Funded by the European Union

CBRN Centres of Excellence
An initiative of the European Union

How to Implement Security Controls for an Information Security Program at CBRN Facilities

With the support of

unicri
United Nations
Interregional Crime and Justice
Research Institute

Action Implemented by

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Funded by the European Union

UNICRI Project 19

How to Implement Security Controls for an Information Security Program at CBRN Facilities

Prepared by the Pacific Northwest National Laboratory within the framework of the Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative (EU CBRN CoE) entitled:

"Development of procedures and guidelines to crate and improve security information management systems and data exchange mechanisms for CBRN materials under regulatory control."

December 2015

The document has been produced with the assistance of the EU. The information and views set out in this document are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Summary

Information assets, including data and information systems, need to be protected from security threats. To protect their information assets, chemical, biological, radiological, and nuclear (CBRN) facilities need to design, implement, and maintain an information security program.

The guidance provided in this document is based on international standards, best practices, and the experience of the information security, cyber security, and physical security experts on the document writing team. The document was developed within the scope of Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative.

This document is the third in a series of three documents produced by Project 19. The first document in the series, *Information Security Best Practices for CBRN Facilities,*[1] provides recommendations on best practices for information security and high-value security controls. The second document in the series, *Information Security Management System Planning for CBRN Facilities*[2] focuses on information security planning. It describes a risk-based approach for planning information security programs based on the sensitivity of the data developed, processed, communicated, and stored on facility information systems.

This document is designed to assist CBRN facilities in developing a comprehensive set of security controls to support the implementation of a risk-based, cost-effective information security program. A security control is a "safeguard or countermeasure…designed to protect the confidentiality, integrity, and availability" of an information asset or system and "meet a set of defined security requirements." (NIST 2013). Security controls cover management, operational, and technical actions that are designed to deter, delay, detect, deny, or mitigate malicious attacks and other threats to information systems. The protection of information involves the application of a comprehensive set of security controls that addresses cyber security (i.e., computer security), physical security, and personnel security. It also involves protecting infrastructure resources upon which information security systems rely (e.g., electrical power, telecommunications, and environmental controls). The application of security controls is at the heart of an information security management system (ISMS). The selection and application of specific security controls is guided by a facility's information security plans and associated policies.

Not all facilities can afford to purchase, install, operate, and maintain expensive security controls and related systems; therefore, decisions on the application of security controls have to balance considerations of security risk and resource constraints. When resources are limited, investments in security controls should focus on implementing a set of controls that provide the greatest overall risk reduction given the

---

[1] UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015a. Information Security Best Practices for CBRN Facilities. United Nations Interregional Criminal Justice Research Institute, Turin, Italy.

[2] UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015b. *Information Security Management System Planning for CBRN Facilities*. United Nations Interregional Criminal Justice Research Institute, Turin, Italy.