Possible approaches to ensure security of information for nuclear facilities

Dimitar Dimitrov
Bulgarian Academy of Sciences - Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
E-mail: ddimitrov@ims.bas.bg

Abstract: *Sensitive information is information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. Information security not only includes ensuring the confidentiality of information, but also includes ensuring the accuracy and completeness of the information (its integrity) and the accessibility or usability of the information on demand (its availability).*

KEYWORDS: *INFORMATION, SENSITIVE INFORMATION, CONFIDENTIALITY, INFORMATION SECURITY, ENSURING SECURITY OF SENSITIVE INFORMATION, IDENTIFYING AND SECURING SENSITIVE INFORMATION, SECURITY POLICIES*

1. Introduction

The overall objective of a country's nuclear security regime is to protect persons, property, society and the environment from harmful consequences of a nuclear security event.

Groups or individuals wishing to plan or commit any malicious act involving nuclear material or other radioactive material or associated facilities may benefit from access to sensitive information. Such information should therefore be identified, classified and secured with the appropriate measures [1].

Ensuring the security of sensitive information is a cross-cutting prerequisite for nuclear security, and the systems and measures to achieve effective information security are key elements of a countries' nuclear security regime.

This report provides short guidance on implementing the principle of confidentiality and on the broader aspects of information security. Much national and international guidance exists regarding the establishment and management of information security frameworks for information of various types, in the form of both high level guidance and detailed standards.

Instead, its goal is to assist operators in bridging the gap between existing government and industry standards on information security in general, the particular concepts and considerations that apply to nuclear security, and the special provisions and conditions that exist when dealing with nuclear material and other radioactive material.

2. Concepts and context

2.1 Definition of information

Information is knowledge, irrespective of its form of existence or expression. It includes ideas, concepts, events, processes, thoughts, facts and patterns. Information can be recorded on material such as paper, film, magnetic or optical media, or held in electronic systems.

Information can be represented and communicated by almost any means. In the nuclear domain, there is a vast amount of information in many forms.

Information assets are the equipment or components (including media) that are used to store, process, control or transmit information.

For the purpose of handling and security, information may be grouped into information objects. These may be defined as all elements of information that have value to an organization.

Typically, an information object comprises a set of data, information or knowledge that shares a common usage, purpose, associated risk or form of storage or transmission.

2.2 Identifying and securing sensitive information

Sensitive information is information, the unauthorized disclosure (or modification, alteration, destruction or denial of use) of which could compromise nuclear security or otherwise assist in the carrying out of a malicious act against a nuclear facility, organization or transport.

Such information may refer, for example, to the nuclear security arrangements at a facility, the systems, structures and components at a facility, the location and details of transport of nuclear material or other radioactive material, or details of an organization's personnel

Securing sensitive information is necessary because easy access to inadequately secured information can help adversaries to plan or commit malicious acts with relatively little effort or risk.

If, for example, a facility's physical protection plan were acquired by adversaries planning an attack on the facility, they would know the obstacles they would face, the size and arming of the guard force, the size of the response force and the approximate time it would take for that force to arrive at the site.

They would also know the important targets within the facility, their locations and the measures protecting them. Similarly, if an adversary wishing to steal nuclear material during transport succeeded in acquiring a device giving access to detailed information about the planned transport - because the device had been inadequately secured - the adversary could plan an attack more effectively. Thus, the possession of such information or information assets by adversaries would increase the likelihood of their success.

Ensuring confidentiality depends on the application of security measures to selected sensitive information and sensitive information assets (the equipment or components, including media, that process, handle, store or transmit sensitive information) in order to ensure that it does not fall into the hands of unauthorized individuals or organizations, either external or internal.

Guidance on measures against the insider threat is contained in Preventive and Protective Measures against Insider Threats [2]. Security measures should be based on risk analysis. The risk analysis should be kept up to date by a process of periodical reviews.

2.3 Information security

Information security, refers to the system, programme or set of rules in place to ensure the confidentiality, integrity and availability of information in any form [3].

At a minimum, it includes:

(a) Security of information in physical forms (e.g. paper and electronic media);

(b) Security of computer systems, sometimes referred to as computer security, information technology (IT) security or cybersecurity (additional IAEA guidance can be found in Computer Security at Nuclear Facilities [4];

(c) Security of information assets (e.g. information storage and processing equipment, communication systems and networks);

(d) Security of information about facility employees and third parties (e.g. contractors and vendors) that could compromise the security of the above;

(e) Security of intangible information (e.g. knowledge).

While confidentiality is often singled out, organizations should ensure that their information security programme addresses all three attributes. Loss of integrity or availability can negatively affect nuclear security just as loss of confidentiality can.

For example, if authorized users do not have timely access to information necessary for their duties (loss of availability), or if that information has been altered in such a manner as to mislead them (loss of integrity).

Information security should be considered and applied in the context of the overall security framework. It is closely interdependent with other security domains such as physical protection and personnel security [5].

For example, physical protection measures can be used to protect sensitive information and sensitive information assets, while confidentiality measures make attack against physical protection systems more difficult or uncertain for adversaries.

Gaps or shortfalls in any of the security domains can affect security in the others, so it is essential to use a comprehensive approach considering all domains together.

3. Framework for securing sensitive information

Securing sensitive information on a fragmented, facility by facility basis will not be effective. An effective national framework is necessary to ensure comprehensive security measures across all facilities, sites and organizations (governmental and non-governmental) handling sensitive information.

The operators should build this national framework, which will include establishing:

(a) The responsibility of the operator;

(b) A legal and regulatory framework;

(c) National guidance;

(d) Security policies;

(e) Classification schemes.

3.1 Responsibilities

The responsibility for ensuring the existence and effective operation of a countries' comprehensive nuclear security regime rests with the government of that country. Ensuring the security of sensitive information is an integral part of the nuclear security regime that the country should enforce.

Countries typically have government organizations or agencies that are responsible for overall national security, hereafter referred to as national security authorities. The national security authorities usually have the responsibility of defining the fundamental national policy on all aspects of security.

The security policies and instructions issued by the national security authorities are often general in nature, and not specifically designed for nuclear security.

However, many countries' national security authorities do have policies and guidance for securing sensitive information, for example in government or military use.

The countries relevant competent authorities should develop and issue policy and requirements specific to the security of sensitive information at nuclear material and other radioactive material associated facilities and activities.

These are usually based on, and in accordance with, any national security policy and requirements issued by the national security authorities, but taking into account the special nature of the activities that involve such materials.

The competent authorities should also maintain close liaison with the national security authorities in order for the national threat assessment or design basis threat to be devised (for more information, see Development, Use and Maintenance of the Design Basis Threat [6].

Each organization should establish its internal policy, plans and procedures for ensuring the confidentiality, integrity and availability of any sensitive information related to nuclear security that it holds or handles, and for protecting related sensitive information assets, in compliance with the national security policy and the relevant national laws and requirements. All employees should be fully aware of the need for information security and follow their organizations' information security rules and procedures.

3.2 Legal and regulatory framework for securing sensitive information

Requirements for the maintenance of nuclear security within a country' boundaries should apply to all ministries, departments, agencies and other organizations that deal with matters identified by the country to be necessary for national nuclear security. The country may impose these requirements by laws, regulations or other legally binding requirements.

There should also be legislation in place that defines the sanctions or punishment that will be applied to any individual or organization who breaches such information security requirements. Such legislation may have sections which define the severity of particular types of breach of confidentiality or other information attributes and corresponding sanctions.

The competent authorities' regulatory powers should allow them to place obligations on the holders of sensitive information. The laws enacted for this purpose should mandate sanctions or punishment for unauthorized disclosure.

The legislation should also mandate that State ministries, departments, agencies and other organizations provide the competent authorities with all necessary support to enable it to fulfil its task of ensuring the security of sensitive information.

3.3 Security policies

In addition to issuing information security policies that comply with national requirements, the competent authorities should provide details of how these requirements should be applied to facilities and activities involving nuclear material and other radioactive material.

The countries' policy on nuclear security should demonstrate a commitment to information security. It should encourage this through the issue and maintenance of a comprehensive and appropriate information security policy to be applied to all facilities and activities involving nuclear material and other radioactive material, as well as any other locations where related sensitive information is held. The aim of the policy is to ensure that sensitive information is secured against compromise

Each organization and facility that handles sensitive information should then compile its own dedicated information security policy, based on that of the competent authorities where applicable. This policy should be communicated throughout the organization in a form that is relevant, accessible and understandable to the intended users.

4. Identifying sensitive information

The first step in classifying and securing information is to identify the information that is considered sensitive information.

Security controls should be considered for information of at least the following types, which could affect nuclear security

(a) Details of physical protection systems and any other security measures in place for nuclear material, other radioactive material, associated facilities and activities, including information on guard and response forces;

(b) Information relating to the quantity and form of nuclear material or other radioactive material in use or storage, including nuclear material accounting information;

(c) Information relating to the quantity and form of nuclear material or other radioactive material in transport;

(d) Details of computer systems, including communication systems, that process, handle, store or transmit information that is directly or indirectly important to safety and security;

(e) Contingency and response plans for nuclear security events;

(f) Personal information about employees, vendors and contractors;

(g) Threat assessments and security alerting information;

(h) Details of sensitive technology;

(i) Details of vulnerabilities or weaknesses that relate to the above topics;

(j) Historical information on any of the above topics.

Some of the above information, such as personal information, may also be subject to specific security requirements under other national laws or company policies.

5. Sharing and disclosing sensitive information

5.1 Sharing information

It is sometimes necessary for certain sensitive information to be shared with authorized agencies or companies and organizations that have a need to know the information. Sharing information can create efficiencies that would not exist if the information were to be developed and handled independently.

There are also occasions where not sharing information may damage security or weaken the overall planning, design and implementation of security measures.

Furthermore, as nuclear security responsibilities are often not held exclusively by any single agency, company or organization, it is often necessary that information be shared among those who share the security responsibilities.

For example, it is often necessary in the interests of national security for the competent authorities to pass sensitive information to the national security authorities and vice versa, for example changes in threat assessments or information on security events should be communicated in a timely fashion to relevant parties, in order to enable adjustment of security measures and exchange of operational experiences as a basis for continual improvement. In addition to security considerations, information sharing may be needed to support other objectives, including safety assessment, operational and commercial needs.

It is often also necessary to share certain information with other countries or relevant international organizations. In such a case, there should be an agreement in place to guarantee that sensitive information is secured by the recipient in a manner consistent with the requirements of the owner of the information.

Security of information may be assured through a bilateral or multilateral treaty or agreement that defines how information will be secured against disclosure. Such agreements would typically describe the required protection measures to be applied to sensitive information for different classification levels in each country.

5.2 Disclosing information

Most countries have in place laws addressing the security of information of importance to the national interest. Such laws specify sanctions that will be imposed should a person, a national of that country or otherwise, breach the laws on confidentiality of such information.

There are also usually laws that regulate an individual's access to official government information. There may be mechanisms to resolve disagreements between the government and other parties regarding which information can be withheld to protect national security.

Several countries have freedom of information legislation or other laws that allow members of the public to request access to information held by the authorities. Typically, the only information that may be withheld by the authorities is that of types covered by specified exemptions, such as information associated with national defence, or private and personal information.

Other laws and regulations may require that certain types of information, which may include sensitive information, be disclosed. One example is environmental legislation that requires public reporting of specified information. It should be ensured that such laws allow exemption of information that might affect national security or the security of third parties.

6. Management framework for confidentiality

A management system should be in place that establishes policies and objectives and enables the objectives to be achieved in an efficient and effective manner. An integrated management system, The Management System for Facilities and Activities [7], is a vital support element to a nuclear security culture. Many activities at facilities are controlled by management systems.

These ideally integrate security, safety, health, environmental, quality and economic elements in a single management process or a set of integrated and mutually reinforcing systems. Information security should be integrated into the existing management system of the facility or organization to ensure information confidentiality, integrity and availability.

Ensuring the confidentiality, integrity and availability of sensitive information depends on effective designation of roles and responsibilities, classification to identify which information is sensitive and needs to be secured, why it needs to be secured and to which level, decisions on how to secure such information, implementation of the necessary security measures, and response (including recovery) if such information is compromised, stolen or lost.

The management framework explained in the following applies to all levels of management at organizations holding or handling sensitive information.

Management has the overall responsibility for ensuring information security is in place and effective throughout the facility or organization, in order to secure sensitive information.

All personnel who handle sensitive information have a responsibility to ensure its security in accordance with related national legislation as well as the organization's policies and procedures.

7. Conclusions

All information security incidents should be investigated. Policies and procedures should be defined governing information security incident investigation. An investigation should aim to determine

whether a security incident has a minor or major impact on information security and confidentiality [8].

The competent authorities may then initiate any appropriate action. An example of a minor incident may be a failure to lock up or secure a document properly that did not result in the loss or compromise of any information. A major incident, for example, may be the theft of a security plan that results in a strategic threat to an organization.

The competent authorities should maintain records of the number and type of reported information security incidents. Recurring incidents or trends in security failures should be identified and may indicate the need for changes to security policy or improvements in security procedures or programmes.

Updates on trends and changes should also be included in awareness training so that an appropriate security culture among employees and contractors is maintained. Organizations and facilities should also maintain their own records.

Bibliography

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, Vienna (2015).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[3] PANEVSKI V.S., "Opportunities for determining factors affecting the development of intelligent security systems models", 1/2020, International Scientific Journal Security & Future, 2020, ISSN:(PRINT) 2535-0668, ISSN: (ONLINE) 2535-082X, p.p. 6÷9;

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[5] PANEVSKI V.S., "COMPATIBILITY BETWEEN DESIGN OF MECHATRONIC SYSTEMS FOR CRITICAL INFRASTRUCTURE SECURITY AND TECHNOLOGICAL READINESS LEVELS", International Scientific Journal "Security & Future", 4, 3, Scientific Technical Union of Mechanical Engineering "Industry-4.0", 2020, ISSN:2535-0668, p.p. 111÷114;

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[8] Valeri Panevski, Lyudmil Nedelchev, "Structuring key partnerships in the field of critical infrastructure security systems", International Scientific Journal Innovations, 10 (2022), 2, SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING "INDUSTRY-4.0", 2022, ISSN:ISSN PRINT 2603-3763; ISSN WEB 2603-3771, p.p. 53÷56;