NATIONALITY(IES) ACQUIRED AT BIRTH	CURRENTLY HELD NATIONALITY(IES)

YEAR OF ACQUIRING THE FRENCH NATIONALITY	YEAR OF ARRIVAL IN FRANCE	COUNTRY OFORIGIN

COMPLETE ADDRESS OF CURRENT RESIDENCE IF DIFFERENT FROM THAT OF THE CANDIDATE (N°, STREET, TOWN) (1)	POSTAL CODE	FROM	Phone numbers* - email

COMPLETE ADDRESS OF OCCASIONAL OR SECONDARY RESIDENCE (including abroad) (1) IF DIFFERENT FROM THAT OF THE CANDIDATE	POSTAL CODE	FROM	Phone numbers* - email

ADMINISTRATIVE DOCUMENTS

NATIONAL IDENTITYCARD	NUMBER	DATE OF DELIVERY	DELIVERING AUTHORITY
PASSPORT(S)°(Specify private, official or diplomatic)	NUMBER	DATE OF DELIVERY	DELIVERING AUTHORITY

LEVEL OF EDUCATION AND GENERAL KNOWLEDGE

DEGREES OBTAINED OR EQUIVALENCES	FOREIGN LANGUAGES	KNOWLEDGE LEVEL

CURRENT PROFESSIONAL STATUS

CIVIL ☐ POST PROFESSION	MILITARY ☐ GRADE - POST	ARMY / ARMED CORPS

MINISTRY OF ORIGIN	MINISTRY OF EMPLOYMENT

ASSIGNED ORGANISATION	FROM

PROFESSIONAL ADDRESS	PROFESSIONAL TELEPHONE NUMBER° E .MAIL -

TRIPS AND STAYS ABROAD IN THE LAST 5 YEARS STARTING BY THE MOST RECENT (1)

COUNTRY AND ADDRESS IN CASE OF STAY EXCEEDING 6 MONTHS	YEARS	REASONS (professional / family / tourism)

CHILDREN (mention only children from a previous union)

Surnames and first names	Sex	Date of Birth	Place of birth	Postal code	Nationality	Different residence if any

	FATHER OF THE SPOUSE	MOTHER OF THE SPOUSE
SURNAME - FIRST NAME (maiden name for the mother)		
DATE AND PLACE OF BIRTH (with postal code)		
NATIONALITY BY BIRTH / CURRENT NATIONALITY		

DATE OF ARRIVAL in FRANCE / COUNTRY OF ORIGIN		
YEAR OF ACQUIRING THE FRENCH NATIONALITY		
NUMBER OF THE NATIONAL IDENTITY CARD OR PASSPORT		
COMPLETE ADDRESS OF THE CURRENT RESIDENCE (WITH POSTAL CODE) OR LAST RESIDENCE IN CASE OF DEATH (AND DATE OF THE LATTER)		
NAME AND ADDRESS OF THE PREVIOUS EMPLOYER		

SECURITY INFORMATION

Answer by **YES** or **NO** to the following questions:

1) Do you think that yourself as well as your spouse or partner:

a) have been asked to provide sensitive information outside of your professional capabilities?

b) have you or members of your family been under pressure following an incident that took place in a foreign land?

c) have you been approached by members of a foreign information service office or security office?

If you answer YES to any of the questions above, please describe the circumstances.

2) Do you have close relatives residing overseas or do you maintain professional or private relations with foreign residents?

If your response to the above question is YES, please identify the persons concerned (name, date and place of birth, nationality).

3) Do you wish to bring a particular issue with the department in charge examining this dossier?

ADDITIONAL INFORMATION (if (in) any)

Specify the names of other persons living under the same roof: Name - First name – Place and date of birth – Nationality – nature or level of kinship

STATEMENT

I, (name, first name): _____

a) Certify that I have been informed of the definition of the security clearance for which I am applying, and of its scope. It has thus been indicated to me that the decision of security clearance, if favorable, grants me access to classified information or material at the level specified in this decision as well as at lower level(s), based a need to know principle. It has also been specified to me that the present request for security clearance triggers a procedure that is meant to verify whether it is possible for me to have access to classified information or material in the execution of my tasks, without any national security or personal risk.

b) Certify that I have been informed:

- of the mandatory nature of answers expected from me;
- that in absence of a response to the questions asked, no security clearance decision will be taken;
- that I have a right to access and rectification, by application of articles 34 and those following of the no. 78-17 dated January 6, 1978 law relative to computers, files and liberties.

c) Certify the correctness of the information that I have provided in the present notice and admit to having been informed that I will be subject, in case of fraudulent alteration of the truth, to 3 years of imprisonment and a fine of €45,000, by application of the prescriptions of article 441-1 of the Criminal Code;

d) Declare that I have also been informed that by virtue of the legislative and regulatory prescriptions related to protection of secrets, the security clearance to which I have applied binds my responsibility and induces obligations on my behalf, of which:

- guaranteeing the security of classified information or material to which I could have access, by strictly adhering to the applicable regulations;
- be accountable, legally and administratively, for any acts of malice, imprudence, negligence or carelessness resulting in the destruction, misappropriation, removal, reproduction or making public by an unqualified person of the contents of any classified information or material that I may have access to or hold in my possession[156].

PLACE	DATE	SIGNATURE

[156] Art. 413-10 of the Criminal Code, punishing the offence of compromising national Defence secret.

Ministry
Requesting organization
(stamp)
N° . . . /

SECURITY CLEARANCE REQUEST[157]

- Renewal[158]

(Mle 02/IGI 1300)

Level [159] of classified information or material: . . . . . .

Personal information:
- Name[160] and first name: . . . . . .
- Date and place of birth: . . . . . .

Professional information:
- Grade or title: . . . . . .
- Function and duties performed: . . . . . .
. . . . . .
- Security clearances previously obtained [161](if applicable): . . . . . .
. . ..

Grounds for security clearance:

The post to be occupied appears at post n°. . . . in the catalogue of positions in my organization requiring an security clearance decision.

The emergency procedure [162] must be activated for the following reasons:
. . . . . .
. . . . . .

Date . . . . . , Place . . . . . .
Name, designation, signature of the competent hierarchal authority and seal of the organization

Stamp (*name and signature*) of the security officer, the security official or the head of the requesting office, or of the information control office of the NATO, the EU and seal of the organization Place . . . . . , Date	Stamp (name and signature) of the central security officer or of the head of the main or isolated office for NATO, EU information and seal of the organization. Place . . . . . , Date. . . . .

[157] Attach three Mle 01/GI 1300 forms (of which one original) and three identity photographs; place a request for each classification.
[158] Delete as appropriate.
[159] For the Très-Secret level, indicate the classification level and, if necessary, the categories.
[160] Maiden name for married women, followed by the formulation "marital name X".
[161] Attach the Mle 07/IGI 1300 statement in case of a change of assignment.
[162] Usable in exceptional cases and for justifiable emergency.

Ministry
Requesting organization
(stamp)
N° . . . . . /

REQUEST FOR BASIC VERIFICATION

(Mle 03/IGI 1300)

Personal information:

- Name[163] and first name: . . . .

- Date and place of birth: . . . .

- Nationality at birth: . . . .

- Current nationality (*in case of dual nationality, please specify):* . . . .
. . . . . .
- Current place of residence: . . . . . .
. . . . . .
- Earlier place(s) of residence (*if there has been a change in less than five years*): . . . . . .
. . . . . .

Professional information:

- Grade or title: . . . . . .
. . . . . .
- Function and duties performed: . . . . . .
. . . . . .
- Expiry date of the current elementary verification *(if required)*:
. . . . . .

If need be, the level of classification of information or material[164] to which the applicant could have access (without being security cleared to take cognizance of the same):

- Confidentiel Défense or Secret Défense.

Place . . . . . , Date . . . . . .

Name, designation, signature of the competent authority[165]
and seal of the organization

[163] Maiden name for married women, followed by the formulation “marital name X”.
[164] Delete as appropriate.
[165] Decision-making authority having received delegation of authority to that effect.

Ministry
Employer organization
(stamp)
N° /

DECISION OF SECURITY CLEARANCE
to classified information or material
(Mle 04/IGI 1300)

The[166] . . . . . .

decides that

Mr or Mrs: . . . . . .
(*NAME and first name*)

Date of birth **:** . . . . . , Place of birth: . . . . . .

Grade or title **:** . . . . . .

Positions held: . . . .

is security cleared to classified information or material up to and including:

- SECRET DÉFENSE

- CONFIDENTIEL DÉFENSE

This decision is valid until [167] : . . . .

Place . . . . . Date. . . . . .

Name, designation, signature of the competent authority [168]
and seal of the organization

[166] Competent authority.
[167] Date of expiry of the decision.
[168] Decision-making authority having received delegation of authority to that effect.

Ministry
Employer organization
(stamp)
N° /

SECURITY ESCORT DECISION

(Mle 05/IGI 1300)

The [169]. . . . . .

decides that

Mr or Mrs: . . . . . .
(*NAME and first name*)

Date of birth **:** . . . . . , Place of birth: . . . . . .

Grade or title **:** . . . . . .

Positions held: . . . . . .

is authorised to **(1) classified material up to and including[170] :**
(peut effectuer le convoyage(1) de supports classifiés jusques et y compris)

- SECRET DÉFENSE

- CONFIDENTIEL DÉFENSE

This decision is valid until [171] : . . . . . .

Date . . . . . Place. . . . . .

Name, designation, signature of the competent authority [172]
and seal of the organization

[169] Competent authority.
[170] Delete as appropriate.
[171] Date of expiry of the decision.
[172] Decision-making authority having received delegation of authority to that effect.

Ministry
Employer organization
(stamp)
N° /

SECURITY CERTIFICATE[173]

(Mle 07/IGI 1300)

Delivered by (*Ministry, organization*): . . . . . .
. . . . . .
Date and place of issue: . . . . . .

Number: . . . . . Valid until: . . . . . .

Objective / mission: . . . . . .

It is hereby certified by the present document that Mr. or Mrs.

NAME and first name : . . . . . .

Grade and duties : . . . . . .

Date and place of birth: . . . . . .

Holder of passport / identity card no.: . . . . . .

Issued at: . . . . . dated: . . . . . .

has been the subject of a security clearance procedure from: . . . . . to: . . . .

for accessing classified information or material at the level[174] **:** . . . .

In compliance with the prescriptions of the Inter-ministerial directive no. 1300 on the protection of national defence secrets
or
In compliance with the prescriptions of the Inter-ministerial instruction no. 2100 for the application in France of the NATO security system [175]
Or
In compliance with the provisions of the security rules for the protection of EU classified information (2011/292/UE)

NAME, designation, signature of the authority issuing the certificate
And seal of the organization

[173] Certificate to be returned to the issuing authority, upon completion of the mission for which it was issued.
[174] Highest level of classification
[175] Delete as appropriate

LIABILITY COMMITMENT

(Mle 08/IGI 1300)

NAME and first name : . . . . . .
Grade or position : . . . . . .
Employing office : . . . . . .

- 1st part -

I hereby declare:

- having taken **cognizance** of the general inter-ministerial directive no. 1300/SGDSN on the protection of national defence secret, as well as of the Criminal Code provisions cited in the annexure of the directive;
- being fully aware of my **responsibilities** with regard to protection of national defence classified information or material.
- having been informed of the legal **consequences** (in particular articles 121-2, 411-1 to 411-11, 413-9 to 413-12 and 414-7 to 414-9 of the Criminal Code) and administrative regulations, namely in cases where deliberately or by negligence, I were to allow such classified information or material to reach non-security cleared individuals.

Consequently, **I commit not to disclose**, even after the cessation of my functions, to any non-security cleared individual(s) the classified information or material whose knowledge I would have gained during my tenure.

NAME, designation, signature of the competent authority certifying that the applicant has been informed of his/her responsibilities with regard to the protection of classified information or material.

Place. . . . . ., Date . . . . . .

Signature of applicant

I, hereby, declare that I have been informed of the decision taken on my account.

NAME, designation, signature of the competent authority certifying that the interested party has been informed of the decision taken on his account.

Date . . . . . , Place. . . . . .

Signature of applicant

- 2nd part - REMINDER

As from the date of termination of functions, for which an security clearance decision for national defence classified information or material has been accorded to me, **I commit to not to disclose** to any unsecurity cleared individual(s) any classified information or material whose knowledge I would have gained during my tenure, and to **not retain** any classified document or material.

I have been informed of the legal **consequences** (in particular articles 121-2, 411-1 to 411-11, 413-9 to 413-12 and 414-7 to 414-9 of the Criminal Code) and the administrative regulations, namely in cases where deliberately or by negligence, I were to allow such classified information or material to reach non-security cleared individual(s).

Name, designation, signature of the competent hierarchal authority certifying that the applicant has been informed of his/her responsibilities with regard to the protection of classified information or material.

Date . . . . . , Place. . . . . .

Signature of the interested party

Ministry
Employer organization
(stamp)
N . . . /

Reproduction prohibited

COURIER CERTIFICATE
(CERTIFICAT DE COURRIER)

(Mle 09/IGI 1300)

For the international carriage by security cleared escort, of CLASSIFIED DOCUMENTS/EQUIPMENT/ COMPONENTS
pour le convoiement international de DOCUMENTS/EQUIPEMENTS/COMPOSANTS CLASSIFIES

Name of the program/project
…….....……..……
Nom du programme/projet

This is to certify that the bearer, Mr/Mrs (name and title)
Il est certifié que le porteur Monsieur/Madame (nom, prénom et titre)…… ……

Born on (day/month/year) – Né(e) le (jour, mois, année)**: …… in (country) –** (en pays) **: ……**

A national of (country) – Ressortissant (pays)**:……**

Holder of passport/identity card n° - Titulaire du passeport ou de la carte d'identité n°**……...**

Issued by (issuing authority):…… **on (day, month, year):**…….
Délivré(e) par (autorité) le (jour, mois, année)

And employed with (company or organisation) :…… ……...
Et employé(e) par (société ou organisme)

Is security cleared to carry on the journey detailed below with the following consignment: (number, weight and dimensions of each package)
Est autorisé(e) à effectuer le voyage décrit ci-dessous avec l'envoi suivant: (indiquer n° des paquets, poids et dimensions de chaque colis)

……
……
……

Itinerary: departure on (date) :...….....….....**from (country) :** ...….....….....**to (country)** :...….....….....
Itinéraire: départ le (date): de (pays) à (pays)

through (countries): ….....……..

Via (pays traversés)

Anticipated return (date)– Retour prévu le (date)**:** …….....

The attention of Customs, Police, and/or Immigration Officials is drawn to the points stated on the back of this certificate.

L'attention des autorités des douanes, de police ou des services d'immigration est attirée sur les points indiqués au dos de ce certificat.

Company security officer ***Officier de sécurité de la société ou de l'établissement*** (Stamp and signature) (Cachet ou timbre et signature) **Date :**	*Designed Security Authority* ***Autorité de sécurité déléguée*** (Stamp and signature) (Cachet ou timbre et signature) **Date :**

The Notice of Customs, Police, and/or Immigration Officials is drawn to the following:
L'attention des autorités des douanes, de police et/ou des services d'immigration est attirée sur les points suivants:

- The material comprising this consignment is classified in the interests of national security of the countries here above;
  Le contenu de cet envoi est classifié dans l'intérêt de la sécurité nationale des pays cités ci-dessus;

- It is requested that the consignment will not be inspected by other than properly security cleared individuals or those having special Permission;
  Il est demandé que l'envoi ne soit inspecté que par des personnes dûment autorisées ou titulaires dune autorisation spéciale ;

- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of individuals who do not have a need to know and in the presence of the courier;
  Si une inspection est jugée nécessaire, il est demandé quelle soit effectuée dans une zone hors de vue des personnes qui nont pas une nécessité daccès aux informations et en présence du courrier ;

- It is requested that the package, if opened for inspection, be marked after reclosing to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened;
  Il est demandé que le paquet sil a été ouvert pour inspection, soit muni, après avoir été refermé, de la preuve de cette ouverture, par signature et cachet et par annotation des documents d'expédition (sil y en a) attestant l'ouverture de l'envoi ;

- Customs, Police, and/or Immigration officials of countries to be crossed, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.
  Les fonctionnaires des douanes, de la police et /ou des services d'immigration des pays traversés, à l'entrée ou à la sortie, sont priés d'apporter leur assistance en cas de besoin afin que l'envoi soit amené à destination en toute sécurité.

Annex to courier certificate no.

INSTRUCTIONS FOR THE ATTENTION OF THE AUTHORISED ESCORT

Annex to mission . . . . . for international transportation
by authorised escort, of classified documents, equipment and/or components

You have been designated as the escort for a classified package. A "courier certificate" has been delivered to you. Before starting out, you will be informed of security regulations relating to the transportation of classified shipments, and your security obligations during such a trip (behavior to be adopted, itinerary, schedule, etc.) You will also be asked to sign a declaration certifying that you have read and understood these security obligations and that you comply with them.

Your attention is drawn to the following general points:

1. You will be responsible for the transportation of the shipment described in the courier certificate.
2. During the entire trip, this classified shipment must remain in your possession and under your direct supervision.
3. The shipment must not be opened along the way, except under circumstances described in paragraph 10 below.
4. You must neither speak of the classified shipment nor display it in a public place.
5. This classified shipment must not, in any circumstance, be left unsupervised during night-time halts. Military installations or industrial companies having appropriate security clearances can be used. In this respect, you will be guided by the Security Officer of your company or organization.
6. While escorting a classified shipment, any deviation from the provided route is forbidden.
7. In case of emergency, you must take the necessary measures for the protection of the package, but in no circumstance must the shipment leave your care; to this end, your instructions specify how to establish contact with security organizations in the countries through which you will be transiting (see paragraph 12 below). If these instructions have not been given to you, request them from the Security Officer of your company or organization.
8. It is your responsibility and that of the Security Officer of your company or organization to ensure that the documents necessary for your exit from the territory and your travel (passport, exchange certificates, health booklet, etc.) are complete and valid.
9. If unforeseen circumstances require that you place the shipment in the hands of individuals other than representatives designated by the company or the government that you have to make contact with, you will hand it over only to security cleared officials of one of the contact points listed in paragraph 12.
10. You will not be granted any immunity with regard to verifications carried out by the customs, police and/or immigration services of the different countries whose borders you will cross. Hence, in case you are asked to reveal the contents of the shipment, you will show them the "courier certificate" and the present note and you will insist on presenting them to the head of the customs services, head of police and/or immigration in person; this approach must normally suffice to get the shipment through without having to open it. However, if the head of the customs services, head of police and/or immigration ask to see the contents of the shipment, you may open it, provided that it is done out of sight from other individuals.

    You must take precautions not to display the entire contents of the shipment but only a part of it to the officer so as to convince him that the shipment contains no other object, and you will ask him to close the shipment or help you to close it immediately after having conducted the inspection.

You will ask the head of customs services, police and/or immigration to provide you with proof that the shipment was opened and inspected by affixing his signature and seal on the shipment after closure and by confirming on the back of the inventory list that the shipment was opened.

If you have been asked to open the shipment in the circumstances described above, you must make it known to the Security Officer of the recipient company or organization and the Security Officer of the company or organization sending the package, who in turn must inform the security authorities concerned in their respective governments (National Security Authority / Delegated Security Authority).

11. Upon your return, you must produce an acknowledgement of receipt of the shipment signed by the Security Officer of the company having received the delivery or signed by a competent security authority of the recipient government.

12. During your journey, you may enter in contact with the authorities mentioned below in order to seek their assistance: .....

.....

.....

.....

Annex to courier certificate N°

STATEMENT OF THE AUTHORISED ESCORT

Mr./ Mrs. (name, first name): ...….....….....

from (name of the company or organization):

Function in the company or organization: …….....….…

STATEMENT:

The Security Officer (name of the company or organization):

gave me the notes relative to the handling and custody of the classified documents/equipment which I must carry. I have read and understood them.

I shall keep these classified documents/equipment in my possession throughout the trip and will not open the shipment unless it is required by customs authorities.

On my arrival, I will submit to the designated recipient, against signature on an acknowledgement of receipt, these classified documents/equipment meant for the recipient company/organization.

Place: ……..... , Date: …….

Signature of the courier: …….……..

In the presence of the Security Officer (name, first name and signature):

Annex to courier certificate no.

AUTHORISED ROUTE

Details of the itinerary:
Details d'itineraire :

Departure on (date): ...….....….....
Départ le (date)

From (country): ...….....….....
De (pays)

To (country): ...….....….....
A (pays)

Through (countries): …….....……..….
Via (pays traversés)

Security cleared stops (countries):
…….....……..….
Arrêts autorisés (pays)

Anticipated return (date) – Retour prévu le (date) **:** …….....

References of receipt or inventory list – Références du bordereau d'envoi ou du récépissé **:** …….....

Report to be filled in and signed at the end of the trip:

I solemnly declare that during the trip corresponding to the present description, to my knowledge, no event or act occurred, of my doing or that of others, that would compromise the security of the shipment, except for the elements noted below, if applicable:

Prepared at (place): ……... , on (date): ……. Signature of courier: ….……..

In the presence of the Security Officer (name, first name and signature):

MULTI-TRAVELS COURIER CERTIFICATE
(*CERTIFICAT DE COURRIER MULTIVOYAGES*)

(Mle 09 bis/IGI 1300)

for international carriage of classified DOCUMENTS, EQUIPEMENTS AND/OR COMPONENTS
pour le convoiement international par convoyeur autorisé de DOCUMENTS/EQUIPEMENTS/COMPOSANTS CLASSIFIES

For the international carriage by security cleared escort, of CLASSIFIED DOCUMENTS/EQUIPMENT/ COMPONENTS
pour le convoiement international de DOCUMENTS/EQUIPEMENTS/COMPOSANTS CLASSIFIES

Name of the program/project ……..……..……
Nom du programme/projet

This is to certify that the bearer, Mr/Mrs (name and title) ……
Il est certifié que le porteur Monsieur/Madame (nom, prénom et titre)

Born on (day/month/year) – Né(e) le (jour, mois, année)**: …… in (country) –** en pays) **: ……**

A national of (country) – Ressortissant (pays)**:……**

Holder of passport/identity card n° - Titulaire du passeport ou de la carte didentité n°**……...**

Issued by (issuing authority):…… **on (day, month, year):**…….
Délivré(e) par (autorité) le (jour, mois, année)

And employed with (company or organisation) :…… …..……...
Et employé(e) par (société ou organisme)

Is security cleared to carry classified documents, equipments and components between the following countries :
Est autorisé(e) à transporter des documents, équipements et matériels classifies entre les pays suivants :

……

The bearer above is security cleared to use the present certificate as many times as necessary, for classified shipments between the countries here above until (validity date): .....
Le porteur ci-dessus est autorisé à utiliser le présent certificat autant que de besoin, pour des transports classifiés entre les pays ci-dessus jusqu'au (date de validité):

Each sending is attached with a description of shipment.
Chaque envoi est accompagné d'un descriptif de transport.

The attention of Customs, Police, and/or Immigration Officials is drawn to the points stated on the back of this certificate.
L'attention des autorités des douanes, de police ou des services dimmigration est attirée sur les points indiqués au dos de ce certificat.

Company security officer	***Designed Security Authority***
Officier de sécurité de la société ou de l'établissement	***Autorité de sécurité déléguée***
(Stamp and signature) (Cachet ou timbre et signature)	(Stamp and signature) (Cachet ou timbre et signature)
Date :	**Date :**

The attention of Customs, Police, and/or Immigration Officials is drawn to the following:

L'attention des autorités des douanes, de police et/ou des services d'immigration est attirée sur les points suivants:

- The material comprising this consignment is classified in the interests of national security of the countries here above;
  Le contenu de cet envoi est classifié dans l'intérêt de la sécurité nationale des pays cités ci-dessus;

- It is requested that the consignment will not be inspected by other than properly security cleared individuals or those having special permission.
  Il est demandé que l'envoi ne soit inspecté que par des personnes dûment autorisées ou titulaires d'une autorisation special.

- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a need to know and in the presence of the courier.
  Si une inspection est jugée nécessaire, il est demandé quelle soit effectuée dans une zone hors de vue des personnes qui nont pas une nécessité daccès aux informations et en présence du courier.

- It is requested that the package, if opened for inspection, be marked after reclosing to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.
  Il est demandé que le paquet sil a été ouvert pour inspection, soit muni, après avoir été refermé, de la preuve de cette ouverture, par signature et cachet et par annotation des documents dexpédition (sil y en a) attestant louverture de lenvoi.

- Customs, Police, and/or Immigration officials of countries to be transmitted, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.
  Les fonctionnaires des douanes, de la police et /ou des services dimmigration des pays traversés, à lentrée ou à la sortie, sont priés dapporter leur assistance en cas de besoin afin que lenvoi soit amené à destination en toute sécurité.

Annexure to multi-travel courier certificate no.

INSTRUCTIONS FOR THE ATTENTION OF THE AUTHORISED ESCORT

Annexure to mission . . . . . for international transportation

by authorised escort of classified documents, equipment and/or components

You have been designated as the escort for a classified package. A "courier certificate" has been delivered to you. Before the beginning of travel, you will be informed of the regulations related to the security of the classified shipment and of your obligations in terms of security during the said travel (behavior to be adopted, itinerary, timing, etc.). You will also be asked to sign a declaration certifying that you have read and understood the security-related obligations and that you will comply with them.

Your attention is drawn to the following general points:

1. You will be responsible for the transportation of the shipment described in the courier certificate.
2. During the entire trip, this classified shipment must remain in your possession and under your direct supervision.
3. The shipment must not be opened along the way, except under circumstances described in paragraph 10 below.
4. You must neither speak of the classified shipment nor display it in a public place.
5. This classified shipment must not, in any circumstance, be left unsupervised during night-time halts. Military installations or industrial companies having appropriate security clearances can be used. In this respect, you will be guided by the Security Officer of your company or organization.
6. While escorting a classified shipment, any deviation from the provided route is forbidden.
7. In case of emergency, you must take the necessary measures for the protection of the package, but in no circumstance must the shipment leave your care; to this end, your instructions specify how to establish contact with security organizations in the countries through which you will be transiting (see paragraph 12 below). If these instructions have not been given to you, request them from the Security Officer of your company or organization.
8. It is your responsibility and that of the Security Officer of your company or organization to ensure that the documents necessary for your exit from the territory and your travel (passport, exchange certificates, health booklet, etc.) are complete and valid.
9. If unforeseen circumstances require that you place the shipment in the hands of individuals other than representatives designated by the company or the government that you have to make contact with, you will hand it over only to security cleared officials of one of the contact points listed in paragraph 12.
10. You will not be granted any immunity with regard to verifications carried out by the customs, police and/or immigration services of the different countries whose borders you will cross. Hence, in case you are asked to reveal the contents of the shipment, you will show them the "courier certificate" and the present note and you will insist on presenting them to the head of the customs services, head of police and/or immigration in person; this approach must normally suffice to get the shipment through without having to open it. However, if the head of the customs services, head of police and/or immigration ask to see the contents of the shipment, you may open it, provided that it is done out of sight from other individuals.

    You must take precautions not to display the entire contents of the shipment but only a part of it to the officer so as to convince him that the shipment contains no other object, and you will ask him to close the shipment or help you to close it immaterialstely after having conducted the inspection.

You will ask the head of customs services, police and/or immigration to provide you with proof that the shipment was opened and inspected by affixing his signature and seal on the shipment after closure and by confirming on the back of the inventory list that the shipment was opened.

If you have been asked to open the shipment in the circumstances described above, you must make it known to the Security Officer of the recipient company or organization and the Security Officer of the company or organization sending the package, who in turn must inform the security authorities concerned in their respective governments (National Security Authority / Delegated Security Authority).

11. Upon your return, you must produce an acknowledgement of receipt of the shipment signed by the Security Officer of the company having received the delivery or signed by a competent security authority of the recipient government.

12. During your journey, you may enter in contact with the authorities mentioned below in order to seek their assistance: .....

.....

.....

.....

Annex to multi-travel courier certificate n^o^.

STATEMENT OF THE AUTHORISED ESCORT

Mr./Ms. (Name and first name): ..……....…..

from (name of the company or organization):

Function in the company or organization: ……..…

STATEMENT:

The Security Officer of (name of the company or organization):

gave me the notes relative to the handling and custody of the classified documents/equipment which I must carry. I have read and understood them.

I shall keep these classified documents/equipment in my possession throughout the trip and will not open the shipment unless it is required by customs authorities.

On my arrival, I will submit to the designated recipient, against signature on an acknowledgement of receipt, these classified documents/equipment meant for the recipient company/organization.

Place: ……………..... , Date: ………….

Signature of courier: …….……………………..
In the presence of the Security officer (full name and signature):

Annex to multi-travel courier certificate no.

DESCRIPTION OF TRANSPORT
No

Transport from (date): ..... **to (date):** ..... **bearer (name):** ....
Transport du (date) au (date) effectué par (name)

Itinerary from (country): ...…....…..... **to (country :** ...….....….....
Itinéraire de (pays) **à (pays)**

Through (countries) : ……..... **Security cleared stops (countries) :** …….....
Via (pays traversés) Arrêts autorisés (pays)

References of receipt or inventory list : …….....…..…
Références du bordereau d'envoi ou du récépissé

Description of the shipment (number of package, dimensions and, if needed weight of each package) :
Descriptif de l'envoi (nombres de paquets, dimensions et éventuellement poids de chaque paquet)

Officials you may contact to request assistance:
Coordonnées des autorités susceptibles d'être contactées en cas de besoin

Signature of Security Officer

Report to be filled in and signed at the end of travel:

I solemnly declare that during the trip corresponding to the present description, to my knowledge, no event or act occurred, of my doing or that of others, that would compromise the security of the shipment, except for the elements noted below, if applicable:

Place: ……..….... , Date: ……. Signature of courier: …….……

In the presence of the Security officer (name, first name and signature): .....

INVENTORY LIST

(Mle 10/IGI 1300)

Inventory list put together in respect of courier certificate no . . . . ./. . . . . *dated* . . . . . .*20*..

Place . . . . , Date . . . . 20..

DOCUMENTS.	
EQUIPMENT.	
COMPONENTS.	
LEVEL OF CLASSIFICATION.	

The inventory written on the back has been approved by : . . . . . .

(NAME, first name, address, Programme, project or contract manager)

Security clearance reference: . . . . . .
……
(given by the program manager for Secret Défense)

Any inspection on the back has been endorsed by: . . . .…….. . . . . .
(NAME, first name, address, Programme, project or contract manager)

Security clearance reference: . . . . . .
(given by the program manager for Secret Défense)

Authorised escort : . . . . . .
(NAME, first name and signature)

Sending Security Officer : . . . . . .
(NAME, first name and signature)

RECEIPT (1)

Date and time of shipment handover to the recipient, Date . . . . . , at . . . . (hours). . ....

Seal, stamp or official mark of the sending organization or company

NAME and function of signatory

(1) Delete as appropriate
Number of copies:
- Inventory list procedure without receipt
- Inventory list procedure with receipt
- Definitive archiving: 1 copy to sending security officer
  (last copy on return)

INVENTORY

Order number	Precise description of classified documents, equipment and/or components	Number of copies or quantity	Number of pages per document including Annexes	Total number of pages	Number of packages
	TOTAL	. . . . .		. . . . .	

AREA RESERVED IN CASE OF INSPECTION OF THE SHIPMENT(S)

- Visa and seal of the head of:

- customs

- police

- immigration services

SEAL

Ministry
Organization
(stamp)
N° . . . /

REQUEST FOR REPRODUCTION of Secret Défense classified information

(Mle 11/IGI 1300)

Information [176] concerning the classified information for which reproduction is requested:

- References:
  - registration number and stamp : . . . . . .
  - creation date : . . . . . .
- Reference of the copy from which reproduction will be made: . . . . . .

Requesting organization: . . . .
. . . . . .

Brief purpose of the request: . . . . . .
. . . . . .

Copies requested:

- Number : . . . . . .
- Numbering : . . . . . .
- circulation : . . . . . .

Place. .. . . . . , Date . . . . . .

Name, designation, signature of the authority having made the request and seal of the organization.

[176] The purpose of the information or material must not be mentioned in any case.

Ministry
Organization
(stamp)
N° . . . ./

AUTHORISATION FOR REPRODUCTION of Secret Défense classified information

(Mle 12/IGI 1300)

Security cleared reproduction of Secret Défense classified information:

- References:
  - registration number and stamp : . . . . . .
  - creation date : . . . . . .
- Reference of the copy from which reproduction will be made: . . . . . .

Requesting organization: . . . . . .

- Reference of the request: . . . . . .
  . . . . . .

authorised copies:

- Number : . . . . . .
- Numbering : . . . . . .
- Circulation : . . . . . .

Place. .. . . . . , Date . . . . . .
Name, designation, signature of the authority having made the request and seal of the organization.

Recipients:

Ministry
Organization
(stamp)

Place. . . . . , Date . . . . .
N° /

MINUTES OF DESTRUCTION
of Secret Défense classified information
(Mle 13/IGI 1300)

- Destruction date : . . . . . .
- Grade, name and function of responsible holder : . . . . . .
. . . . . .

Reference of information or material [177]	**Date**	**Category** (eventually)	**Number of copies**

We hereby certify that the classified information information listed here below has been destroyed on this day, in our presence and that of the responsible holder.

Name, function and signature of the witness

Name, function and signature of the responsible holder and seal of the organization

Copy to[178] :
- . . . . . .

[177] The references must be mentioned in the minutes in such a manner that it is impossible to modify or complete them at a later date, by adding for example, between the two mentions, the references of another document, information or materials.
[178] Authority having given the order for destruction.

Ministry
Organization
(stamp)
N° . . . ./

Place . . . . . , Date . . . . . .

SLIP A - B - B [179]
for the dispatch of Secret Défense
Confidentiel Défense[180]
classified information or material
(Mle 14/IGI 1300)

References[181]	**Date**	**Number of copies:**	**Number of Annexures**

RECIPIENT: . . . . . *Name, designation, signature of the sender and seal of the organization*
. . . . . .
. . . . . .
. . . . . .
. . . . . .

Received on: . . . . . .

Received by: . . . . . .

[179] A . To be kept by the recipient.
B : To be sent back immaterialstely to the sender after marginal note.
B' : To be retained in archives by the sender until receipt of sheet B by which it will be substituted.
[180] Delete as appropriate.
[181] Excluding the purpose which must never be mentioned.

Ministry
Organization
(stamp)
N° . . . . /

In. . . . . , on the . . . . . .

SLIP A - **B** - B [182]
for the dispatch of Secret Défense
Confidentiel Défense[183]
classified information or material
(Mle 14 A/IGI 1300)

References[184]	Date	Number of copies	Number of Annexes

RECIPIENT: . . . . . *Name, designation, signature of the sender and seal of the organization*
. . . . . .
. . . . . .
. . . . . .
. . . . . .

Received on: . . . . . .

Received by: . . . . . .
(Name, designation, signature and seal of the organization)

[182] A . To be kept by the recipient.
B : To be sent back immaterialstely to the sender after marginal note.
B' : To be retained in archives by the sender until receipt of sheet B by which it will be substituted.
[183] Delete as appropriate.
[184] Except the purpose which must never be mentioned.

Ministry
Organization
(stamp)
N° . . . . /

At . . . . . , on . . . .
. . . . .

SLIP A - B - **B**[185]
for the dispatch of Secret Défense
Confidentiel Défense[186]
classified information or material
(Mle 14 C/IGI 1300)

References[187]	**Date**	**Number of copies**	**Number of Annexures**

RECIPIENT: ……...
……
……
…….
……..

[185] To be kept in archives by the sender till receipt of sheet B by which it will be substituted.
[186] Delete as appropriate
[187] Except the purpose which must never be mentioned.

STAMP TEMPLATES[188]
for classification and protection
(Mle 15/IGI 1300)

I – Cover [189] and title page of the document

SECRET DÉFENSE

Any individual in possession of this document without the proper security clearance falls under the provisions of the Criminal Code punishing violations of national defence secrets.

CONFIDENTIEL DÉFENSE

This document can only be distributed to qualified individuals who need to know.

II – Internal pages of the document or correspondence[190]

SECRET DÉFENSE

Letters 4 mm in height and 3 mm in width; border and letters 1.5 mm thick

CONFIDENTIEL DÉFENSE

Letters 4 mm in height and 2 mm in width; border and letters of 1 mm thick

SPÉCIAL FRANCE

Letters 4 mm in height and 2 mm in width; border and letters of 1 mm thick

[188] Stamps are affixed with red indelible ink, except the Special France stamp which is affixed in blue.
[189] In the middle of the bottom of the cover.
[190] In the middle of the top and bottom of the page.

STAMP TEMPLATES
for downgrading
or
for declassification

(Mle 16/IGI 1300)

1° - <u>In order to downgrade an information or material</u>

The downgrading of SECRET DEFENSE level to CONFIDENTIEL DEFENSE level can start as from:	**To be downgraded CONFIDENTIEL DEFENSE after approval from the issuing authority**

2° - <u>In order to declassify information or material</u>

To declassify as from:	**To declassify on order from the issuing authority**

Ministry
Requesting organization
(stamp)
N° . . . /

WARNING CERTIFICATE

(Mle 17/IGI 1300)

I[191]……

…….....

hereby certify that I have been warned in the presence of

.....

against risks caused by allowing entry of [192] ……..…….....

…….

- to *Confidentiel Défense* information ☐
- to *Secret Défense* information ☐
- to *Très Secret Défense* information ☐

to national defence secret.

Place…….Date…….

[191] Name, first name, designation or function.
[192] Tick the appropriate boxes.

Ministry
Requesting organization
(stamp)
N° . . . /

PARTICULAR VIGILANCE CERTIFICATE

(Mle 18/IGI 1300)

I[193]……
…….....

hereby certify that I have been made aware in the presence of
.....

against risks caused by my entry [194]

- to *Confidentiel Défense* information ☐
- to *Secret Défense* information ☐
- to *Très Secret Défense* information ☐

I pledge to observe utmost discretion in regard to classified information that I could have known in the carrying out of my duties and to immaterialstely report to my hierarchal superiors any attempt to pressurize me.

Place…….Date …….

[193] Name, first name, designation or function.
[194] Tick the appropriate boxes.