ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY

2015 (LVI) 3 (202)

DOI: 10.5604/0860889X.1178572

Tomasz Sobczyński*, Karol Listewnik**

THE PRINCIPLES OF CLASSIFIED INFORMATION SECURITY MANAGEMENT SYSTEM ORGANISATION WITHIN THE REALISATION OF EUROPEAN DEFENCE AGENCY RESEARCH PROJECTS (PERSONNEL AND FACILITY SECURITY ASPECTS)

ABSTRACT

The article presents the aspects of personnel and facility security principles for classified Information Security Management System (ISMS) implemented within the realization of European Defence Agency research and technology projects. In the contents of article, authors characterised the rules and procedures, resulting from the legal acts, which regulates procedures of handling and exchanging of classified information, obtained during the realisation of research process. Special attention has been focused on the European Defence Agency projects during which, wide range of international participants have to implement, not only efficient but also common ISMS for all membership countries, to be able to fulfil all legal requirements for classified and sensitive information.

Key words:
classified information, sensitive information, personnel security, facility security, risk assessment, dissemination of EUCI, risk level valuation, physical security measures.

INTRODUCTION

Contemporary world is dependent on information. In fact, we live in Information *Age*, where information has become a material value for all forms of organizations

* Polish Naval Academy, Śmidowicza 69 Str., 81-103 Gdynia, Poland; e-mail: t.sobczynski@amw.gdnia.pl
**Polish Naval Academy, Faculty of Mechanical and Electrical Engineering, Śmidowicza 69 Str., 81-103 Gdynia, Poland; e-mail: k.listewnik@amw.gdynia.pl

and remains a critical element of their management systems. The exceptional part of this system are information categorised as classified. In view of different classification levels of organization's assets, we have to remember that, loss or unauthorised access to this specific information may result in serious consequences, not only for specific institutions or local society, but also a national or worldwide range can be considered.

The sensitive nature of many research projects, especially this which are connected with defence and security areas, causes that, the ability and the reliability of individual contributors to protect classified information are indeed crucial for the award and execution of such a project. As far as we consider multinational projects, branded by European Defence Agency (EDA), with wide variety of EU State Members, safety of the project can be hampered by the absence of unified Information Security Management System (ISMS). This is the reason why, all participants of the research projects, are obliged to organise and implement a common ISMS, from the very beginning of cooperation process. What is more, ISMS have to be constructed on principles, which are based on legal acts regulating area of information security.

In view of European Union, the *Council Decision of 31 March 2011 on the security rules for protecting EU classified information 2011/292/EU*[1] is the very main act which provides guidelines for all European Union Classified Information (EUCI) and defining rules for areas such as: personal security, facility security, physical security of classified materials, IT security, etc.

This article, focused on procedures and principles, connected with organisation of personnel and facility security systems, which are in fact crucial element for all institutions attempting to be awarded with execution of defence and security research projects.

PERSONNEL SECURITY CLEARANCE

The desired degree of secrecy of classified information is known as its sensitivity. Sensitivity is based upon a calculation of the damage that would be caused

[1] On 15th October 2013 in the EU Official Gazette, L 274, *Council Decision dated 23rd of September 2013 on the Rules for protection of EU classified information 2013/488/EU* was published. The new rules revoke and replace *Council Decision 2011/292/EU* dated 31st March 2011 on the Security Rules for protection of EU classified information. The information of EU classified in accordance with *Council Decisions 2001/264/EU* and *2011/292/EU*, shall be protected in compliance with the new Decision.

to: an institution, local society, national security or defence system, international policy, etc., by uncontrolled release or loss of the classified materials. What is more, classified information is material that a standardization norms described as sensitive information that requires protection of: *confidentiality, integrity, or availability*[2]. Access to this kind of materials is restricted by law or regulation to particular group of people, and any departure in this area can cause criminal penalties and loss of respect.

A security clearance is granted to an individual and generally recognizes a maximum level of clearance. The personnel working with classified information is required for possession of specific security clearance of an appropriate type and classification level in order to meet the legal requirements. Each of governmental or non-governmental institution, which is handling classified materials, is obliged to prepare a categorization of the positions which demands a Personnel Security Clearance (PSC) and define a degree of secrecy, known also as level of classification. For the person who apply for a job which requires a PSC, or who already is appointed on such position, initiation of procedure for issuing a relevant PSC certificate is necessary.

The European Union has four levels of classification: RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. Each level of classification indicates an increasing degree of sensitivity. According to EU rules for protecting EU classified information, PSC can authorised an individuals to access classified information starting from: CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET up to TRÈS SECRET UE/EU TOP SECRET[3]. However, the RESTREINT UE/EU RESTRICTED classification level is settled in Council decision[4], there is no need for PSC possession to be granted an access to this kind of materials. In this case, an executive manager of institution which is handling restricted information, is authorised to approve an individual to access such a classified materials.

Organizing procedures connected with access to classified materials, security information manager is obliged to consider, not only authorisation level of an individual, but also area of responsibility and level of each person awareness regarding the knowledge about principles of ISMS. Area of responsibility, known also as the

[2] *ISO/IEC TR 13335-1:1996 Information technology — Guidelines for the management of IT Security*, Part 1, *Concepts and models for IT Security (ISO 13335).*

[3] *Decisions Council Decision of 31 March 2011 on the security rules for protecting EU classified information 2011/292/EU*, Annex I, *Personnel Security, Authorising Access to EUCI*, p. 26.

[4] *Decisions Council Decision of 31 March 2011 on the security rules for protecting EU classified information 2011/292/EU*, Annex V, *Industrial Security, Handling and Storage of Information Classified RESTREINT UE/EU RESTRICTED*, pt 33, p. 51.

need to know principle[5], indicates the range and also type of information, to which an individual shall be permitted. Knowledge about an individual's level of awareness regarding the principles of ISMS function, will allow to perform a proper security briefing for each person which is handling sensitive materials.

Bearing in mind, the sensitiveness of information handled during the execution of many research and technology projects branded by European Defence Agency, access to this information has been limited only for individuals authorised to access classified information, for example at the CONFIDENTIAL level. This restriction signifying that, a person shall only be authorised to access information classified CONFIDENTIAL maintained during the research procedure after:

- his/her need-to-know has been determined;
- he/she has been granted a PSC to the appropriate level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations;
- he/she has been briefed on the security rules and procedures for protecting classified and sensitive information and has confirmed his /her responsibilities with regard to protecting such information.

Eligibility for access to classified and sensitive information, commonly known as a personnel security clearance, is granted only to those for whom an appropriate personnel security background investigation has been completed with positive result. To initiate the investigation an individual has to complete the security questionnaire and give detail information about: personal data, criminal incidents, credit background, educational and professional qualifications, previous employment and references, abroad travels and contacts, etc.[6] Using the information provided by the applicant in his or her clearance application materials, a background investigation of the applicant is conducted by National Security Authority (NSA) of each EU State Member, which is responsible and authorised by multinational agreements to operate in the security of information area.

Personnel security clearance process is an administrative procedure carried out by a certified adjudicator to determine that an individual, taking into account his:

[5] The term 'need to know', when used by government and other organizations (particularly those related to the military or espionage), describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information, or read into a clandestine operation, unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's official duties. See: https://en.wikipedia.org/wiki/Need_to_know.

[6] Range and specificity of questions depend on level of clearance to be applied for.

loyalty, strength of character, trustworthiness, honesty, reliability, discretion, as well as freedom from conflicting allegiances and potential for coercion is eligible from a security standpoint under national security standards for access to classified information. Considering the access to EDA classified projects, eligibility will be granted only where facts and circumstances indicate access to classified information is clearly consistent with the security interests of EU. A security investigation procedure requires detailed documentation of whole process and can take as few as 3 to 6 months to obtain the final result. At the moment when a certified adjudicator will receive the outcome of the investigation, which points that there is no doubt that an applicant is reliable and give guarantee of secrecy, NSA will issue a personnel security clearance adequate to required classification level.

A personnel security clearance has different validity periods, during which an individual is authorised to access classified information. The specific period of access is depending on classification level of PSA.

Table 1. Validity periods of Personnel Security Clearance depending on classification levels of certificate

Personnel Security Clearance		Validity periods		
		Top Secret	Secret	Confidential
Classification level	TRÈS SECRET UE/EU TOP SECRET	5 years	7 years	10 years
	SECRET UE/EU SECRET	–	7 years	10 years
	CONFIDENTIEL UE/EU CONFIDENTIAL	–	–	10 years

Considering the situation, when an applicant has been granted the highest authorisation level — *Top Secret Personnel Security Clearance*, it means that person is allowed to access and handle information up to the level of *Top Secret* for the period of five years, *Secret* for the period of seven years and *Confidential* for the period of ten years. Similarly is the situation with the other classification levels of PSC (e.g., an individual holds a *Secret PSC*, it means that an individual is not permitted to access and handle *Top Secret* information, but is allowed to access and handle *Secret* and *Confidential* classified information, adequately for the period of seven and ten years). What is more, all individuals granted with PSC are allowed to access information classified as Restricted, but with *Need to Know* principle preservation.

Apart from the fact, that an individuals has successfully passed personnel security investigation process and has been granted with required PSC, the final

decision about the area of access to sensitive materials, what fallows for example with responsibilities for some part of research process, depends on the most fundamental security principle which is *Need-to-Know* principle.

Bearing in mind EDA research and technology projects, determination made by a possessor of classified information is crucial for the interest of research program security. At the very beginning, during the planning phase, the coordinator of the research program is obliged to define the information areas, then appoint the personnel who is responsible for and allowed to access to this areas. A potential contractor, may be granted with an access, knowledge, or possession of the classified information in order to perform tasks or services, which are essential for the duties fulfilment within the confines of research project. Access to classified information connected with some specific areas of interests will be terminated when an individual no longer has need such access.

Last but equally important element of the personnel security policy, is procedure that all employees, contractors, etc. must be provided with an initial security briefing, prior to their being permitted access to classified information.

There are various subject areas to be covered in the initial briefing which provide the guidance necessary to protect security of information system. Upon completion of this course every trained should be able to:

- describe threat awareness;
- be aware of Operations Security (OPSEC)[7] threats and conditions;
- understand your reporting requirements;
- define security concepts;
- explain the concepts of a security clearance and Need-to-Know;
- understand classified information handling;
- identify the requirements for processing classified information on a computer system;
- Understand Communications Security (COMSEC)[8];
- Understand the Visit Request process and describe proper travel procedures.

[7] Operations Security, or OPSEC, is the process by which we protect unclassified information that can be used against us. OPSEC challenges us to look at ourselves through the eyes of an adversary (individuals, groups, countries, organizations). Essentially, anyone who can harm people, resources, or mission is an adversary. See: http://www.dodea.edu/Offices/Safety/OPSEC.cfm.

[8] Communications Security (COMSEC) is the practice of preventing unauthorized interception/ access of telecommunications traffic to its intended source. Within COMSEC there are several disciplines including: Cryptographic Security, Emission Security, Physical Security, Traffic-flow security, Transmission security, Electronic Key Management System. See: http://www.securestate.com/Federal/ESS/Pages/Communication-Security-COMSEC.aspx.

The knowledge about fundamental principles and rules of security information system established for classified program needs, as well as awareness of the program personnel, about consequences resulting from disobeying the legal regulations, is very important and fundamental for security information management process. What is more, regular training in this area, allow to reduce the risk of appearance of incidents connected with loss or unauthorised access to classified information, to acceptable level.

FACILITY SECURITY CLEARANCE

The term facility is used as a common description for a functioning entity consisting of a plant, laboratory, office, college, university, or commercial structure with associated warehouse, storage areas, utilities and components, which are related by function or location. It does not refer to Government installations. Considering, an institution which is going to apply for realisation of a contract within the confines of classified EDA research program, this institution is obliged to hold required security certificate. This certificate, known as Facility Security Certificate (FSC)[9], similarly to PSC with reference to personnel, officially acknowledge that an institution is recognizable as credible in area of classified information security management. A Facility Security Clearance is required before an institution can be awarded classified contracts.

A Facility Security Clearance, at the classified level is an administrative determination that an organization is entitled, from a security viewpoint, for access to classified and protected information and assets of the same or lower classification level as the clearance being granted. There are three types of Facility Security Clearances:

1. Third Level Certificate
   This is the most basic type of Facility Security Clearance. It normally applies to institutions which are involved in contracts for 'services'. A *Third Level Facility Security Clearance* will involve security screening of the institution's Key Senior Officials and employees. There is no requirement to evaluate the physical security status of the institution's facilities. A Third Level Facility Security Clearance

[9] *Decisions Council Decision of 31 March 2011 on the security rules for protecting EU classified information 2011/292/EU*, Annex V, *Industrial Security, Facility Security Clearance*, Chapter III, pt 8, p. 48.

does NOT authorize the institution to possess or store classified information and assets within its facilities.

2. Second Level Certificate
   This type of Facility Security Clearance includes the security screening of the institution's Key Senior Officials and employees. In addition, the physical security of the institution's facilities is evaluated to ensure they meet the requirements for the protection of government information and assets. A *Second Level Facility Security Clearance* will authorize the organization to possess and store CLASSIFIED information and assets at their facility, but with the exception of possibility to process classified materials within institution's IT systems.
3. First Level Certificate
   This type of Facility Security Clearance includes all the same elements such as a *Second Level Facility Security Clearance*. In addition, holders of this FSC are entitled to creating, modifying, maintaining or otherwise work with classified information with use of their own IT systems which meet the government security requirements.

Each type of Facility Security Clearance, apart from the type of certification, may be divided according classification levels such as: *CONFIDENTIAL, SECRET or TOP SECRET,* what depend on classification level of information handled by institution.

A Facility Security Clearance certification process, can be carried out by the National Security Authority (NSA) or Designated Security Authority (DSA) or any other competent security authority of a European Union Member State to indicate, in accordance with national laws and regulations, that an industrial or other entity can protect classified information at the appropriate classification level within its facilities.

Before a FSC will be granted, an institution and its facilities shall meet the adequate protection measures, defined as physical and administrative security requirements which are necessary for the performance of the classified work to be executed under the future contract.

During the verification procedure, appropriate NSA or DSA shall, as a minimum:

- evaluate the integrity of the industrial or other entity;
- evaluate ownership, control, or the potential for unnecessary influence that may be considered as a security risk;
- verify that the industrial or any other entity has established a security system at the facility which covers all appropriate security measures necessary for the protection of information or classified material;

- verify that the personnel security status of management, owners and employees who are required to have access to classified information has been established in accordance with the requirements;
- verify that the industrial or any other entity has appointed a Facility Security Officer who is responsible to its management for implementing the security obligations and administering of the ISMS.

After a positive validation process, confirmed by the dedicated *check and control* procedure of all issues mentioned above, competent security authority of State Member are able to issue a positive opinion about an institution's information security system and this institution can be granted with a proper FSC.

In the same way as a Personnel Security Clearance, a Facility Security Clearance certificate can authorise an institution to maintain sensitive and classified materials within a different periods of time. This periods, analogous to principle established for PSC, depend on classification level of certificate which institution was granted.

Table 2. Validity periods of Facility Security Clearance depending on classification levels of certificate

Facility Security Clearance		Validity periods		
		Top Secret	Secret	Confidential
Classification level	TRÈS SECRET UE/EU TOP SECRET	5 years	7 years	10 years
	SECRET UE/EU SECRET	–	7 years	10 years
	CONFIDENTIEL UE/EU CONFIDENTIAL	–	–	10 years

During all the validity period of FSC, visible in the table above, an institution is obliged to preserve the same level of standards connected with ISMS as it was during the moment of FSC certification. To maintain a desirable level of security in facilities granted with FSC, NSA institutions are authorised to carry out a periodic security checks. If the institution fails to maintain the required security standards, a Facility Security Clearance can be suspended or revoked by competent security authority. What is more, programs, contracts, etc. which are in effect will be cancelled and the institution will not be entitled for future security related contracts while the organization's Facility Security Clearance is under suspension.

CONCLUSION

The certification process, either personnel or facility, is very important not only for the effectiveness of the project management, but also for final results of the researches. Considering research projects, strictly connected with defence or security of EU, it was very essential, for all EU State Members handling EUCI, to organise and also standardize procedures for sensitive and classified information security management. In view of bilateral contracts or programs with small number of participants there is no significant problems to establish common rules in this area, but if the program is international with wide variety of contributing institutions, some specific procedures can be troubled by the absence of unified regulations for *Security of Information* and this can have a direct impact on possible malfunction in project execution.

All institutions which have been an FSC granted, give a guarantee that they meet the legal requirements and have implemented an efficient Information Security Management System. What is more, implemented system is based on internationally recognized standards which are acknowledged and executed by all participants of the process. For the classified information safety, it means that the legal framework applied, thanks to FSC and PSC certification procedure, give an assurance of putting into practice an appropriate resolutions in area of confidentiality of information which are obtained or exchanged, during a defence and security procurements, by all contributors. Moreover, acceptation of system which is based on FSC certification standards, signify that contributing Member States have to ensure that, within their territory, obtained information will receive a level of protection which is equivalent to the level of protection offered by the security measures established by commonly accepted rules.

REFERENCES

[1] *Council Decision dated 23rd of September 2013 on the Rules for protection of EU classified information 2013/488/EU.*

[2] *Council Decision of 19 March 2001 adopting the Council's security regulations 2001/264/EU.*

[3] *Council Decision of 31 March 2011 on the security rules for protecting EU classified information 2011/292/EU.*

[4] *Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC.*

[5] European Defence Agency, [online], http://www.eda.europa.eu/info-hub/data-protection, [access 12.06.2015].

[6] European Union Agency for Network and Information Security, [online], https://www.enisa.europa.eu/activities/risk-management, [access 12.06.2015].

[7] *Information Security Risk Assessment. Practices of Leading Organizations*, Accounting and Information Management Division Executive, GAO Guide on Information Security Management, 1999.

[8] *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.*

[9] *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.*

[10] *ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance.*

[11] *ISO/IEC TR 13335-1:1996 Information technology — Guidelines for the management of IT Security*, Part 1, *Concepts and models for IT Security (ISO 13335).*

[12] Taylor A., Alexander D., Finch A., Sutton D., *Information Security Management Principles*, 'The British Computer Society', 2008.

[13] *The Treaty of Rome*, 25 March 1957, [online], http://www.civitas.org.uk/eufacts/download/TR.1.Treaty%20of%20Rome.pdf, [access 28.05.2015].

ZASADY ORGANIZACJI SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACYJNYM PODCZAS REALIZACJI PROJEKTÓW NAUKOWO-BADAWCZYCH EUROPEJSKIEJ AGENCJI OBRONY (ASPEKTY BEZPIECZEŃSTWA OSOBOWEGO I PRZEMYSŁOWEGO)

STRESZCZENIE

Artykuł przedstawia aspekty bezpieczeństwa osobowego i przemysłowego w ramach organizacji systemu zarządzania bezpieczeństwem informacji wdrażanego podczas realizacji projektów naukowo-badawczych Europejskiej Agencji Obrony. Autorzy charakteryzują procedury oraz zasady wynikające z aktów prawnych regulujących obszar związany z ochroną informacji niejawnych przetwarzanych w procesie realizacji projektu naukowo-badawczego. Szczególną uwagę zwrócono na wielonarodowe projekty naukowo-badawcze wspierane przez Europejską Agencję Obrony, gdzie organizatorzy procesu zarządzania projektem muszą wykreować i wdrożyć wspólny system zarządzania bezpieczeństwem informacji, który jest nie tylko skuteczny, ale również spełnia

wszelkie wymogi formalnoprawne wynikające z regulacji kształtujących zasady postępowania z informacjami niejawnymi oraz wrażliwymi.

Słowa kluczowe:

informacje niejawne, informacje wrażliwe, bezpieczeństwo osobowe, bezpieczeństwo przemysłowe, oceny ryzyka, rozpowszechnianie informacji klasyfikowanych UE, analiza poziomu zagrożeń, środki ochrony fizycznej.