National Security Authority

INDUSTRIAL SECURITY MANUAL

Finland

unofficial translation

draft

1 December 2011

1 Introduction

The purpose of this manual is to provide instructions for Finnish companies participating in international classified projects. An international classified project means a project launched by a public authority of another country or a foreign company, in which access to classified information may be necessary.

The advance knowledge of specific features of classified projects improves a company's prospects for participating in international projects. The objective of this manual is to provide a description of the security requirements of classified projects and thus promote the competitiveness of Finnish companies in international trade.

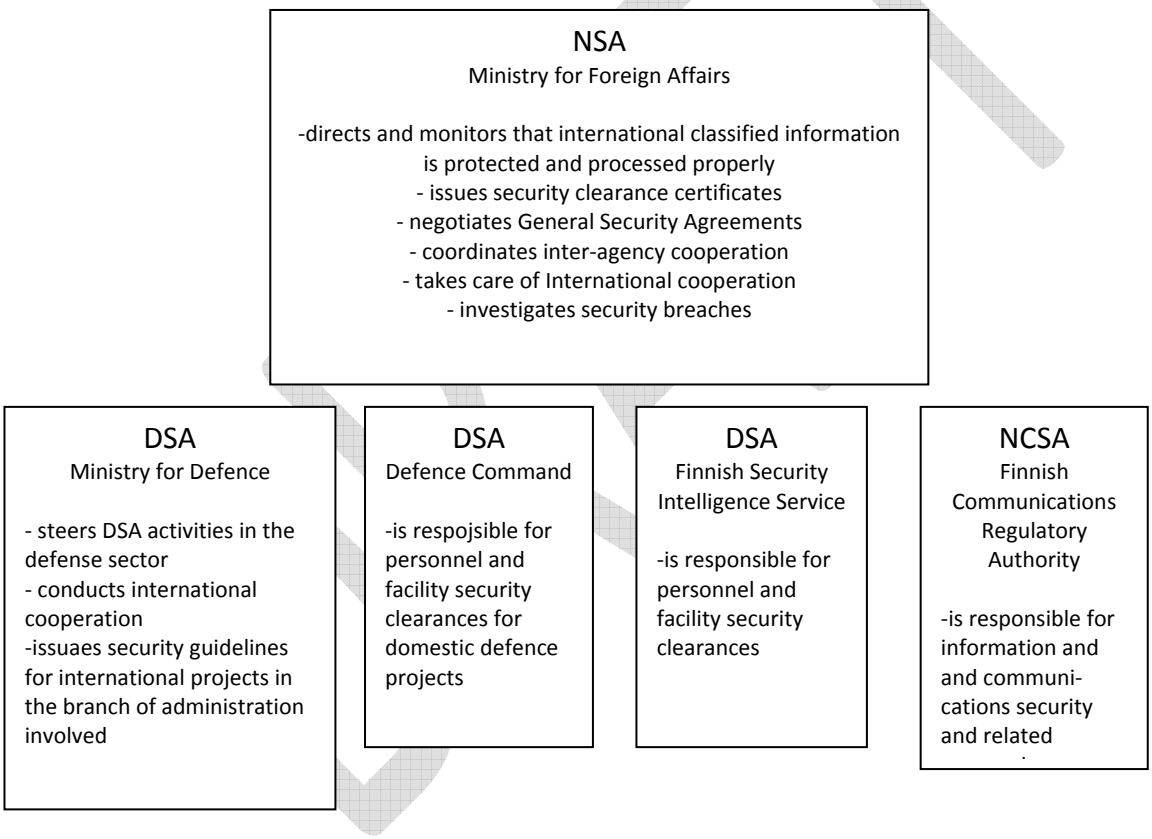
The manual serves as a tool when preparing for project negotiations and gives practical advice on the various project stages. Companies are well advised to give due consideration to the instructions provided here also in their in-house security planning, which will lower the threshold for participation in classified projects in the future.

Chapters 2 to 4 of the manual discuss the basic concepts of international projects and the activities of the security authorities. Chapters 5 and 6 address the individual types of projects and the various stages of project negotiations. Chapter 7 deals with the different aspects of security, typical security instructions issued for projects and the request for visits procedure. Chapter 8 discusses the transfer of classified information and Chapter 9 security certificates. Chapter 10 addresses the responsibilities of companies participating in classified projects.

2 Duties and organisation of the National Security Authority

2.1 Organisation of the National Security Authority in Finland

The National Security Authority (NSA) and the organisation operating under its auspices have jointly created the necessary preconditions for Finnish companies to participate in international projects in which classified information or materials are handled. Provisions on the activities of the NSA organisation and its duties are set out in the Act on international information security obligations (Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004).



2.2 National Security Authority

As provided in the Act on international information security obligations, the National Security Authority (NSA) in Finland is the Ministry for Foreign Affairs. The NSA oversees and controls that international classified information is duly protected and processed in the central government and in companies. The NSA coordinates the activities of designated security authorities, represents Finland on international security committees and working parties, and participates in the preparation of international security regulations. Additionally, the NSA concludes bilateral and multilateral general security agreements and grants Personnel and Facility Clearance Certificates (PSCCs) for the purpose of international cooperation. The NSA is also responsible for investigating breaches of information security.

2.3 Designated Security Authorities

Pursuant to the Act on international information security obligations, the Designated Security Authorities (DSA) in Finland are: the Ministry of Defence, the Defence Command, the Finnish Security Intelligence Service, and the Finnish Communications Regulatory Authority. The DSAs are responsible for the duties stipulated by law and for international information security obligations.

The Ministry of Defence is responsible for the duties of the DSA in the branch of administration and participation in international cooperation as the expert representing the NSA. Additionally, the Ministry of Defence approves the security instructions for international projects and issues guidelines for their preparation in its branch of administration.

The Defence Command conducts Personnel Security Clearances (PSCs) in the defence administration as well as Facility Security Clearances (FSCs) for domestic defence contracts.

The Finnish Security Intelligence Service is responsible for PSCs based on international obligations as well as for Finnish companies' FSCs. With defence contracts, clearance is granted by the Defence Command.

The Finnish Communications Regulatory Authority serves as the National Communications Security Authority (NCSA). The NCSA's duties include approval of data systems processing international classified information in its capacity as the Security Accreditation Authority (SAA). The approval procedure covers, for example, the systems of companies participating in international competitive bidding for which NCSA approval is required.

3 International information security obligations

3.1 Act on international information security obligations

The Act on international information security obligations lays down provisions on measures required to implement the international information security obligations. International information security obligations mean, for example, the provisions of bilateral General Security Agreements (GSAs) for the protection of classified information, i.e. documents and materials classified in accordance with the international information security obligation. Such documents include for instance classified documents of another State and EU classified documents.

The Act on International Information Security Obligations is also applied to a company and its employees when the company is party to a contract or subcontractor in a classified project, or participates in competitive bidding preceding such a contract. Consequently, the secrecy and non-disclosure obligation defined in said Act, and the prohibition to make use of confidential information are binding on the company as well.

3.2 General Security Agreements

Finland has concluded General Security Agreements with several countries and certain international organisations. The purpose of the General Security Agreements is to protect the classified information owned by States and international organisations that the parties exchange directly between themselves or between public or private legal entities or individuals under their jurisdiction. Consequently, business secrets or sensitive corporate documents are not covered by the GSAs.

The General Security Agreements contain provisions on the protection and handling of classified information, classified contracts, visits and breaches of security. They provide the basis for international classified projects and their provisions are also applicable to companies as appropriate. All security documents pertaining to the project must make reference to the General Security Agreement and must be prepared so that they are not incompatible with the provisions of the GSA.

As a rule, a General Security Agreement is required for international projects in which a Finnish company gains access to the classified information of another State. Due consideration, therefore, must be given to this at the project planning stage. In Finland, international General Security Agreements are ratified by Parliament and the obligations contained in them enforced by law. The whole process takes one to three years. Any need for such an agreement may be communicated to the NSA which will take action at its discretion. A list of the existing General Security Agreements is provided in Annex 1.

4 International cooperation

4.1 Cooperation between security authorities

In order to fulfil the information security obligations, different countries' security authorities may contact one another. Normally, cooperation is based on the provisions of a bilateral General Security Agreement on security cooperation. Such cooperation includes, among other things, granting security clearance certificates of citizens and companies of the other country; assistance with security clearances and requests for visits; the planning and supervision of classified projects; and investigating breaches of security.

In Finland, the NSA has access to the contact details of the competent security authorities of all its contracting parties. Additionally, the NSA has the full, up-to-date contact details of all EU Member States and the Members of the Multinational Industrial Security Working Group (MISWG) including international organisations' observers in their security agencies. If necessary, the network of Finnish diplomatic missions can be used as a channel of communication.

In cases where a Finnish company gains access to classified information during the course of a project, contacts between foreign security authorities are handled by the Finnish National Security Authority.

4.2 Cooperation in the EU

The Member States' NSAs participate in the preparation of the rules and guidelines for the protection of EU classified information and the security instructions relating to EU projects.

The Council's security rules[1] provide the basis for the protection of EU classified information. Additionally, the Commission, the European Parliament and the European External Action Service have their own security rules corresponding to those applied by the Council. The Council security rules contain a section on corporate security specifying minimum requirements for EU projects in which EU classified information is processed. Other security rules, such as the Commission's security rules, may be applied to individual projects on a case-by-case basis.

The equivalence of the classification markings used by Finland and by the EU, as well as the general protection requirements associated with the classifications, are presented in the NSA Guide "Instructions for handling international classified information", published in 2010.

[1] Council Decision on the security rules for the protection of EU classified information, "Council Security Rules" (2011/292/EU).

4.3 Cooperation with NATO

NATO's existing Security Policy[2] is maintained by the NATO Office of Security (NOS). Amendments are adopted by the NATO Military Committee in which all the member countries are represented.

Procurement in NATO is governed by the NATO Maintenance and Supply Agency (NAMSA) Procurement Regulations that put non-members in a weaker position because the organisation is bound to favour suppliers from its member countries. However, if the material being procured is not produced in a member country, NATO may procure the material from a non-member country.

The equivalence of the classification markings used by Finland and NATO as well as the general protection requirements associated with the classifications are presented in the NSA Guide "Instructions for handling international classified information" (Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje) published in 2010.

4.4 Cooperation with MISWG

In 1985, the key NATO countries established the Multinational Industrial Security Working Group (MISWG) to prepare best corporate security practices and to standardise procedures and general concepts in order to facilitate the activities of the international security agencies. MISWG is an unofficial and informal entity. Currently, its membership includes 39 states or organisations. Finland was invited to the Group in 2005.

MISWG has prepared a large number of jointly approved guidelines and forms that facilitate cooperation between security agencies. For example, standardised templates are used when a request is made to the public authority of another State for a Facility or Personnel Security Clearance and when a response is given. The documentation also provides descriptions of the international security instructions applied in international commercial projects.

[2] NATO Security Policy, NSP (C-M(2002)49)).

5 International Classified projects

An international classified project means a project launched by a foreign government authority, company or international organisation, in which participation may require access to classified information. A company may need access to classified information already at the bidding stage or at least when performing a classified contract related to the project.

5.1 Bilateral projects

A bilateral project means a project in which the contracting parties are a foreign procurement unit and a Finnish company. As a rule, participation in a bilateral project requires a General Security Agreement (GSA) between Finland and the host country. Under certain circumstances, the procurement unit may accept participation by the Finnish company even without a GSA.

The national security authorities of the countries involved approve the security documentation[3] related to an international project . It is only after such approval that the processing of classified information in the project may start. The national security authorities of both contracting parties control project security in the manner specified in the security documentation until the project is considered to be completed. However, completion of the project does not necessarily mean that the project-related security obligations would automatically lapse as information processed in the course of the project may continue to remain confidential and thus governed by the provisions of the project security documentation.

5.2 Multilateral projects

Multilateral projects differ from bilateral projects mainly in how the project security documentation is implemented and approved. With multilateral projects, it is often necessary to reconcile the security requirements of several participating countries. Consequently, the resulting security documentation becomes more multidimensional than in bilateral projects.

EU and NATO projects with their own specific features are governed by the in-house security regulations of these organisations.

[3] See section 7.1 for more details.

6 Phases of project negotiations

When a classified project is launched, the foreign procurement unit provides preliminary information about the project. Normally, no classified information is exchanged at this point. In the next stage, the procurement unit submits an invitation to bid together with documents specifying the security requirements for the project. The protection of classified information imposes special requirements on the company and usually increases the cost of the project. Using the information contained in the invitation to bid, the company may make an estimate of the total project costs. If the bidding documents contain classified information, it may be necessary for the proper handling of such information in accordance with the security classification that the individuals accessing the information undergo security vetting and are given a a Personnel Security Clearance (PSC). Under certain circumstances, the procurement unit may require that the company hold a Facility Security Clearance (FSC).

The Facility Security Clearance -procedure is initiated when participation in the project by the company concerned is certain, if not earlier. The standard procedure is that the NSA of the project host country or another competent security authority approaches the Finnish NSA, inquiring whether the company holds a FSC. If not, the foreign NSA or other competent security authority may ask the Finnish NSA to start the FSC procedure. Under certain circumstances, the Finnish company itself may request the FSC procedure. Any such request must be accompanied by the project documents specifying the requirement for a FSC. The NSA grants the FSC upon completion of the FSC procedure.

Finally, the company and foreign procurement unit sign the Classified Contract, which also contains the project-specific security instructions.

7 Project security

7.1 Project security documentation

All Classified Contracts contain security documentation. If the project involves complex security requirements, specific Programme Security Instructions (PSI) are prepared for it. Alternatively, a Security Aspect Letter (SAL) may be drafted, either as a substitute for or a supplement to the PSI. Normally, the SAL is a more concise document than the PSI and often used in the bidding stage. The security documentation also includes a Security Classification Guide (SCG).

7.1.1 Programme Security Instructions (PSI)

The Programme Security Instructions (PSI) provide comprehensive security guidelines for the project and are designed to:

- serve as a reference to the key security regulations to be applied to the project;
- provide more detailed instructions for application;
- reconcile national differences;
- allocate responsibilities for the fulfilment of the security requirements; and
- serve as a set of principles and help memorise regulations during project implementation.

A PSI is usually accompanied by a Security Classification Guide specifying the security classifications to be applied for individual project parts or materials.

In bilateral projects, the company participating in the project normally drafts the PSI , after which the PSI is to be submitted for approval to the security authorities of the countries concerned. It is also advisable to keep the security authorities of the participating countries informed of the progress made in the preparation of the PSI. It is a time-consuming process which needs to be initiated at an early phase. An example of the contents of the PSI is provided in Annex 2.

7.1.2 Security Aspects Letter (SAL)

The Security Aspects Letter (SAL) is a more concise security document. SAL specifies the security requirements for the project or the parts of the contract that need to be

protected from disclosure. SAL may be used if the security requirements related to the project are straightforward or if it is needed to supplement the PSI with regard to a specific subcontractor.

As a rule, SAL provides answers to the following questions:

- How can the authorisation to handle the information be obtained?
- What laws and regulations are applied?
- What level of protection the project information requires?
- For what purposes can the classified information be used?
- What technical means must be employed to transfer the information?
- How is the information marked, and how are the markings to be interpreted in practice?
- Who may or may not be given the information and on what terms (subcontractors)?
- What is the non-disclosure period specified for the information?
- How is the information to be destroyed or returned upon completion of the project?

7.1.3 Security Classification Guide (SCG)

The Security Classification Guide (SCG) is an important part of the PSI or SAL. It provides a description of the elements of the classified project and specifies the applicable security classification levels. The SCG indicates to the individuals involved in the project the security classification level of each process or project component. An example of the contents of the SCG is provided in Annex 3.

7.2 Elements of security

7.2.1 Security management

Security management – or the management of classified information – means all the measures implemented by a company to protect classified information.
A key element of security management is the administration of classified information. International classified projects impose additional requirements on the administrative security processes to be employed by companies. The processes are to include a description of the management of international classified information over its entire life cycle. Such a description must cover at least the following life-cycle stages:

- Creation of the information

    - For many projects, it is necessary to make a distinction between information created before the project (*background information*) and during it (*foreground information*). This may determine which party holds the intellectual property rights to the given item of information.
- Information classification and marking
    - Even if the intellectual property rights were deemed to belong to a company, the originator of the information is the State or international organisation under whose auspices or on whose assignment the classified information has been created.
    - The originator determines the security classification level of the information.
    - The security classification level may not be changed without the consent of the originator.
    - The employees involved in the project must understand the equivalence of the security classifications relative to the company's in-house classification system.
- Transfer, movement and reception of information
    - Secure procedures.
- Record of entry (registration according to security classification level)
    - Possibly in a project-specific file.
- Copying rules
- Dissemination rules
    - Special considerations regarding third parties.
- Transfer of information (physical, electronic)
    - Project-specific procedures.
- Requirements concerning storing and saving the information
- Right to process information
- Filing the information
- Procedures for the return or destruction of the information
- Action under exceptional circumstances

7.2.2 Personnel security

Personnel security means the protection of classified information from the security risks posed by the staff members.

With international classified projects, the importance of security training and control, and the vetting of staff are highlighted. The security instructions applying to an international project define the classification levels at which the people handling classified project information need to be security cleared. Normally, the lowest

security level at which a Personnel Security Clearance is required is CONFIDENTIAL. All security clearances are carried out in accordance with national legislation. When steps are taken to ensure the fulfilment of international security obligations, employees are often security cleared as part of the Facility Security Clearance.

According to the project security instructions, access to classified information is only given to people involved in the project on a need-to-know basis. Additionally, the project security documentation may require that those who do not directly handle classified information in their work, but who have access to the premises in which such information is handled, are security cleared.

Staff must know how to handle project-related classified information securely. While basic level security training must be an integral part of induction, more detailed guidance is always required in connection with international classified projects. Oversight is also required to ensure an adequate level of security.

As described, the security authorities of various countries cooperate to create standardised procedures for personnel security (particularly in the area of Personnel Security Clearances and Certificates).

7.2.3 Physical security

Physical security means the security arrangements in premises, production facilities and business travel. Physical security covers the requirements for the protection of premises as well as the requirements concerning the equipment and devices used for the protection of classified information. Such equipment and devices include safes, shredders, control and alarm systems, and locks. Access control is also part of physical security. Finland applies the National Security Auditing Criteria (KATAKRI), which follow the internationally accepted level of physical security. The physical security requirements are attended to in the FSC procedure.

7.2.4 Technical information security

International projects' security instructions determine the security level of the systems in which project information may be processed. Normally, detailed instructions are not given for the technical implementation of data system security in the project organisation. Responsibility for the verification of the level of data system security rests with the competent national authority. This can be accomplished either as part of the FSC procedure or a separate data system accreditation process.

7.3 Request for Visit

International classified projects often involve reciprocal visits between the project partners. Visitors to secured areas in the premises of a foreign public authority or company need an approval for the visit. Secured areas mean premises in which classified information is handled or stored.

The Request for Visit (RfV) procedure ensures that the visitor holds the required PSC and that there is a reason for the visit.

Often, the RfV procedure is applied even if the visit is to other than secured areas. If so, the visitor is not required hold a valid Personnel Security Clearance (PSC). All countries do not require a PSC for access to RESTRICTED information.

The RfV is submitted using a special form in which the information on the visit and visitors is entered. The need for a PSC depends on whether the visit is classified or unclassified. The visiting company submits the RfV form to the competent security authority in Finland (NSA in civil matters and Defence Command in military matters) which, in turn, forwards the request to the competent security authority of the host country.

8 Transfer of classified information and material

The security instructions for international classified projects include provisions for the transmission of classified information. Internationally, the transmission methods are divided into two categories: electronic transmission and physical transfer. Although electronic transmission is often regarded as the most efficient and secure method of transmitting information, it imposes certain requirements for the IT systems. Physical transfer of classified information usually takes place in one of three ways: military and diplomatic courier, hand carriage, or commercial courier. Classified machinery and equipment, for example, may also have to be transported as freight due to the large size of the consignment. The transmission methods to be applied for each category of classified information are indicated in the project security instructions. A specific plan of the transportation of classified material may be required in the security instructions, specifying the safeguards for the protection of the shipment in detail. The transportation plan is to be approved by the security authorities concerned.

8.1 Diplomatic courier and diplomatic mail

The project security instructions may – depending on the security classification of the consignment – require that a diplomatic courier or government-to-government channels are to be used. Consignments carried by a diplomatic courier or dispatched as diplomatic mail enjoy immunity under the Vienna Convention.

The diplomatic courier services available in Finland consist of the Ministry for Foreign Affairs' diplomatic mail and freight and diplomatic courier. When the diplomatic mail services of the Ministry for Foreign Affairs are used, it should be noted that as they operate according to a certain pre-determined schedule, they may not always be suitable for urgent deliveries. Another point worth mentioning is that the level of security of diplomatic mail is based on the carrier's security policy and that regular commercial channels are used for such carriage.

As a rule, civil servants travelling on a diplomatic or service passport can be assigned as diplomatic couriers. The diplomatic courier must have a sufficiently high PSC status. Training is provided for couriers to ensure that they understand their obligations and know how to act in exceptional circumstances.

Before accepting the assignment, the courier must sign a declaration stating that he or she understands and accepts the obligations associated with the assignment.

The diplomatic courier is to be provided with the necessary courier documents consisting of:

- a courier passport

- a border certificate

The courier passport serves as proof of the courier's diplomatic status. It is always signed by a head of mission or, in the case of the Ministry for Foreign Affairs, the head of the courier service. The border certificate is a document presented to the foreign authorities, indicating the parcel codes and number of parcels in the courier consignment.

The material to be transported is packed and unpacked at a diplomatic or consular mission abroad or the Courier and Logistic Services of the Ministry for Foreign Affairs.

8.2 Hand carriage

Normally, the project security instructions permit the use of hand carriage up to a specified security classification level.

The hand carriage courier receives a Courier Certificate[4] and other relevant documents from the dispatching party authorising him or her for the mission. When necessary, the courier can present this certificate to the public authorities in the country of destination as proof of the mission. However, hand-carriage consignments do not enjoy immunity at border crossings as defined in the Vienna Convention.

A hand-carriage courier must hold a sufficiently high PSC status and be given adequate training for the task. Additionally, before accepting the assignment, the courier must sign a declaration stating that he or she understands and accepts the obligations associated with the assignment.

8.2.1 Performance of the courier's assignment

The courier is required to:

- Assume personal responsibility for the delivery of the courier mail to the final destination and/or recipient.
- Ensure that the mail is never left unattended.
- Hand over the mail and other documents to a pre-determined recipient at the final destination. The recipient's identity must be verified before the courier mail is handed over. The recipient acknowledges receipt of the courier mail. The

[4] Courier Certificate. Not to be confused with the courier passport issued by the Ministry for Foreign Affairs.

dispatching party may require the courier to report on the completion of the assignment by phone.

- Return the copy of the receipt with the recipient's signature retained by the courier to the dispatching party.

8.3 Commercial courier services and postal services

Commercial courier services and national postal services may normally be used at least for carrying material of lower security classification. The use of commercial courier services usually requires the approval of the security authorities. Often, the commercial courier services available are listed in the project security instructions.

Countries have different policies on the use of commercial courier services. However, the guiding principle is that if the consignment does not specify that it contains classified information and the commercial courier is unaware of carrying classified documents and material, the commercial courier need not be security cleared. If, on the other hand, the commercial courier is aware of carrying classified documents, they must usually be security cleared.

8.4 Freight

Classified material, such as machinery and equipment that cannot be carried by courier, are transported by commercial freight carriers. The carrier company must have an adequate FSC clearance status and those handling the material need a PSC. Normally, a transportation plan is to be prepared for freight transports for approval by the security authorities concerned.

9 Security clearances

9.1 Phases of facility security clearance

In the FSC procedure, the competent authority verifies the security performance of the company concerned in the following respects: security management; personnel security; physical security; and technical information security. The security levels verified by the authority are level II (SECRET), level III (Confidential) and level IV (RESTRICTED). In verifying security, the security authorities apply the National Security Suditing Criteria KATAKRI.

Security clearance starts with a meeting of the security authorities and company representatives, during which the public authority tells about the the process and the company representative describes the project at hand. At the meeting, the parties agree on the timetable for security clearance and appoint persons who will be responsible for it.

The actual security clearance begins when the company presents its security documentation or prepares it to an agreed timetable for review by the security authority. The authority reviews the documentation and reports any non-conformances to the company, which takes the necessary measures to correct the incidences identified by the authority. When the corrections have been made, the next step is the actual security auditing phase. During this phase, the NSA/DSA security auditors verify the practical implementation of the measures necessary to achieve the required level of security. Any information security incidences detected in the course of security auditing are reported to the company, which will then take the necessary action.

If the company fails to remedy the indicated information security incidences and to achieve the required level of security within the agreed period of time, or the company withdraws from the project, the public authority will discontinue the security audit.

Additionally, all persons taking part in the project undergo a Personal Security Clearance (PSC), which is always included in the FSC process.

When the public authority deems that the overall security level of the company meets at the least the minimum requirements, the company signs a written commitment to maintain the level achieved. Based on this commitment, the NSA grants the Facility Security Clearance (FSC) to the company which, in turn, forwards it to the foreign authority requesting such clearance.

As long as the commitment remains in force, the company is required to report any changes in the company's ownership base, project personnel or security arrangements to the competent authority. Normally, the undertaking is valid for five

years. Under the Act on International Information Security Obligations, any breach of the undertaking is punishable (Laki kansainvälisistä tietoturvallisuusvelvoitteista, 2004/588, chapter 3, section 20).

9.2 Accreditation of information systems

If classified project information is handled in the company's information system, the system must be accredited. Accreditation means the approval of the technical information security solution, which indicates that it satisfies the level of security required for the project. Accreditation is a process during which the competent authority defines, in consultation with the owner of the information system, the level of risk the system is exposed to and approves the protective measures commensurate with the risks including the instructions for the secure use of the system. Usually, the accreditation process includes a specific audit of the information system which will not be carried out until all the security features of the system have been deployed.

In the accreditation process, the reference level of protection is provided by the National Security Auditing Criteria KATAKRI. More detailed security requirements may arise out of the contract on the international classified project or other international obligations.

9.3 Phases of Personnel Security Clearance

The Facility Security Clearance process always includes the Personnel Security Clearance of all the company employees participating in the project. Under certain circumstances, a Personnel Security Clearance alone is enough for participation.

When conducting a PSC, the competent authority[5] checks the background of the person in question by using the procedure stipulated by law. A PSC requires the person's written consent, which is given using a standardised form.[6] The person's job description and role in the project are also specified in the form.

A foreigner employed by a Finnish company may also be security cleared; however, it should be borne in mind that the Finnish authorities have limited resources to investigate the background of foreigners. The Act on Background Checks (177/2002) contains an exhaustive list of the registers to be used for security clearance; however,

[5] Limited security clearance: local police; standard or extensive security clearance: Finnish Security Intelligence Service. In case of defence projects, the authority is always Defence Command.

[6] http://www.poliisi.fi/poliisi/supo60/home.nsf/files/Perusmuotoinen_turvallisuusselvitys_060801b/$file/Perusmuotoinen_turvallisuusselvitys_060801b.pdf.

conducting a security clearance does not, as such, provide any basis for investigating the data held by foreign authorities on the person in question.

When a security clearance is made of a foreigner or a Finn who lives or has lived abroad, the period of time from which the data is available to the public authorities is to be indicated in the security clearance report.

A precondition applied by the National Security Authority for the granting of a PSC is that the person has lived in Finland for the five years preceding the issuance of the clearance.

When conducting a PSC, the Finnish Security Intelligence Service takes no position on the eligibility of the person; instead, it gives an evaluation of the information that may be relevant to the clearance based on the data contained in the registers. This information will be reported in writing to both the employer and the National Security Authority who will then determine whether the preconditions for the granting of the PSC are met.

According to the Act on Background Checks (Laki turvallisuusselvityksistä, 177/2002), the subject is entitled to know whether any security investigation has been conducted in respect of him or her and to access the information provided in the PSC report. To exercise such right of access, an appointment is made with the Finnish Security Intelligence Service or Defence Command. It should be noted, however, that such right of access does not exist if the item of information originates from a register to which the person has no right of access (e.g. Finnish Security Intelligence Service's operative information system). If so, he or she may ask the Data Protection Ombudsman to check his or her data contained in the Finnish Security Intelligence Service's operative information system.

9.4 Security Clearance Certificates

The NSA evaluates the reliability of the company or individual based on the statement issued by the authority conducting the security investigation and, if no impediment exists, grants the requested security certificates (PSC, FSC). The NSA informs the requesting foreign authority of the issuance of the PSC or FSC certificate.

With domestic defence contracts, the competent security authority is the Defence Command.

Both PSC and FSC certificates may be granted for a maximum period of five years. The security authorities regularly audit the security procedures applied by the company during the validity of the Facility Security Clearance certificate.

Should any incident occur during the validity of the Facility Security Clearance

certificate affecting the company's capacity to maintain the required level of security, the clearance level granted under the certificate may be downgraded. A FSC certificate is cancelled if its basis ceases to exist or if such a change takes place in the company's circumstances that the authority is no longer satisfied that the security and reliability criteria continue to be met. Any financial costs incurred due to a cancellation are to be paid by the company concerned. The National Security Authority informs the party requesting the certificate of any changes in the security level. Before a FSC certificate can be restored to the previous level, a proper audit is to be carried out by the competent authority.

10 Security responsibilities and obligations of companies

10.1 Responsibilities of the prime contractor

Companies participating in international classified projects are advised to engage in cooperation with the national security authorities at the outset of the project in order to be able to identify their responsibilities and obligations.

Once project participation is certain and the company has recognised that the project involves security requirements pertaining to it, the company should initiate a preliminary risk management process. A risk analysis helps identify the areas in which the company's security performance should be improved. A useful tool in this process is the National Security Auditing Criteria (KATAKRI)[7], which specifies the detailed security requirements applied by the Finnish authorities in respect of projects with different security categories.

The responsibilities of the company participating in the project as the principal contracting party (prime contractor) are defined in the Classified Contract drafted for the project. In addition to the general contractual provisions concerning the project, the contract contains the security instructions such as the PSI and/or SAL. Usually, the security instructions are an integral part of the contract and the obligations imposed by it are binding on the company just like the contract itself.

The subcontractors used by the prime contractor are normally mentioned in the contract and are thus automatically bound by the obligations imposed in the project security instructions. If the use of other subcontractors becomes necessary during the course of the project, their security level must be verified as specified in the Classified Contract. Usually at least a minimum update of the project security instructions and the undertaking given to the authority are required. The prime contractor is responsible for ensuring that any subcontractors not approved by the procurement unit are not hired in the project.

The procurement unit may specify certain restrictions as to the use of foreigners or subcontractor companies owned by foreigners. The prime contractor must give due consideration to any such restrictions in the selection of subcontractors.

Usually, subcontractors are subject to the same security requirements as the prime contractors. The prime contractor is responsible for the security requirements applicable to their subcontractors.

If the subcontractor is a Finnish company, it should contact the Finnish Security Intelligence Service to obtain a FSC certificate.

[7] www.defmin.fi

10.1.1 Foreign subcontractors

If the subcontractor is a foreign company, the prime contractor may ask the NSA of Finland to obtain an FSC certificate for the company. The Finnish NSA will then forward the request to the subcontractor's NSA. As a rule, a General Security Agreement should exist between Finland and the country concerned.

For the request, the NSA needs at least the following:

- Information on the subcontractor company (name, business registration number and street address) and contact person.

- An indication whether an answer confirming the existence/non-existence of an FSC is enough; or whether an FSC procedure is to be started if the company has no FSC.

- As accurate reasons for the FSC request as possible. Such reasons may, for example, be participation in a project in which classified information of some State is handled and in which the foreign company is to serve as a subcontractor of a Finnish company. Reference is also to be made to the project security standard requiring an FSC certificate of the subcontractor. Additionally, the reasons should indicate the type of classified information to be protected (classified information of national importance to Finland; EU classified information; NATO classified information; classified information of national importance to other State). The request should be accompanied by the relevant sections of the security instructions in which the reasons are specified.

- The protection level (*confidential / secret*) for which security clearance is requested.

10.1.2 Foreign employees

If a Finnish company intends to use foreign employees in international classified projects, the first step is to check whether the security instructions impose any restrictions on the use of foreign labour. Usually, the consent of the procurement unit is required for the use of foreigners.

To obtain a PSC certificate for foreign employees, the Finnish company must contact the NSA. The NSA may request security certificates from countries with which Finland has a General Security Agreement. Certificates may also be requested from EU and MISWG countries on a case-by-case basis. The security clearance procedure varies from one country to another.

The following information must be submitted to the NSA for the request:

- Information on the persons concerned (name, date of birth, citizenship and address).

- A copy of the particulars page in the passport or a copy of an identification certificate.

- As accurate reasons for the PSC request as possible. The reason may, for example, be participation in an international classified project in which the persons have access to classified information or premises where they may gain access to classified information. Additionally, the reasons should indicate the type of classified information to be handled in the project (classified information of national importance to Finland; EU classified information; NATO classified information; classified information of national importance to other State).

- The protection level (confidential / secret) for which security clearance is requested.

10.2 Duties of the project security officer

A Facility Security Officer (FSO) is always to be appointed for the project in the security instructions. Often, the officer is the company's security manager. While the company may also have others responsible for security, such as the data security officer, responsibility in respect of the foreign procurement unit and authorities will always rest with the designated Facility Security Officer.

The Facility Security Officer plays a key role in the assurance of project security. He or she is responsible for the practical implementation of the requirements specified in the security instructions, including staff training and supervising activities. Additionally, the Facility Security Officer or his/her alternate are required to report all incidences detected. The Facility Security Officers are required to keep in contact with one another, for example in connection with requests for visits.

10.3 Breaches of security and compromise of classified information

Any breach or a suspected breach of security and compromise of classified information must be promptly reported to the NSA and the parties specified in the project security instructions. Normally, the minimum requirement in the security instructions is that the incident is reported to the Originator.

Further damage must be prevented where possible and steps taken to ensure that those directly involved in the breach of security are not assigned to investigate it.

The NSA will inform the national security authority of the other country concerned of any breach of security and/or compromise of classified information that may come to

its attention. The NSA will take prompt action to resolve the matter and bring to justice those guilty of a punishable act or omission.

List of Finland's General Security Agreements

PARTIES	EFFECTIVE DATE OF THE AGREEMENT
NATO (NORTH ATLANTIC TREATY ORGANISATION)	22 SEPTEMBER 1994
WEU (WESTERN EUROPEAN UNION)	1 MAY 1998 (Treaty Series 41–42/1998; WEU's activities wound up)
EU (EUROPEAN UNION)	Intergovernmental treaty signed 25 May 2011; and Council security regulations (2011/292/EC) effective as of 27.5.2011
GERMANY	16 JULY 2004 (Treaty Series 96–97/2004)
ESA (EUROPEAN SPACE AGENCY)	1 AUGUST 2004 (Treaty Series 94-95/2004)
FRANCE	1 AUGUST 2005 (Treaty Series 66-67/2005)
SLOVAKIA	1 JANUARY 2008 (Treaty Series 116-117/2007)
POLAND	1 MAY 2008 (Treaty Series 46–47/2008)
ESTONIA	1 MARCH 2008 (Treaty Series 12–13/2008)
LATVIA	1 MARCH 2008 (Treaty Series 33–34/2008)
ITALY	1 MARCH 2008 (Treaty Series 23–24/2008)
OCCAR (ORGANISATION FOR JOINT ARMAMENT COOPERATION)	10 OCTOBER 2008 (Treaty Series 109–110/2008), applies only to ESSOR programme
BULGARIA	1 JANUARY 2009 (Treaty Series 116–117/2008)
SLOVENIA	1 JUNE 2009 (Treaty Series 22–23/2009)
CZECH REPUBLIC	1 OCTOBER 2009 (Treaty Series 53–54/2009)
SPAIN	1 MAY 2010 (Treaty Series 38–39/2010)
NORDIC COUNTRIES	Signed on 7 MAY 2010; applied by Finland in respect of Sweden and Norway

Example of a table of contents of a PSI (Programme Security Instructions):

1. Presentation of the document
    a. Purpose of document
    b. Definition of security responsibilities
    c. Terminology
2. General security instructions
    a. General principles
    b. Access to classified information
    c. Cross-border transfer of information and material
    d. Marking project information
    e. Procedures to protect unclassified but restricted information
    f. Procedures to protect classified information
    g. Security classification
    h. Information security incidences
3. Disclosure of information
    a. Unilateral disclosure
    b. Disclosure of information and material to non-participants or third parties
    c. Disclosure of project information at public events
    d. General disclosure of project information
    e. Authorisations regarding exhibitions
4. International visits
    a. General
    b. General Request for Visit procedures (or)
    c. Simplified Request for Visit procedures
5. Subcontractors
    a. Finnish subcontractors
    b. International subcontractors
6. Security cleared premises
    a. General
    b. List of security cleared premises
    c. Distribution of the list
    d. Updating the list
    e. Use of the FIS and PSCI/RfV forms
7. Security plan in the event the contract expires or the principal contracting party is not elected to continue
    a. General
    b. Information owned by the public authorities

c. Information owned by the principal contracting party

8. Security training
    a. General principles
    b. Induction to security issues
    c. Security awareness
    d. Induction to travel security
    e. Security instructions related to the completion of the task
9. List of annexes
    a. Annex A
        i. Particulars of the project parties and principal commercial contracting parties
    b. Annex B
        i. Security Classification Guide
        ii. Contents
        iii. General
            1. Purpose
            2. Authorisation
            3. Security classifications
            4. List of terms used in the Guide
            5. Recommended classifications
            6. Instructions for downgrading the security level
            7. Other instructions
            8. Marking classified information
            9. Update plan
    c. Annex C
        i. Request for Visit procedure
    d. Annex D
        i. Protection of information in data and data transmission systems
            1. Introduction
            2. Non-technical security measures
            3. Technical security measures
            4. Accreditation
            5. Computer hardware
            6. Annex A: Definitions
    e. Annex K
        i. Abbreviations and acronyms

Example of the contents of the Security Classification Guide (SCG):

1. General observations
    a. Purpose of the Guide
    b. Authorisation
    c. Security classification
    d. Applicability
    e. Concepts
    f. Detailed recommendations and instructions for classification
    g. Instructions for downgrading the security classification
    h. Other instructions
    i. Marking instructions
    j. Updating the schedule
2. Other issues (e.g. identification and protection of project elements / components requiring classification)