

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

PNNL-33582

Remote Computer Security Assessments for International Nuclear Security Capacity Building – Fiscal Year 22

September 2022

Office of International Nuclear Security

National Nuclear Security Administration

Intentionally blank

REMOTE COMPUTER SECURITY ASSESSMENTS FOR INTERNATIONAL NUCLEAR SECURITY CAPACITY BUILDING – FISCAL YEAR 22

September 2022

Prepared by
Dr. Jennifer Marek, PNNL
Michael Rowland, SNL
Greg White, LLNL

Name

under Contract Number

DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

CONTENTS

Abbreviations, Acronyms, and Initialisms iv
Executive Summary iv
1. Introduction 1
1.1 Purpose 1
1.2 Key Terms 1
1.3 Scope 2
2. Execution Strategy 3
3. Control benchmark review of an international standard 3
3.1 Selection of a benchmarking standard 3
3.2 Benchmarking process 4
4. Decision point and path forward 5
5. Example control and developed guidance 5
6. Recommended path forward 10
7. Conclusion 10
8. References 10

FIGURES

Figure 1: IEC 63096:2020 Controls Assessment for Possible Remote Assessment 4
Figure 2: IAEA Security Levels Within a Nuclear Facility (IAEA, 2021) 7
Figure 3: IEC SDs Within a Nuclear Facility 8

ABBREVIATIONS, ACRONYMS, AND INITIALISMS

CEA	cyber essential asset
DCSA	defensive computer security architecture
FY	fiscal year
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
INS	International Nuclear Security
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
RCSI	remote cybersecurity inspection
SD	Security Degree

EXECUTIVE SUMMARY

Following the outbreak of the COVID-19 pandemic that began in 2019, the U.S. federal and state governments, employers, and foreign governments enacted significant measures to restrict international travel. To further reduce the possibility of spreading the infectious disease, many employers in both the public and private domain instituted measures allowing employees to work remotely from home, where possible. In support of these measures, International Nuclear Security initiated the Remote Cybersecurity Inspection project to explore methods and tools to perform computer security assessments remotely and assist international partners in developing this capability.

In 2022, the pandemic eased and the world started a return to the former way of doing business. However, the project team realized that conducting remote inspections, even if performed partially, resulted in significant savings of resources through reduced travel costs and increased staff efficiency. New team members reflect the continued and increased interest in remote cybersecurity inspections.

This document summarizes the fiscal year 2022 efforts. Section 1 of this report describes the motivation and process used in selecting a single international standard as a test case for guidance development. Once the standard was selected, an initial review was performed to assess the applicability of remote inspection of each listed control.

Sections 2 through 4 discuss the efforts and process of the project team. The initial review results were presented and discussed with the team. It was agreed that the enormity of the effort in addressing all the low-level controls was neither feasible nor helpful to organizations looking to implement remote inspections. The team also agreed to exclude the controls considered too challenging to inspect remotely. Additionally, the team settled on a format to address each control when providing remote inspection guidance.

Section 5 provides an example inspection guidance of a selected control in the agreed-upon format. The long-term goal is to use this format and develop a guidance document for implementing remote cybersecurity inspections at nuclear facilities. Finally, Section 6 addresses possible next steps.

1. INTRODUCTION

1.1 PURPOSE

The COVID-19 pandemic affected the ability of many competent authorities to execute onsite inspections of the computer security posture of nuclear facilities. This publication aims to support these authorities and relevant stakeholders by expanding on the fiscal year (FY) 2021 efforts by developing guidance for remote cybersecurity inspections (RCSIs) for nuclear power plants (NPPs).

This remote inspection capability will then support making balanced judgments and informed decisions concerning policy, design, and development of computer security solutions in the same way onsite inspections do. This report summarizes the FY 2022 efforts and concludes with suggested follow-on actions to complete the development of the guidance document.

1.2 KEY TERMS

The term most used in this document is "assessment." The National Institute of Standards and Technology (NIST) defines a computer security control assessment as “the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for an information system or organization” (National Institute of Standards and Technology 2015). However, in most cases the INS does not perform assessments of bilateral partner countries for three reasons: 1) the United States have no regulatory basis for conducting assessments, which should be perceived as an equal partnership, assisting in increasing global nuclear security; 2) accurate assessments of nuclear facilities, especially in other disciplines such as physical security, material control, and accounting, would divulge a host country's sensitive information; and 3) it would open the United States to reciprocity requests, which are unlikely to be approved. Most equivalent facilities would not be under the Department of Energy or National Nuclear Security Administration control.

The International Atomic Energy Agency’s (IAEA's) document TDL-006, *Conducting Computer Security Assessments at Nuclear Facilities (IAEA 2016)* (a non-serial publication[1]), defines an assessment as an activity that could also be referred to as advisory service, expert visit, or self-assessment. TDL-006 continues by stating that the term *assessment* should not be construed as having authority or responsibility to an organization conducting an assessment. The use of the broader definition of an assessment aligns with this document's purpose and the computer security tasks discussed between INS and its bilateral partners.

This publication has been written to meet the need for specific guidance regarding the nuclear domain that complies with international standards, IAEA guidance, and recognized good computer security practices. To reduce confusion, the following definitions will be used in this paper when referring to *cybersecurity*:

- Computer security assessment is an activity or effort that aims to support and assist with hardening or assessing the security of computation, communication, instrumentation, and

[1] Nonserial documents are typically technical guidance by a group of experts working with the IAEA. In this case, TLD-006 was prepared with the assistance of over 30 experts in three consultancy meetings and several additional expert meetings, with input from more than 10 Member States. Serial documents are sent to all Member States for review and must receive broad consensus.

control devices that make up functional elements of the nuclear facility (IAEA 2011, 2016, 2018).

- Computer security is an aspect of information security concerned with computer-based systems, networks, and digital systems. It is a subset of information security (as defined, for example, in ISO/IEC 27000) with which it shares many goals, methodology, and terminology. The term computer security will cover the security of all computers as defined above and all interconnected systems and networks formed by the sum of the elements. For this publication, the terms "IT security," "cybersecurity," and "computer security" are considered synonyms of computer security (IAEA 2011).

In most cases competent authorities inspect and do not assess. The different use of these terms within the nuclear and cyber industries can cause confusion. Within the nuclear facility industry, *inspection* most often refers to the critical examination of cybersecurity implementations to ensure a nuclear facility's safe and secure operations.[2] Conversely, computer security *assessments* are performed to identify potential threats, vulnerabilities, and weaknesses. Regardless of the purpose, inspection or assessment, the fundamentals of remote access to these systems would be very similar. Therefore, the term *inspection* will be used in this paper to address both purposes.

Definitions of additional terms used in this publication are adopted from IAEA Nuclear Security Series No. 17 (IAEA 2011).

1.3 SCOPE

The RCSI project was initiated in 2020, and each year since the project has continued to work with national and international partners to identify best practices and lessons learned from the team's practical experience when performing a remote cybersecurity inspection.

This document summarizes the FY 2022 progress in developing a guidance document to perform RCSIs at NPPs. The goals were to:

1. Develop an RCSI controls catalog crosswalk and categorize each control as:
    a. Remote inspection is expected to be straightforward
    b. Probably can be inspected but needs to be examined further
    c. Improbable to be inspected remotely.
2. Develop an RCSI controls guide using the crosswalk to identify associated challenges, where applicable, for each control and provide methods to assess these controls via remote inspection. Where challenges are identified, provide guidance to assist the remote inspection of that control.
3. Develop an RCSI workshop outline to enhance the ability of regulators to provide effective oversight and address hesitation by some regulators to adopt remote inspections by providing a suggested process.

This report provides a summary of the accomplishments for FY 2022, an explanation of challenges identified in working toward goals, and a potential path forward for continuing to develop remote inspection guidance and implementation.

[2] https://www.nrc.gov/about-nrc/regulatory/safety-oversight.html; https://www.nrc.gov/security/cybersecurity.html

2. EXECUTION STRATEGY

The FY 2022 effort was performed through a partnership of multiple Department of Energy laboratories and international partners. Specifically, this was a combined effort between Pacific Northwest National Laboratory, Lawrence Livermore National Laboratory, Sandia National Laboratories, the U.S. Nuclear Regulatory Commission (NRC), Radiation and Nuclear Safety Authority in Finland, Consejo de Seguridad Nuclear in Spain, the Swiss Federal Nuclear Safety Inspectorate, and the Office of Nuclear Regulation in the U.K. This year, an additional team member joined the group from the Canadian Nuclear Safety Commission.

The method and analysis results at each step were discussed through regular virtual meetings. The team agreed that the first step was to identify a benchmark standard for core cybersecurity NPP controls, followed by a determination whether the controls could be evaluated remotely during an assessment. The resulting list of controls would then be crosswalked through other cybersecurity NPP standards to ensure that: (1) the controls were consistent among the standards and (2) there was no omission of essential controls. A remote inspection guidance document would then be developed to evaluate these controls. The final deliverable of developing a workshop outline would be completed based on the results of the efforts.

3. CONTROL BENCHMARK REVIEW OF AN INTERNATIONAL STANDARD

3.1 SELECTION OF A BENCHMARKING STANDARD

Several national and international standards were identified as possible benchmarks. The team discussed selecting International Electrotechnical Commission (IEC) 63096:2020, *Nuclear power plants – Instrumentation control and electrical power systems – Security Controls.*

There were some well-founded questions regarding the suitability of this standard. Specific points identified were:

1. IEC 63096:2020 is not a freely available standard. To access an IEC document, an organization must purchase it, which could significantly restrict INS's capacity-building mission with respect to countries with limited resources.
2. The copy of IEC 63096:2020 being presented during team meetings was labeled: BS IEC 63096:2020, with "BS" representing "British Standard." The issue was reaching out to all international partners using a British standard, which may not be inclusive or applicable.
3. The project's original scope provides for the inclusion of several standards for a more complete and useful result.

Points for using the IEC standard as a benchmark were:

1. Currently, there are 173 countries represented in the IEC; 89 are members and 84 are affiliates. The document used during discussions was labeled BS IEC since this was the member country through which the standard copy was purchased.
2. The standard is not associated with a specific organization.
3. There is considerable congruence between IAEA and the International Organization for Standardization (ISO) published documents and standards.

4. An added advantage is a complete listing of the controls provided in the IEC Annex.

After discussing and considering all perspectives, it was agreed the most straightforward approach was to use IEC 63096:2020 as the basis for developing a remote inspection guidance document of the listed controls. When developing the guidance document, the team members would include references to their national standards. During the remote inspection guidance development, if any controls were identified as not being addressed by the IEC standard, these controls were brought to the team for discussion.

3.2 BENCHMARKING PROCESS

Using the controls listed in the IEC 63096:2020 appendix, each control was reviewed and categorized as:

1. Possible to evaluate remotely
2. Challenging to evaluate remotely
3. Not possible to evaluate remotely.

The review results illustrated an even split between two categories, 369 were identified as possible to evaluate remotely and 371 were considered challenging to evaluate remotely. The breakdown of results for each of the topical sections in IEC 63069:2020 is provided in Figure 1.

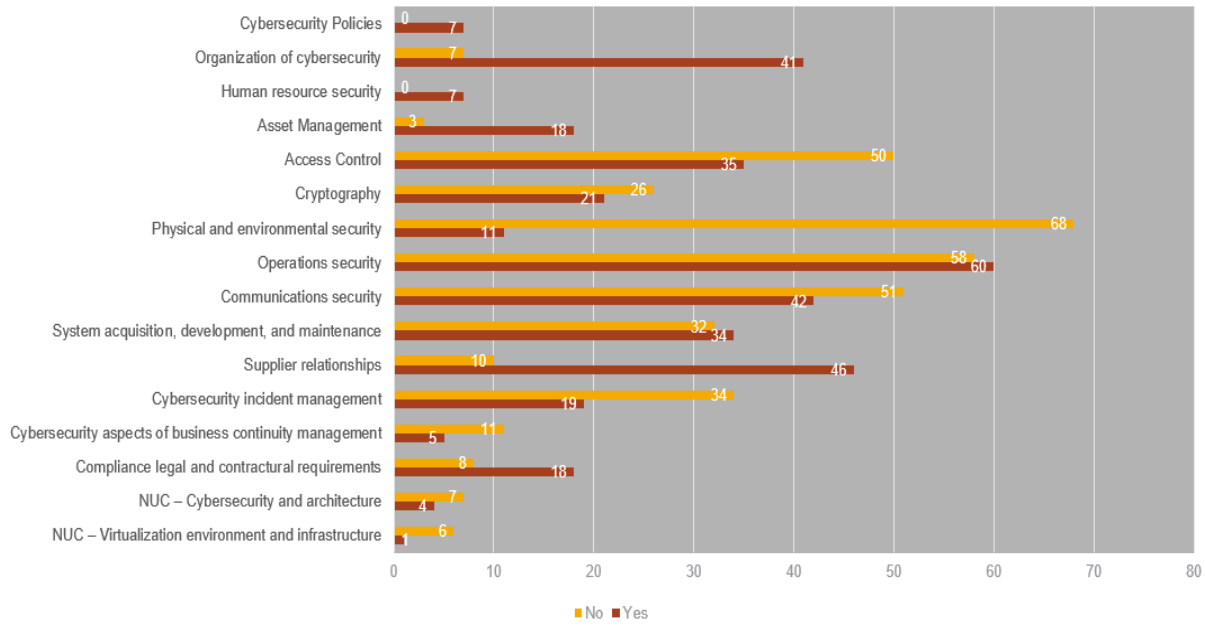


Figure 1: IEC 63096:2020 Controls Assessment for Possible Remote Assessment

The topical areas that were identified as possible to evaluate remotely were:

- Cybersecurity Policies
- Organization of Cybersecurity
- Asset Management
- Supplier Relationships

- Compliance, Legal and Contractual Requirements

The topical areas identified as not possible to evaluate remotely were:

- Access Control
- Physical and Environmental Security
- Incident Management

The team discussed how to proceed with the even split of the two categories. It was clear that the development of a complete guidance document was not possible with the remaining time in the current fiscal year with the current budget.

4. DECISION POINT AND PATH FORWARD

Given the results of the initial review of the IEC 63096 controls, it was evident that achieving the initial FY 2022 project goals and deliverables was unrealistic. The team was asked to select how they preferred to proceed:

1. For the controls that were designated as YES but may be challenging to inspect, provide additional explanatory text to assist in the remote inspection of the control.
2. For the controls that were designated as NO but may be possible to remotely inspect, provide additional explanatory text to assist in the remote inspection of the control.
3. For the controls that were not considered challenging, write more explanatory text for higher level objectives but not implementation guidance.

NOTE: Option three was selected by an overwhelming majority (86%) of the votes.

Since the project was taking a different direction than approved in the proposal, status briefings were provided to the project sponsors. It was agreed that while IEC 63096 is excellent in structuring discussions, it lacks the detail required to support remote inspections. The team decided to focus on developing explanatory text for the high-level objectives and guidance on challenges that could be encountered if the control was remotely inspected. Within the remaining FY 2022 budget and the bandwidth of the team members, it was agreed that one control would be selected and developed as an example of how the team could proceed in the next fiscal year.

5. EXAMPLE CONTROL AND DEVELOPED GUIDANCE

The team was asked for their recommendation for a control to develop as a representative example. Section 19.1 – Cybersecurity and architecture within the IEC 63096 standard was selected. It is envisioned that the final remote inspection document would contain an introductory section, and each control would have its own section containing detailed guidance. Example sections of the guidance follows.

Introduction

Protections for the facility, facility functions, actions, processes, and operations are needed to ensure the safety and security of nuclear assets. Protection against exploitation of nuclear assets and associated sensitive informational assets is the purpose of cybersecurity, which includes the architected design of the protections that implement cybersecurity operational technology

environments. The architecture is the implementation of the strategy for protecting facility functions. Segmenting a network with a heightened security profile should be grouped and separated from other devices with a lower security profile (US Department of Homeland Security, 2009). Architecture provides for defense in depth through the arrangement of zones and subzones, establishment of physical and logical control at zone boundaries (using a graded approach), and deployment of measures within the zones (using a graded approach).

Below is an example of explanatory text for the high-level objectives from IEC 63096 (International Electrotechnical Commission 2020) and guidance on challenges that could be encountered if the control was remotely inspected.

19 NUC – Cybersecurity and Architecture

19.1 NUC – Cybersecurity and architecture controls

Objective: Provide high-level cybersecurity measures and controls for the instrumentation and control and electrical systems architecture.

> *The defensive cybersecurity architecture consists of policy and programmatic requirements to ensure that architecture, once constructed, provides* ***protection to all sensitive digital assets according to the security requirements of their assigned degree, and provides the*** *greatest level of protection to* ***sensitive digital assets*** *assigned to security degree SD1 (International Electrotechnical Commission, 2020, p. 179).*
>
> The IAEA Computer Security at Nuclear Facilities technical guidance document (International Atomic Energy Agency 2021) states that reducing attack pathways to sensitive digital assets is a defensive computer security architecture (DCSA) requirement. Architecture is designed and established to eliminate or reduce cyberattack pathways to sensitive digital assets and to defend the remaining pathways against cyberattack.

19.1.1 NUC – Security Levels

> *Ensure that cybersecurity architecture defines security measures for all SDs.*
>
> *Ensure that elements within the same SD all have consistent cybersecurity measures applied.*
>
> *Security Degrees (SD) are required by policy to group required protections into stratified levels, thereby reducing the complexity of the security program implementation.*

Summary

Implementing the grouping of facilities and devices with similar security profiles, IAEA identifies five security levels in their document, *Computer Security Techniques for Nuclear Facilities* (IAEA, 2021). For each level, specific protective and preventive measures have been identified. The IAEA security levels are represented in Figure 2 (IAEA, 2021).

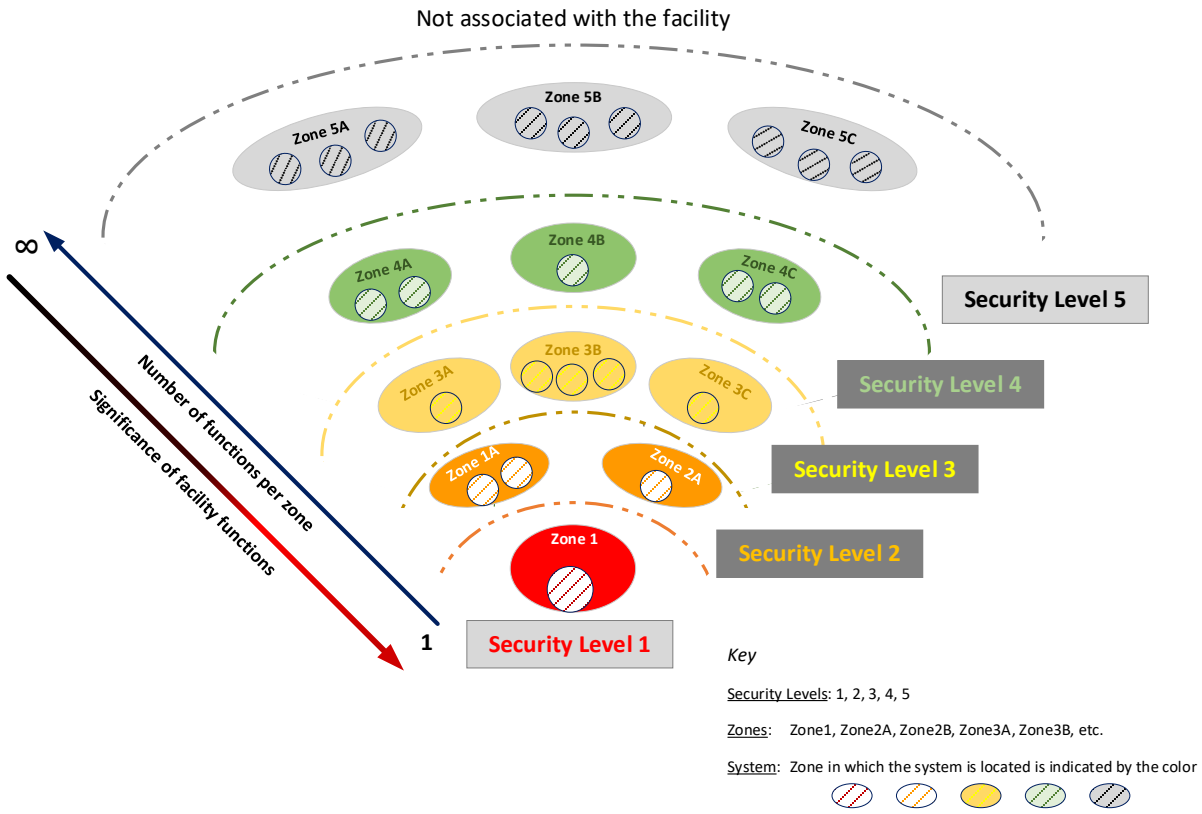


Figure 2: IAEA Security Levels Within a Nuclear Facility (IAEA, 2021)

Like the IAEA, the International Electrotechnical Commission has developed and published standards that identify and define similar protective control levels but refer to them as SDs broadly equivalent to IAEA security levels (International Electrotechnical Commission, 2019; International Electrotechnical Commission, 2020). IEC provides SD1 through SD3 (IAEA security levels 1-3), with SD1 providing the most protective requirements. The main difference between IEC and IAEA concepts is the IEC is limited to instrumentation and control and electrical systems, whereas the IAEA encompasses all functions (and the systems that perform these functions) significant to nuclear security (including safety). A diagram showing IEC security zones is provided in Figure 3.

The concept of a graded approach to the protection application is the same. Still, the IEC SDs omit technical data management (IAEA Level 4) or systems not directly crucial to technical control or operating purposes, such as office automation (IAEA Level 5). Therefore, only three zones, or levels, are provided. This is consistent with Canada, CSA N290.7:21, which uses the concept of cyber essential asset (CEA) significance,[3] determined based on the consequence of cyberattack against the safety, security, emergency preparedness, or safeguard functions performed by the system.

[3] CEA significance is a classification result of the consequences of a successful cyberattack on the most important safety, security, emergency preparedness, or safeguard functions that the CEA performs. Note: A CEA is classified into a CEA significance level of high, moderate, or low.

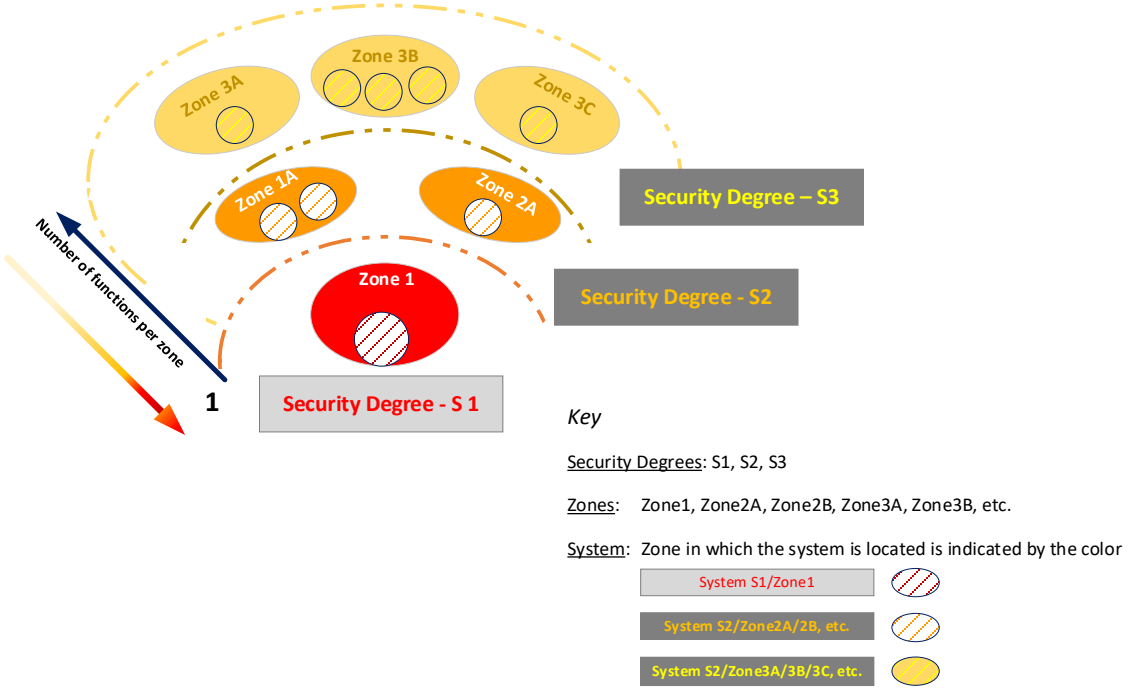


Figure 3: IEC SDs Within a Nuclear Facility

IEC 63096 outlines security controls for each SD, from SD1 to SD3, which is assigned based on the level of consequence to plant safety and performance.[4] As stated before, systems in SD1 have the most stringent requirements for protection. A documented process for categorizing sensitive digital assets for all SDs should be provided. If there is doubt as to which SD the system should be assigned, a conservative approach is recommended, and the most protective degree is selected.

Control implementation outlined in IEC 63096 (International Electrotechnical Commission, 2020) is based on proving the same level of controls and technical constraints for all systems at the same level.

Guidance, challenges, and inhibitors to remotely inspect the control

Inspecting a control for compliance can be broken into two parts, the specification within the requirements documents (laws, standards, guidance, organizational specifications, etc.) and the implementation of the specification. An inspection could look at either or both, depending on the scope. For remote inspection, field inspections to confirm implementation are the challenge.

Examples of how the control can be remotely inspected

1. Request and review
    a. Policy and procedures for assignment of SD1 to SD3, including records evidencing application of the policy and procedures.
    b. System design documents (e.g., criteria, manuals, specifications) for each SD.

[4] IEC 62645 (International Electrotechnical Commission, 2019) provides further detail on defining SDs.

c. SD requirements and DCSA specification.

d. Policy and procedures for selection of control measures and verification of requirements and DCSA compliance.

e. Assurance records for DCSA, system cybersecurity, and assurance of control measures.

f. Performance testing, assessments, and audit procedures of DCSA and control measures, including records.

2. Based on document review, request and review threat and risk assessments defined by the design basis threat for systems within each of the SDs.

Examples of potential challenges and inhibitors to remotely inspect the control (incorporate lessons learned from FY 2022 as relevant)

1. Performing field inspection to confirm implementation, which would demand onsite inspections.
2. Requirements for design and the actual implementation of systems can vary significantly due to:
   a. Misunderstanding of the requirements
   b. Lack of documentation on why a system receives a specific designation, so the SD designation is not repeatable for similar systems
   c. Lack of regard for the need for required security controls
   d. Lack of education or training so security controls are not configured correctly and consistently.
3. Information protection requirements are addressed in an additional RCSI Working Group document, *Cybersecurity Remote Inspection Information Security Guide* (White & Rowland, 2022). Classifying and protecting sensitive information is critical to any inspection effort and is more complicated when the inspection is hybrid or fully remote. Information protection is often specified in national regulations and laws, with specific guidance to the nuclear industry provided by the regulator. This guidance will direct the regulator and facility to specific solutions for information protection while performing hybrid or fully remote inspections. Some key topics that are covered in more detail in the guide are:
   a. Security Considerations for Remote Inspections (section 4.6)
   b. Cybersecurity for Remote Inspector's Computers (section 4.7)
   c. Preparing for a Remote Inspection (section 5)
      i. Paper Documentation Considerations (section 5.2)
      ii. Electronic Documentation (section 5.3)
      iii. Remote Inspectors at Regulator's Offices and Home ((White & Rowland, 2022)sections 5.4 and 5.5)
      iv. Remote Inspection Video Conferencing Considerations (section 5.6)
   d. Typical Inspection Activities (section 6)
      i. Document Review (section 6.1)
      ii. Direct Observations (section 6.2)
      iii. Considerations for Remote Inspection Interviews with Personnel (section 6.3)
      iv. Finalization Stage and Report Writing (section 7)

6. RECOMMENDED PATH FORWARD

To fully realize the benefits of the remote inspection team's work that has been performed, the following future actions are recommended:

1. Prioritize and develop the remainder of the controls. One control was selected and developed to demonstrate how the control could be remotely inspected. The remainder of the controls must be equally developed based on the priority of that control. The priority can be determined by surveying the whole team, similar to the survey selecting the example control.
2. Develop a 2- to 3-day course to cover information protection, assessment of controls, and walking through an exercise.

7. CONCLUSION

The international team has provided their experience and lessons learned, and shown remote inspections are possible and a valuable tool for regulatory inspectors. It provides a method to reduce time in the field, and project team members have reported no identified reduction in the quality effectiveness of the inspections.

The efforts in FY 2022 have been more successful than expected. This success has required the project to reduce the scope to allow the team to focus on specific actions that the inspector can take to perform an effective inspection.

Recommended actions in FY 2023 and later provide a practical conclusion and will allow the effort to be put to practical and effective use.

8. REFERENCES

CISA. (2020). Downloading and Installing CSET. Retrieved 10 02, 2020, from Cyber Security Evaluation Tool (CSET®): https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET

Findlay, T. (2019). THE IAEA'S ROLE IN NUCLEAR SECURITY SINCE 2016. GLOBAL DIALOGUE ON NUCLEAR SECURITY PRIORITIES.

Fisher, M. (2020g, July 16). Nuclear Power Operators Use Remote Assessments to Overcome Pandemic Mobility Restrictions. Retrieved from International Atomic Energy Agency: https://www.iaea.org/newscenter/news/nuclear-power-operators-use-remote-assessments-to-overcome-pandemic-mobility-restrictions

IAEA. (2011). Computer Security at Nuclear Facilities. Retrieved from INTERNATIONAL ATOMIC ENERGY AGENCY: https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities

IAEA. (2011). Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). Vienna : IAEA.

IAEA. (2016). Conducting Computer Security Assessments at Nuclear Facilities. Retrieved from INTERNATIONAL ATOMIC ENERGY AGENCY: https://www.iaea.org/publications/10999/conducting-computer-security-assessments-at-nuclear-facilities

IAEA. (2016b). COMPUTER SECURITY FOR NUCLER SECURITY. Vienna: International Atomic Energy Agency.

IAEA. (2017, August). IAEA Nuclear Security Technical Guidance. Retrieved July 19, 2022, from International Atomic Energy Agency: https://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst047.pdf

IAEA. (2017b). COMPUTER SECURITY TECHNIQUES FOR NUCLEAR FACILITIES. Vienna: International Atomic Energy Agency.

IAEA. (2018). Computer Security of Instrumentation and Control Systems at Nuclear Facilities. Retrieved from INTERNATIONAL ATOMIC ENERGY AGENCY: https://www.iaea.org/publications/11184/computer-security-of-instrumentation-and-control-systems-at-nuclear-facilities

IAEA. (2019). International Nuclear Security Advisory Service (INSServ) Guidelines. Retrieved from International Atomic Energy Agency: https://www.iaea.org/publications/13527/international-nuclear-security-advisory-service-insserv-guidelines

IAEA. (2020a). Integrated Nuclear Security Support Plan (INSSP). Retrieved 10 02, 2020, from International Atomic Energy Agency: https://www.iaea.org/topics/integrated-nuclear-security-support-plan-inssp

IAEA. (2020b). International Nuclear Security Advisory Service (INSServ). Retrieved 10 02, 2020, from International Atomic Energy Agency: https://www.iaea.org/services/review-missions/international-nuclear-security-advisory-service-insserv

IAEA. (2020c). International Physical Protection Advisory Service (IPPAS). Retrieved 10 02, 2020, from International Atomic Energy Agency: https://www.iaea.org/services/review-missions/international-physical-protection-advisory-service-ippas

IAEA. (2020d). Nuclear Security Series. Retrieved 10 02, 2020, from International Atomic Energy Agency: https://www.iaea.org/resources/nuclear-security-series

IAEA. (2020e). Training courses. Retrieved 10 02, 2020, from International Atomic Energy Agency: https://www.iaea.org/services/education-and-training/training-courses

IAEA. (2021). Computer Security Techniques for Nuclear Facilities - Technical Guidance (Rev. 1 ed.). Vienna, Austria: International Atomic Energy Agency. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf

International Electrotechnical Commission. (2019). IEC 62645 Nuclear power plants - Instrumentation, control, and electrical power systems - Cybersecurity requirements. Geneva, Switzerland.

International Electrotechnical Commission. (2020). IEC 63096 Nuclear power plant - Instrumentation, control and electrical power systems - Security Controls. Geneva, Switzerland: IEC.

Joint Task Force Transformation Initiative. (2015, 01 22). Security and Privacy Controls for Federal Information Systems and Organizations. Retrieved from NIST: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

NRC. (2010). REGULATORY GUIDE 5.71 - CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES . U.S. NUCLEAR REGULATORY COMMISSION.

NRC. (2017a, August 29). § 73.54 Protection of digital computer and communication systems and networks. Retrieved from Nuclear Regulatory Commission: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html

NRC. (2017b, August 29). General Provisions. Retrieved from Nuclear Regulatory Commission: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html

NRC. (2020a, July 29). Operator Licensing. Retrieved from United States Nuclear Regulatory Commission: https://www.nrc.gov/reactors/operator-licensing.html

NRC. (2020b, February 21). Fuel Cycle Facilities. Retrieved from Nuclear Regulatory Commission: https://www.nrc.gov/materials/fuel-cycle-fac.html

US Department of Homeland Security. (2009). Cyber Security Procurement Language for Controls. Washington, DC: US Government.

White, G., & Rowland, M. (2022). Cybersecurity Remote Inspection Information Security Guide. Livermore, CA: U. S. Department of Energy.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov