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 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. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

ORNL/SPR-2025/3994

Capability Building Progression of an Insider Threat Mitigation Program at an International Research Reactor

August 2025

National Nuclear Security Administration

Intentionally blank

ORNL/SPR-2025/3994

CAPABILITY BUILDING PROGRESSION OF AN INSIDER THREAT MITIGATION PROGRAM AT AN INTERNATIONAL RESEARCH REACTOR

Oak Ridge National Laboratory

Alyson Coates

Garl Bultz

Y-12 National Security Complex

Jason Davenport

Russ Clark

Date: **July 2025**

Prepared by

OAK RIDGE NATIONAL LABORATORY

Oak Ridge, TN 37831

Managed by

UT-BATTELLE LLC

for the

US DEPARTMENT OF ENERGY

under contract DE-AC05-00OR22725

Intentionally blank

CONTENTS

LIST OF TABLES

Intentionally blank

ABBREVIATIONS, ACRONYMS, AND INITIALISMS

A/CPPNM	Convention on the Physical Protection of Nuclear Material and its 2005 Amendment
BOP	behavioral observation program
DBT	design basis threat
EAP	employee assistance programs
IAEA	International Atomic Energy Agency
INFCIRC	Information Circular
INS	Office of International Nuclear Security
ITM	insider threat mitigation
ITMP	insider threat mitigation program
NMAC	nuclear material accounting and control
NPP	nuclear power plant
NSC	nuclear security culture
NSS	Nuclear Security Series
PPS	physical protection system
RR	research reactor
RTS	representative threat statement(s)
SOP	standard operating procedure
TID	tamper-indicating device

Intentionally blank

EXECUTIVE SUMMARY

The nuclear industry recognizes the difficulties involved in developing effective managerial and leadership skills in a highly technical and proficient workforce such as that found in nuclear facilities. Implementing an insider threat mitigation program (ITMP) within the nuclear industry is a complex and ongoing process that demands a comprehensive understanding of human behavior, an organization's security culture, and rigorous regulatory requirements yet also accounts for facility characteristics, physical security, material flow, and activities involving nuclear material. Given the high-consequence nature of research reactor operations, even minor lapses can lead to safety, security, and reputational risks. An effective ITMP requires a defense-in-depth approach that incorporates behavioral analysis, robust vetting procedures, continuous monitoring, and cross-disciplinary coordination. It must also promote a culture of vigilance and accountability at all levels up to and including executive leadership but be flexible enough to adapt to evolving global threats and technological advances. Insider threat mitigation is not a one-time effort but rather a sustained commitment to excellence in safety and security. Establishing a culture in which personnel proactively report incidents and issues that could affect nuclear safety and security is vital to maintaining a safe and secure operational environment.

This document was developed to guide senior management and research reactor organizations in creating comprehensive programs to effectively manage and mitigate insider threat behaviors and actions. It focuses on the key pillars of an effective ITMP, including the national legal framework, security culture, preventive and protective measures, cyber security, and performance evaluation. By using a systematic approach during implementation, facilities can foster environments conducive to insider threat detection and support long-term program sustainability. The document also provides strategies for improving communication across all levels of an organization, helping to eliminate barriers that hinder the development of robust ITMPs and enhance overall security culture. In today's organizations, the concept of leveraging safety and security culture lessons to facilitate knowledge transfer is rapidly evolving to expedite insider threat management and security culture improvements.

This document outlines the rationale for evaluating an ITMP based on national customs, culture, and stakeholders. The elements are all germane to reliability and trustworthiness and relate to security concerns that states may encounter. The document focuses not only on individual perceptions regarding security issues and capability building but also on team building and how to resolve concerns. The implementers of a facility's ITMP may zero in on indicators of insider threats within their enterprise. This material will benefit organizations when it is applied using a systematic and structured approach as demonstrated throughout the document.

Intentionally blank

CHAPTER 1

1. INTRODUCTION

With threats to nuclear facilities continuously evolving, the development and implementation of insider threat mitigation programs (ITMPs) are increasingly important. The Office of International Nuclear Security (INS) within the U.S. Department of Energy's National Nuclear Security Administration developed *Capability Building Progression of an Insider Threat Mitigation Program at an International Research Reactor* to assist newcomers and existing research reactor (RR) organizations in addressing insider threats and establishing effective response measures for insider activities.

In the realm of insider threat mitigation (ITM), capability building refers to a systematic approach that leverages education, training, exercises, awareness initiatives, workforce and knowledge management, and knowledge networks to develop and continuously enhance the competencies and capabilities needed—at governmental, organizational, and individual levels—to establish, implement, and sustain effective ITMPs [1]. *Capability building* is often used interchangeably with *capacity building*; however, *capacity building* focuses on an organization's ability to perform.

This report is based on a similar report created by INS for nuclear power plants (NPPs) *Capability Building Progression of an Insider Threat Mitigation Program at an International Nuclear Power Plant*.

RRs differ from NPPs by application, fuel enrichment, power level, and location. NPPs are mainly used to produce power, whereas RRs have various applications such as producing neutrons for research, radioisotope production, material testing, medical treatments, education, and training. NPPs are typically located in rural areas, whereas RRs are commonly located in urban areas (e.g., at universities). NPPs typically use ^{235}U enriched to 3%–5%, whereas RRs use ^{235}U enriched up to 20%. Some RRs use highly enriched ^{235}U, with enrichment levels of up to 93%. NPP power levels are typically between 1,200 and 3,000 MWt. RRs can be categorized into three power levels. Low-power RRs operate at ≤ 1MWt and are typically used for educational purposes, training, and small-scale research. Medium-power RRs operate at 1 to 100 MWt and are typically used for a variety of research purposes, including materials testing and neutron research. High-power RRs operate at >100 MWt and are typically used for advanced research, including large-scale experiments and the production of medical isotopes. Apart from their applications, fuel enrichment, and power levels, RRs are subject to distinct security challenges stemming from specific facility configurations, less robust safety systems, dose rates, material attractiveness, ease of access to material, stakeholders, resources/staffing, and reactor age. As a result, security may not have been a priority during their design.

Specific Configurations

A typical RR facility comprises the reactor itself along with associated facilities, such as a neutron beam experiment hall, hot cells for handling irradiated materials, experiment assembly rooms, beam tubes and rabbit systems, and storage areas for fresh and irradiated fuel [3]. RRs are designed to facilitate easy access to the core for the introduction or removal of experiments. Exposed cores and hand tools for the removal of assemblies are designed to enable frequent core reconfigurations. Additionally, glass-walled control rooms facilitate instruction and training, and access to resident

computer systems provides data and network connectivity. Furthermore, RRs use open and exposed spent fuel pools to reduce costs, often at the sacrifice of security considerations [2].

Less Robust Safety Systems

Because of their lower thermal energy and fission product inventory, an RR generally poses less of a hazard than an NPP. Consequently, RRs need less complex safety features to meet regulatory requirements. Thus, an RR may have fewer and less diverse safety systems than an NPP, with fewer redundancies, and its systems may also be less robust. As a result, such safety systems may be more susceptible to being compromised by an insider. These circumstances may amplify the consequences of sabotage, particularly in scenarios in which safety functions also serve security purposes [2].

Dose Rates

RRs typically use a form of uranium that is more highly enriched than that used in NPPs. The duration and frequency of the operation of an RR, especially one that is underused, may also be such that fuel burnup is low and dose rates from spent or irradiated fuel are less likely to be immediately incapacitating to an insider. An RR may, therefore, hold material that is a more attractive target for unauthorized removal by an insider than that held at an NPP [2].

Material Attractiveness

The material at an RR may be more attractive than the material at an NPP. The physical form of RR fuel assemblies—specifically, their size and weight, which affects their portability—increases material attractiveness. RR operations often involve frequent on-site movements of material, and these movements may not consistently adhere to defined, formal security protocols. This informality can create security vulnerabilities, particularly concerning unauthorized removal, which is influenced by the frequency and duration of material movements as well as the attractiveness of the material being handled. RRs should effectively manage the level of risk associated with the potential consequences of unauthorized removal and/or sabotage of nuclear or other radioactive materials. Risk is determined by the potential consequences of such an act, should it occur, and the likelihood of the act happening [2].

Ease of Access to Material

The operational framework of RRs often requires an environment where research areas are easily accessible to technically skilled contractors, staff, guest scientists, students, and other visitors. The presence of a significant number of temporary personnel with unescorted access poses challenges for nuclear security systems. Furthermore, the culture of information sharing and data transparency essential for the research community—driven by the need to remain competitive and viable—can introduce vulnerabilities to nuclear security systems, including the protection of computer-based systems [2].

Stakeholders

Most RRs are owned and/or supported by various organizations, typically of differing types. This diversity can affect the reliability of funding because competing priorities—especially concerning security—can arise [2].

Resources/Staffing

At all but the largest RRs, nuclear security responsibilities are often assigned as one of several duties to a single staff member. Staff tasked with security frequently lack specialized experience and

knowledge of the security systems and measures in place. This issue can be further compounded by a shortage of security expertise among senior management personnel within the organization and/or the regulatory authority, limiting their capability to conduct effective oversight and maintain checks and balances. A lack of expertise can lead to several consequences:

- Oversight and implementation of security responsibilities may be overlooked.
- Security responsibilities may be addressed, but the resulting security measures may be inefficient because of a limited depth of knowledge and experience.
- Security responsibilities may be delegated to a commercial contractor, who may prioritize profit over effective security [2].

Age

Over 70% of RRs are more than 30 years old, which means they were typically constructed using older technology and with insufficient attention given to security considerations during their design and construction. Although many of these reactors have undergone upgrades, such improvements may not have adequately addressed security. Additionally, the effectiveness of security features originally installed or subsequently added may have deteriorated with age. The following are examples of security vulnerabilities caused by aging:

- Insufficiently robust barrier design
- Degradation of security and safety components
- Inability to support upgrades because of inadequate infrastructure or structural integrity
- External contractors accessing the facility and/or its security features during upgrades without undergoing trustworthiness checks
- Obsolescence of security systems
- Facility configuration or geometry that cannot accommodate necessary security upgrades [2]

Because of the distinct security challenges RRs are subject to, regulators and organizations must consider a graded approach to security and the implementation of ITMPs based on radiological consequences and material attractiveness.

ITMP efforts should be tailored to the specific risks and vulnerabilities of a facility, not applied as a one-size-fits-all solution.

This report suggests capability building areas that should be considered in developing or strengthening an ITMP. The goal of ITM capability building is to strengthen the capability of relevant stakeholders to assess, develop, and implement the components of an ITMP designed using a defense-in-depth strategy and composed of preventive and protective measures. ITM capability building is accomplished by developing and strengthening the processes/tools, knowledge/skills, and behaviors that organizations need to prevent, detect, respond to, and minimize the risks posed by malicious insiders. ITM capability building is not only about acquiring new skills but also about transforming mindsets and attitudes toward ITM. To embark on capability building, senior leaders need to be actively engaged in the process and set the precedent for the rest of the organization. Capability building requires participation from all levels of an organization, not just from senior leaders. The capability building progression outlined here can be used to implement a new ITMP or evaluate an existing ITMP. It can also be used to conduct a gap analysis of a current program and identify capability areas that are missing or need improvement or additional training.

The state is responsible for establishing the national legal and regulatory framework, but the organization and individuals at all levels of an organization must actively participate in ITM capability building. The organizations involved in an ITMP should create capability building programs for management, personnel, and other relevant stakeholders, focusing on ITM systems and measures pertinent to their roles. Individuals at all levels of an organization should enhance their knowledge, skills, and capabilities for ITM through education, training, awareness-raising activities, and practical exercises [1].

The ITMP described in this report directly supports states in meeting their obligations as signatories to the Convention on the Physical Protection of Nuclear Material [2] and its 2005 Amendment (A/CPPNM) [3], which requires state parties to establish and maintain appropriate physical protection regimes to safeguard nuclear material and facilities against theft and sabotage. In particular, this report provides practical guidance on implementing key measures associated with the amendment's Fundamental Principle E, "Responsibility of the License Holders," by establishing a facility ITMP; Fundamental Principle H, "Graded Approach," by applying a graded approach to risk mitigation; and Fundamental Principle I, "Defense in Depth," by integrating defense-in-depth strategies into an ITMP using preventive and protective measures and ensuring that individuals granted access to sensitive materials and facilities are trustworthy and reliable. By detailing good practices for ITMPs—spanning personnel security, physical protection, nuclear material accounting and control (NMAC), cybersecurity, system evaluation and performance assurance (Fundamental Principle J, "Quality Assurance"), and nuclear security culture (NSC) (Fundamental Principle F, "Security Culture")—this report offers RR organizations an operational framework for fulfilling the requirements of the A/CPPNM. The report reinforces international commitments, such as those outlined in International Atomic Energy Agency (IAEA) Information Circular (INFCIRC) 908 [4], emphasizing the continuous assessment and improvement of ITM measures.

CHAPTER 2

2. CONTENT ORGANIZATION

This report is a guide and reference for RR senior management and organizations that highlights essential elements and specific capabilities recommended for inclusion in an ITMP. The capabilities in this report are derived from INS's *Insider Threat Mitigation Program: Facility Implementation Handbook* [5], INS's *Security Self-Assessment Toolkit for Nuclear Materials Facilities* [6], IAEA Nuclear Security Series (NSS) No. 7-G (*Nuclear Security Culture*) [7], No. 8-G (*Preventive and Protective Measures against Insider Threats*) [8], and No. 31-G (*Building Capacity for Nuclear Security*) [1]. The capabilities are meant to be a starting point for developing a new ITMP or a means to assess an existing ITMP to identify gaps. If a capability is found to be lacking, responsible personnel should determine what steps are needed to increase understanding, knowledge, or staffing.

This report is organized into essential elements, each designed to guide the development, implementation, and maintenance of a comprehensive ITMP. Users are encouraged to apply a graded approach—tailoring efforts based on risk and context—when identifying potential targets and adversaries and when determining the necessary capabilities at the organizational and individual levels.

The sections on each essential element provide summaries of recommended capabilities based on the processes/tools, knowledge/skills, behaviors, and resources needed to support the development or assessment of an effective ITMP. Additionally, the appendices present a variety of capabilities to help establish a defense-in-depth approach, ensuring that the failure of any single element does not leave an organization vulnerable to insider threats.

The essential elements of an ITMP are as follows:

1) National legal and regulatory framework
2) ITMP plan
3) NSC
4) Preventive measures/personnel security
5) Protective measures
    a. Physical security
    b. NMAC
    c. Cybersecurity
    d. Protective forces
6) Plant operations
7) System evaluation and performance assurance
8) Continuous improvement
9) System sustainability

When reviewing and applying this document, RR organizations should take into account their unique organizational structures and adopt a graded approach to determine the necessary capabilities while

effectively balancing risks and costs. Smaller facilities may not be able to implement all capabilities because of limited resources and staffing.

2.1. NATIONAL LEGAL AND REGULATORY FRAMEWORK

The IAEA's Nuclear Security Fundamentals series asserts that the responsibility for nuclear security within a state lies solely with the state. The state must ensure the security of nuclear material, other radioactive material, related facilities, and activities under its jurisdiction [1] [9]. A robust national legal and regulatory framework provides the foundation for ITMPs. Such a framework guides organizations in establishing defense-in-depth and graded approaches tailored to the risks associated with specific facilities, materials, and operational contexts.

A clear understanding of this framework ensures effective coordination between national authorities, regulatory bodies, and facility organizations, thereby promoting security and resilience against insider threats. A national framework establishes clear parameters for action by defining the roles and responsibilities of organizations, regulators, and other stakeholders. By specifying the boundaries within which facilities must operate, regulatory frameworks create a consistent and coherent approach to ITM [5]. Aligning national frameworks with international standards such as those outlined in the IAEA's NSS ensures that organizations are able to administer ITMPs consistently and collaborate with global security efforts. National standards provide benchmarks for implementing effective ITM measures and facilitate international collaboration to address shared risks [5].

The suggested national legal and regulatory framework capabilities of organizations and individuals detailed in **Error! Reference source not found.Appendix A** should be considered.

2.1.1. National Legal and Regulatory Framework Processes/Tools

Organizations should develop meaningful and useful policies and procedures based on the national legal and regulatory framework.

2.1.2. National Legal and Regulatory Framework Knowledge/Skills

To create effective and practical policies and procedures, organizations must employ individuals who thoroughly understand the regulatory framework and possess the knowledge and resources to translate legal requirements into actionable practices. These individuals should be well-versed in compliance requirements and restrictions, particularly when developing trustworthiness policies that take into account personal privacy and job requirements.

Individuals should be trained in their roles and responsibilities related to ensuring compliance, the importance of a questioning attitude, and reporting and correcting deficiencies.

2.1.3. National Legal and Regulatory Framework Behaviors

Individuals should acknowledge that laws and regulations form the foundation for policies and procedures. Everyone involved in activities related to nuclear safety or security is responsible for acting in a manner that supports organizational success. This responsibility includes ensuring compliance with regulations, fostering a questioning attitude, and actively reporting and addressing any deficiencies.

2.1.4. National Legal and Regulatory Framework Resources

Organizations should prioritize resource allocation to provide sufficient human, financial, and technical resources for compliance with the national legal and regulatory framework.

2.2. ITMP PLAN

Facility organizations play a crucial role in translating national legal and regulatory frameworks into practical and effective security measures. To develop these measures, organizations must first create comprehensive security plans that include ITMP plans designed to address the design basis threat (DBT)/representative threat statement(s) (RTS). A security plan should outline the measures implemented to fulfill the state's physical protection objectives and requirements. It must be based on thorough analysis and supported by sufficient information to demonstrate that the state's requirements will be met upon implementation. The security plan should also provide assurance that the physical protection system (PPS) effectively addresses threats identified in threat assessments or the DBT/RTS [10]. Appendix A in INS's ITMP handbook, *ITM Facility Program Plan Template*, provides a sample ITMP plan outline [5].

The ITMP plan should include a graded approach and defense-in-depth strategies such as layered access controls, management of nuclear and other radioactive material, and strong cybersecurity protocols. By tailoring measures to facility-specific risks and vulnerabilities, organizations can ensure that resources are used efficiently while maximizing the effectiveness of security measures.

Information and capabilities discussed in this report can be used in completing sections of the ITMP plan.

The suggested ITMP plan capabilities of organizations and individuals detailed in **Error! Reference source not found.Appendix B** should be considered.

2.2.1. ITMP Plan Processes/Tools

Organizations should develop processes and tools to establish defense-in-depth strategies for implementing ITMPs. Managing internal threats through effective policies, security measures, and procedures is a fundamental organizational value. Organizations should incorporate ITM into operating and security standards, special procedures, and directives. Additionally, organizations should place a strong emphasis on raising awareness of nuclear security issues and capacity building initiatives at all organizational levels. A systematic approach to capability building should be integrated into the management system and supported by mechanisms for monitoring and evaluating individual and organizational performance. This strategy promotes feedback to identify areas for improvement in personnel training, organizational structure, and procedures. Comprehensive training programs, including regular exercises, should be developed to enhance and sustain skills, assess plans, and foster attitudes and behaviors that promote robust NSC. Moreover, effective coordination at the organizational level is crucial for planning, operations, and communication across relevant entities to prevent, detect, and respond to criminal or other security threats involving nuclear material, other radioactive substances, associated facilities, or related activities.

2.2.2. ITMP Plan Knowledge/Skills

To create an effective ITMP plan, organizations must have knowledgeable and skilled individuals proficient in essential aspects of threat assessment, including the evaluation of DBT/RTS and insider

threats, target identification, vulnerability assessments, and preventive measures. These individuals should receive training in developing and implementing ITMPs and using resources such as INS's *ITMP Handbook* and IAEA's NSS No. 27-G. They must also be capable of identifying potential insiders, understanding the motivations behind insider threats, and recognizing facility targets that may pose significant radiological risks. Furthermore, organizational personnel should have a solid understanding of ITMP components and the design, evaluation, implementation, and maintenance of a PPS and contingency plans. The workforce must be well-acquainted with facility-specific ITM policies and procedures to ensure compliance with state and regulatory requirements. Training should cover identifying job functions that require unescorted access to sensitive areas, establishing trustworthiness criteria, and maintaining a list of authorized positions. Individuals should actively comprehend their roles in ITM, uphold necessary qualifications, and facilitate knowledge transfer by mentoring and training others within their organizations.

2.2.3. ITMP Plan Behaviors

Organizations should recognize the significance and actively support the implementation of ITMPs through communication and action. An organization should position the ITMP as a fundamental organizational value and emphasize that security and ITM are shared responsibilities. Management enforces ITM policies and procedures, ensuring that all individuals understand and embrace this collective responsibility. Consequently, personnel are committed to effectively implementing policies, security measures, and procedures to manage internal threats, reinforcing ITM as a core organizational value.

2.2.4. ITMP Plan Resources

Organizations should prioritize the allocation of sufficient human, financial, and technical resources to develop, implement, and maintain ITMPs.

2.3. NSC

NSC is an assembly of characteristics, attitudes, and behaviors exhibited by individuals, organizations, and institutions that supports and enhances nuclear security. NSC is vital to ensuring that all personnel remain vigilant and that measures are implemented to prevent and address sabotage or the malicious use of radioactive material. A comprehensive nuclear security regime involves various components, including legislation and regulations, intelligence gathering, threat assessments related to radioactive material and relevant facilities, administrative systems, technical hardware systems, and response capabilities, all of which work alongside ITM activities. No singular government, industry organization, or subdivision of these entities can effectively manage these components in isolation. A resilient NSC is built on effective organizational planning, training, and awareness. Even a well-crafted system may falter if operating and maintenance procedures are inadequate or personnel fail to follow established protocols. Therefore, the success of the nuclear security regime hinges on the people involved, particularly those in leadership. Enhancing NSC involves prioritizing the human factor, especially management leadership.

Furthermore, NSC reflects the personal commitment, accountability, and understanding of every individual engaged in actions that affect nuclear security. Cultivating NSC is challenging; however, it can be fostered through role models, training, positive reinforcement, and structured processes.

These methods should be taken into account as states develop or revise their regulatory and policy documents. NSC is dynamic and requires continuous vigilance to prevent deterioration over time. Leadership must nurture and maintain NSC by providing visible support, exemplifying strong behaviors, and encouraging open communication. Without regular monitoring and proactive improvement efforts, NSC can weaken, creating vulnerabilities within organizations.

Effective leadership is fundamental to successful NSC because leaders set the organizational tone regarding security by prioritizing it, promoting accountability, and driving improvement. Key leadership actions include engaging with employees to foster trust and encourage reporting of security concerns; promoting accountability by reinforcing that security is a shared responsibility; investing in resources to ensure that training, employee assistance programs (EAPs), and promotional initiatives receive adequate support; and adapting to evolving threats by regularly updating NSC programs in response to technological advancements and emerging risks.

RR staff may not possess a strong NSC; specifically, there may be a prevailing belief that research priorities can take precedence over adherence to safety and security regulatory requirements. The operating organizations of RR facilities may also lack an appropriate NSC, perhaps viewing the reactor's mission as more critical than compliance with regulatory mandates. This situation can be aggravated by a shortage of nuclear security expertise and/or a lack of organizational independence within the regulatory entity, particularly in countries where the promotion of nuclear research and regulatory oversight fall under the same government organization. Such circumstances can lead to ineffective regulatory oversight. Together with the absence of an NSC among researchers, this situation can significantly hinder the effective implementation of security measures [2].

Although nuclear safety and security both consider the risks of inadvertent human error, nuclear security places a greater emphasis on intentional acts meant to cause harm. Because nuclear security addresses deliberate actions, it requires distinct attitudes and behaviors, such as maintaining information confidentiality and actively deterring malicious acts. These behaviors differ from those of safety culture. The IAEA report, *A Systems View of Nuclear Security and Nuclear Safety: Identifying Interfaces and Building Synergies*, emphasizes the importance of applying lessons from safety culture to strengthen security culture and capability building [11]. Conducting an analysis of NSC and developing a facility-specific program are essential steps toward ensuring a robust security culture.

Organizations should consider the suggested NSC capabilities detailed in **Appendix C**, which underscore the fact that nuclear security ultimately relies on individuals—policymakers, regulators, managers, and employees—as outlined in the IAEA's NSS No. 7-G, *Nuclear Security Culture* [7].

2.3.1. NSC Processes/Tools

Personnel should be encouraged to report security concerns and suspicious behavior, and organizations should establish an anonymous method for employees to voice concerns. Additionally, there should be a formal process in place to handle employee grievances. Management must ensure that security-related experiences and events, including those that occur in other locations, are thoroughly analyzed so that appropriate enhancements or corrective actions can be implemented as necessary. An EAP is a vital resource for addressing stressors, enhancing employee well-being, and reducing risks associated with insider threats. Stressful life events, personal dissatisfaction, and financial challenges heighten insider risks; thus, proactive support is essential. Organizations should

provide EAPs that help alleviate personal stressors and offer resources with the goal of mitigating insider threat risks.

2.3.2. NSC Knowledge/Skills

Training and professional development are crucial for establishing cultural behavioral norms. Training should build awareness, clarify roles, and reinforce accountability on all personnel levels. Additionally, training should combat complacency, ensuring that personnel are attentive to their responsibilities. Specialized training for managers should emphasize leadership within NSC, and periodic refresher courses should address emerging threats and reinforce organizational policies. Organizations should provide a range of training options, including managerial training, general awareness training, and specialized security training.

2.3.3. NSC Behaviors

Through their actions, managers exemplify their commitment to nuclear security and play a vital role in fostering NSC within organizations. They must ensure effective communication internally and, when appropriate, with external organizations; they must also safeguard sensitive security information. In a robust NSC, all personnel are accountable for their conduct and motivated to uphold nuclear security. Employees should be expected to act in a manner that indicates their awareness of the circumstances and potential consequences of their behavior. The beliefs and attitudes of individuals are shaped by the actions of their peers—particularly those of top management—as well as by what is explicitly communicated or left unsaid. In this manner, beliefs and attitudes can spread and take root within organizations. The effectiveness of nuclear security relies on how widely NSC beliefs and attitudes are embraced and reflected in appropriate behaviors and practices.

2.3.4. NSC Resources

Organizations should ensure that employees have time and a method to report concerns. Employees should also be allotted time to complete NSC surveys and participate in NSC assessments.

2.4. PREVENTIVE MEASURES/PERSONNEL SECURITY

Personnel security is a critical component of preventive measures; it ensures the integrity and reliability of the individuals responsible for operating and protecting nuclear facilities. The term *preventive measures* refers to strategies implemented to screen employees for potential insider behaviors and to decrease the number of insiders granted access, thereby minimizing the chances of an insider committing a malicious act and preventing potential insider adversaries from executing harmful actions. Personnel security is essential for the safety and security of RRs, particularly when personnel have unescorted access to risk-significant materials, systems, or sensitive information. Therefore, establishing a well-structured and effective personnel security program is crucial for mitigating insider threats and reinforcing the overall security framework of a facility. Individuals who have access to, authority over, or knowledge of high-consequence systems and information must undergo thorough vetting and meet the highest standards of reliability, trustworthiness, and physical and mental suitability. Personnel security programs should span the entire employment life cycle. A facility's NSC helps ensure that individuals and organizations remain vigilant and maintain ITM measures.

The INS's *ITMP Handbook* offers a graded approach to personnel security measures that adapts to varying risk levels. The handbook details best practices for screening, continuous monitoring, trustworthiness assessments, behavioral observation, and incident management. It provides strategies for the vetting, monitoring, and ongoing evaluation of personnel to guarantee that those with access to sensitive areas are trustworthy and reliable.

Furthermore, a strong ITMP must be well coordinated across the organization. Organizations are encouraged to review the personnel security capabilities recommended in **Appendix D.**

2.4.1. Personnel Security Processes/Tools

Preventive measures are essential for maintaining security. The first step is to identify essential positions that require an assessment of staff trustworthiness because any security barrier can be compromised through insider cooperation. Thus, organizations must implement effective processes for determining trustworthiness and mitigating insider threats. Organizations should establish documented staff screening processes tailored to the specific risks associated with employee roles and responsibilities and conduct screenings regularly. Critical groups should be established based on the roles and responsibilities. A robust trustworthiness assessment process must be put in place to identify specific security risk factors, such as mental health issues and substance abuse. Furthermore, organizations must enforce rigorous adherence to screening procedures and apply appropriate oversight and auditing at all organizational levels; these policies should also apply to temporary staff, contractors, and visitors. Last, thorough investigations and adjudications of any significant or apparent failures of the screening process must be conducted to ensure ongoing reliability and security.

2.4.2. Personnel Security Knowledge/Skills

Security organizations should employ knowledgeable and competent individuals who are adept at aligning personnel security programs with the state's national legal requirements. Training should be provided for management and relevant staff to help them recognize high-risk behavioral indicators and develop effective observational and analytical skills. As part of this effort, management should be trained to identify signs of fatigue, stress, and other factors that may impair judgment or performance in safety-sensitive roles. Additionally, personnel should be educated to recognize and report aberrant behavior that may be indicative of security concerns; security organizations should ensure that personnel understand their responsibilities regarding adherence to fitness-for-duty requirements. Training should also help employees recognize coercion and should foster a culture of safety in which individuals feel empowered to report threats without fear of reprisal.

2.4.3. Personnel Security Behaviors

Employees should be aware and understand the vital importance of trustworthiness assessments in maintaining security within the organization. They should be trained to recognize factors that may compromise trustworthiness, such as substance abuse, workplace violence, or criminal behavior. Personnel should be educated about their role in preventing insider threats and encouraged to self-report incidents and anomalies that may affect their trustworthiness, including financial difficulties and foreign contacts. Self-reporting applies to legal medication usage, which may indicate physical or mental impairment, the use of illegal substances, arrests, business and personal travel outside the country, and changes in marital status. By recognizing the potential for unintentional and malicious

insider threats and understanding their possible consequences, employees contribute to a more secure and vigilant workplace.

2.4.4. Personnel Security Resources

Organizations must allocate ample financial, technical, and human resources to effectively fulfill their security responsibilities. They must ensure that all security personnel possess the necessary qualifications and uphold those qualifications through suitable training and development programs. Additionally, personnel must be provided with appropriate equipment, adequate workspace, current information, and other support needed to effectively carry out their security duties [7].

2.5. PROTECTIVE MEASURES

The term *protective measures* refers to strategies implemented to detect or delay malicious acts, respond to such acts, or mitigate their consequences. A facility's protective measures are not limited to guns, gates, and guards but also incorporate a combination of technical, administrative, and operational measures intended to establish a comprehensive defense-in-depth nuclear security strategy. Protective measures are composed of the PPS, NMAC, cybersecurity, and response forces.

Management must understand the details of the facility and the ITMP measures.

2.5.1. Physical Security

Establishing a PPS entails conducting a comprehensive analysis of the facility, examining factors such as physical structures, material flow, activities involving materials, and operational safety and security. This analysis is essential in determining any additional measures needed to prevent, detect, delay, and respond to malicious insider actions based on the state DBT or RTS. Detecting malicious acts initiated by external adversaries primarily depends on identifying breaches of a facility's protective measures. In contrast, insiders may be able to bypass or compromise some physical protection and NMAC measures because of their authorized access, authority, and knowledge of a facility's systems. To effectively address this vulnerability, security organizations should implement multiple and varied protective measures designed to detect potential malicious acts by insiders and provide information for subsequent investigation and analysis. Security organizations must comprehensively investigate all data generated by these detection measures because signals that appear insignificant individually may collectively indicate a malicious act [8].

Selecting appropriate protective measures and their respective levels should involve all facility organizations responsible for a facility's materials, operations, safety, and security. This collaboration is particularly important for organizations that directly operate facility systems or engage in activities related to a facility's materials.

Security organizations should use a graded approach with identified targets. Measures should protect against unauthorized removal and sabotage.

A facility's PPS incorporates technical, administrative, and operational measures intended to establish a comprehensive defense-in-depth nuclear security strategy for mitigating insider threats, including the following. Such measures include the following:

- Limiting access: Access should be limited to personnel with a need to work in a given area. Enforce escorting policies for individuals who do not have unescorted access authorization, such as maintenance staff, janitorial personnel, and visiting researchers, to reduce risks.
- Biometric access systems: Enhance security by adding a layer of verification beyond traditional access methods such as key cards or personal identification numbers.
- Surveillance systems: Monitor access points to deter unauthorized entry and facilitate rapid responses to unusual activities.
- Audit trails and access logs: Support accountability and investigative efforts by using electronic records that track entry to and exit from sensitive areas.

To ensure that insider adversaries cannot introduce or acquire prohibited items that could facilitate malicious acts, entry and egress searches must be conducted. These searches should include the following measures:

- At access control points, use metal detectors, radioisotope emission detectors, or x-ray systems for hand-carried items to identify prohibited items. Conduct random searches to deter malicious insiders.
- Monitor pedestrian and vehicle traffic for concealed nuclear material on individuals or vehicles by means of radiation control technicians using handheld radiation detectors.
- Monitor radiation in waste streams to identify attempts to remove nuclear material because waste streams are one way that items may exit the facility.

Security organizations are encouraged to review and consider the recommended physical security capabilities outlined in **Appendix E**.

2.5.1.1. Physical Security Processes/Tools

Security organizations should consider a comprehensive approach to security that uses multiple layers of physical protection and procedural measures that complicate the efforts of insider adversaries, such as compartmentalization and the separation of duties. These strategies aim to delay malicious acts, providing additional time for detection and potentially deterring insiders from attempting such actions. To further enhance security, security organizations should restrict access to critical equipment, including badge generation systems, security-related equipment, and access control systems. In addition, they should implement strict control and maintenance procedures to ensure the integrity of this equipment. Measures to protect against theft and sabotage include controlling access to nuclear material and associated operations, conducting vehicle and personnel searches, and implementing search and seizure procedures. Additionally, security organizations should use physical barriers such as tie-downs, restraints, and high-security locks to prevent unauthorized removal of sensitive items. Measures should be put in place to investigate any unauthorized activities.

2.5.1.2. Physical Security Knowledge/Skills

Security organizations should form a cohort of knowledgeable and competent individuals who understand measures to protect against insider threats and can identify equipment and areas that require protection. These individuals should be skilled in designing and implementing integrated security and safety measures that ensure effective operations yet do not compromise overall safety. Those responsible for the implementation of a PPS should be adequately trained to perform searches

for prohibited items using detection equipment and respond appropriately when such items are identified. Additionally, they should be proficient in operating and maintaining essential nuclear security equipment and capable of inspecting and evaluating protective gear to ensure adequate protection and regulatory compliance. These individuals should understand their role in maintaining the integrity of access control, the significance of preventing unauthorized badge usage, and the implications of violating prohibited item policies. Furthermore, they must know the two-person rule and their associated responsibilities.

2.5.1.3. Physical Security Behaviors

Management personnel must recognize the critical importance of protection against theft and sabotage and demonstrate their commitment to this protection in words and actions. They should view physical security equipment as essential and ensure that repairs are carried out promptly to maintain operational integrity. This commitment should be echoed throughout the organization; employees at all levels should recognize the credibility of threats posed by insiders and outsiders. They must prioritize nuclear security and take proactive responsibility for enhancing it through their actions, fostering a culture of vigilance and accountability.

2.5.1.4. Physical Security Resources

Management should view physical security equipment as important. Management's commitment to physical security should be demonstrated through the timely repair of equipment.

2.5.2. NMAC

States with an INFCIRC/153 comprehensive safeguards agreement with the IAEA are required to establish a system for NMAC as mandated by this agreement. Section 5 of IAEA Services Series No. 15, *Nuclear Material Accounting Handbook*, outlines the necessary accounting and reporting elements for nuclear material management at the facility level. Existing accounting and control systems can serve as a foundation for developing enhanced NMAC measures to support nuclear security. At an RR, a graded approach should be employed in developing the NMAC system, taking into account the quantity and attractiveness of the materials present. Additional considerations should include design-related security vulnerabilities, access to tools and equipment, the openness of the facility, the presence of co-located facilities, and the specific uses of the facility. IAEA NSS No. 25-G, *Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities*, provides further guidance on using NMAC to bolster nuclear security [2].

The effectiveness of NMAC systems in enhancing nuclear security stems primarily from maintaining accurate knowledge of the types, quantities, and locations of nuclear material within a facility; conducting efficient physical inventories; and, when applicable, verifying that activities involving nuclear material have been properly authorized. An NMAC system can aid in detecting insider threats in numerous ways. NMAC personnel must recognize that a staff member responsible for NMAC or physical protection may be a malicious insider. A program can be implemented at a nuclear facility in coordination with existing systems (e.g., physical protection, radiation and radioactive contamination monitoring, operational systems) to deter and detect unauthorized removal of nuclear material. Additionally, the program should be able to trigger alarms and initiate responses if unauthorized removal or improper use of nuclear material is detected.

To ensure nuclear security, PPS and NMAC systems must operate in a coordinated and complementary manner. Access to sensitive information regarding nuclear material quantities and locations and vulnerabilities in NMAC and the PPS should be restricted to authorized personnel with a legitimate need to know [12]. Furthermore, detection measures should be rigorously implemented to prevent unauthorized removal of nuclear material from a facility, especially during authorized shipments. These measures may include applying the two-person rule during movement preparations, conducting material measurements, using tamper-indicating devices (TIDs), performing document checks, employing radiation monitors, and adhering to standard operating procedures (SOPs) [8].

NMAC personnel are encouraged to review the NMAC capabilities recommended in **Appendix F.**

2.5.2.1. NMAC Processes/Tools

NMAC processes and tools can substantially decrease the likelihood of successful malicious insider incidents and aid in detecting unauthorized removal of nuclear material. They can help mitigate abrupt theft scenarios and reduce the quantity of nuclear material at risk in cases of protracted theft, thereby extending the time available to respond effectively to such events. The primary aim of access control in a nuclear security system is to prevent unauthorized individuals from gaining access to nuclear material or the equipment used to monitor or process materials; this aim is chiefly the responsibility of the physical protection department. Access control should also prevent unauthorized activities related to NMAC and operations. NMAC personnel should develop and maintain comprehensive plans to control personnel access to nuclear material and associated equipment, addressing routine operations, planned evacuations, and emergency situations that may necessitate unplanned evacuations.

In locations where nuclear material is particularly susceptible to insider threats, additional material control measures should be considered, especially in areas where nuclear material is handled. All exits from these areas—emergency exits, ventilation ducts, windows, and drains—should be treated as potential pathways for the unauthorized removal of nuclear material by malicious insiders.

NMAC personnel should also implement robust TID programs that include strict controls for the acquisition, procurement, storage, issuance, removal, and destruction of these devices. These programs should keep track of the various types of devices used and the unique identification for each unit; they should also include comprehensive training procedures for the proper use, application, storage, issuance, and verification of TIDs.

2.5.2.2. NMAC Knowledge/Skills

NMAC managers should be trained to recognize insider threats and understand the significance of NMAC contributions to nuclear security. Additionally, NMAC personnel must provide appropriate NMAC training to all facility personnel to ensure the effective implementation of NMAC requirements. This training should empower designated individuals to recognize unusual occurrences that may indicate the unauthorized removal of nuclear material. Furthermore, all facility personnel must be trained to understand the importance of NMAC in maintaining nuclear security and fostering a culture of vigilance and accountability throughout the organization.

2.5.2.3. NMAC Behaviors

NMAC personnel should foster strong collaborative relationships between NMAC and other essential departments, including physical protection, operations, radiation safety, and analytical laboratory or measurement groups. All facility personnel must be aware of the potential consequences of losing control over nuclear material and understand the sensitivity of NMAC information. They should actively engage with the rules governing the protection of such information, recognize the serious implications of failures in nuclear security, and be prepared to respond appropriately to any irregularities that arise. By cultivating this mindset, NMAC personnel promote a culture of accountability and vigilance and ensure that all personnel prioritize the security of nuclear material and information.

2.5.2.4. NMAC Resources

Sufficient resources should be provided to ensure an effective NMAC system.

2.5.3. Cybersecurity

Computer-based systems are crucial in ensuring the safety and security of facilities and activities involving the use, storage, and transportation of nuclear and other radioactive material. These systems are integral to maintaining physical protection and implementing measures for detecting and responding to cases in which materials are out of regulatory control. Consequently, all computer-based systems must be secured against malicious and unwitting insider acts [13].

Cybersecurity personnel are encouraged to review the cybersecurity capabilities recommended in **Appendix G.**

2.5.3.1. Cybersecurity Processes/Tools

Cybersecurity personnel should implement a graded approach to cybersecurity programs, systematically identifying and safeguarding critical digital assets. This strategy should be bolstered by defense-in-depth techniques that provide multiple layers of security to enhance a facility's overall resilience to insider threats and cyber incidents. Additionally, cybersecurity plans must include the ability to coordinate with physical security teams to ensure that physical and cybersecurity measures are aligned for effective protection against insider threats. To reduce the risks associated with cyber insider threats, cybersecurity personnel must establish robust security protocols for computer-based systems. Consequently, a well-defined cybersecurity plan should include specific measures for combating insider threats. Furthermore, cybersecurity personnel must establish a comprehensive process for responding to cyber incidents to ensure that ITM strategies are explicitly incorporated within the cybersecurity framework.

2.5.3.2. Cybersecurity Knowledge/Skills

Cybersecurity specialists working at an RR must have specific vital skills for managing and mitigating insider threats. Among these skills is the ability to recognize behavioral indicators that suggest potential insider risks, such as unusual access patterns or notable changes in staff behavior. Additionally, they should be adept at conducting assessments that identify vulnerabilities susceptible to exploitation by insiders—especially vulnerabilities related to access to sensitive systems and information. Furthermore, expertise in designing and implementing robust access control measures is essential for monitoring and restricting personnel access to critical systems and sensitive data.

These measures involve applying the principle of least privilege to ensure that employees have only the access necessary to perform their jobs.

By cultivating these capabilities, cybersecurity specialists can enhance their effectiveness in identifying, mitigating, and responding to insider threats and bolster the overall security posture of a facility. By taking a systematic approach to developing and refining these skills, specialists can significantly reduce the risk of insider threats within a nuclear facility. Their proactive strategies for monitoring and addressing vulnerabilities are vital for maintaining a secure environment and protecting critical infrastructure from deliberate and accidental insider incidents. As cyber threats continue to evolve in complexity, strengthening a facility's security posture not only safeguards physical assets but also ensures the safety and security of the broader community.

Individuals should be made aware of their potential to become unwitting insiders. Tailored education and training programs should equip them with the knowledge necessary to adhere to security protocols. This training should emphasize the importance of protecting sensitive information and systems and help cultivate a culture of vigilance and accountability. Training should also highlight the critical role each individual plays in strengthening the overall security posture of a facility.

2.5.3.3. Cybersecurity Behaviors

Management should prioritize the development, promotion, and upkeep of a robust nuclear cybersecurity culture. Computer security is a vital aspect of this culture, and it requires explicit support and commitment from senior management as well as ongoing awareness initiatives and training programs. Cybersecurity personnel must foster strong collaborative relationships between the cybersecurity department and other key areas, including physical protection, operations, radiation safety, and engineering. All individuals within an RR must fully understand their computer security responsibilities and recognize the importance of these obligations in the context of nuclear security and safety. Furthermore, individuals should be made aware of their potential to inadvertently engage in behaviors that make them unwitting insiders and adjust their conduct to mitigate this risk.

2.5.3.4. Cybersecurity Resources

Cybersecurity personnel should allocate financial resources for the acquisition of cybersecurity defense equipment and software and sufficient personnel to carry out cybersecurity activities.

2.5.4. Protective Forces

Protective forces are vital components of an ITMP, serving as the first line of defense against potential insider threats. Because of their unique role, which often involves access to weapons, sensitive areas, and critical security protocols, security personnel must implement targeted measures to guarantee protective forces' reliability, trustworthiness, and readiness to respond effectively to insider threats. Protective forces fulfill several key functions that extend beyond traditional security duties and integrate smoothly with other ITMP components. Their primary responsibilities include access control, which entails verifying credentials, managing entry and exit points, and detecting prohibited items; incident response, which entails taking action to neutralize insider threats such as theft, sabotage, and other malicious activities; and surveillance and deterrence, which entail conducting patrols, monitoring security systems, responding to alarms, and maintaining a visible presence to deter insider actions. Protective forces also engage in behavioral observation to identify

and report signs of stress or abnormal behavior that may signal insider activities. They provide investigative support in collaboration with other ITMP teams to detect, document, and investigate insider incidents. Their collaborative role also extends to working alongside personnel security, operations, NMAC, and cybersecurity teams to create a unified and comprehensive insider threat management strategy, thereby enhancing a facility's overall protection against potential threats [5].

Security personnel are encouraged to review the protective forces capabilities recommended in **Appendix H.**

2.5.4.1. Protective Forces Processes/Tools

Security personnel should integrate protective forces into the overall security framework and clearly define their roles and responsibilities in managing insider-related incidents. Protective forces employ various processes and tools as part of the ITMP. Moreover, security personnel should implement strengthened screening protocols for members of protective forces because their unique positions often involve access to weapons, sensitive areas, and essential security protocols.

2.5.4.2. Protective Forces Knowledge/Skills

Security personnel should have a team of knowledgeable and competent individuals capable of deterring, detecting, and responding to potential insider threats. They should conduct randomized patrols, badge verifications, and personnel searches to create an atmosphere of uncertainty that deters insider actions. They should also implement unannounced inspections of TIDs and sensitive areas. To ensure that protective forces are prepared to mitigate malicious actions by insiders, security personnel should provide regular training and exercises. Additionally, security personnel should establish scenario-based training programs that emphasize situational awareness, response tactics, and behavioral observation, equipping protective forces to effectively cope with routine and high-stress situations.

2.5.4.3. Protective Forces Behaviors

Management should foster a culture that values and respects protective forces, recognizing the critical role they play in mitigating insider threats. Members of protective forces must understand their significant responsibilities and the pressures that come with their positions. Because of the stress associated with their duties, they should be encouraged to seek help when they need it to ensure their well-being and effectiveness in maintaining security.

2.5.4.4. Protective Forces Resources

Security personnel should provide adequate personnel, training, and equipment for protective forces.

2.6. PLANT OPERATIONS ORGANIZATION

A facility's plant operations organization is accountable for the safe and reliable operation of all plant equipment and holds ultimate decision-making authority in all matters related to plant operations. At an RR, this organization may consist of two or three people. Operations personnel have the closest interaction of all facility personnel with sensitive materials, systems, areas, and critical security protocols. This workforce's management of a facility's nuclear or radioactive material presents both a significant insider threat and an opportunity for threat mitigation. Their proximity to and familiarity with operations uniquely position them to effectively detect and inform security of

potential malicious actions. They are the most highly trained and knowledgeable individuals on-site. Because of their unique positions, plant operations personnel must implement targeted measures that guarantee that operations personnel are reliable, trustworthy, and ready to respond effectively to insider threats. Operations personnel are members of the critical group and fall under the behavioral observation program (BOP) and the fitness-for-duty program. Under the BOP, the plant operations organization engages in behavioral observation to identify and report signs of stress or abnormal behavior that may signal insider activity. They also provide investigative support to the security organization by collaborating with other ITMP teams to detect, document, and investigate insider incidents. Their collaborative role also extends to working alongside the personnel security, NMAC, and cybersecurity teams to create a unified and comprehensive ITM strategy, thereby enhancing a facility's overall protection against potential threats [5].

Plant operations personnel are encouraged to review the plant operations organization capabilities recommended in **Appendix I.**

2.6.1. Plant Operations Organization Processes/Tools

The plant operations organization should be integrated into the overall security framework, with clearly defined roles and responsibilities in managing insider-related incidents. The plant operations organization should use established processes and tools as part of the ITMP, including SOPs, the two-person rule, plan of the day, critical position identification, and the TID program.

- SOPs should provide step-by-step instructions for completing tasks or activities and should list all required equipment, compensatory measures, training requirements, and personnel qualifications. Deviations from the written steps within an SOP may indicate a malicious insider act. Care should be taken to investigate such deviations because they may result from nonmalicious human performance errors and may not represent malicious insider acts.
- The two-person rule, which requires two people to perform tasks or activities that could lead to loss of control of nuclear material or sabotage, provides opportunities for detecting errors or malicious actions through peer checking and validations.
- The plan of the day requires prior authorization of all activities and should include a check to ensure that one person cannot request and approve authorization of a task or activity.
- Critical position identification is a measure that identifies individuals who perform job functions critical to the safe and secure operation of a facility and can contribute to efforts to protect against insider threats.
- A TID program is an effective surveillance measure for material containment or area tamper monitoring. Plant operation personnel should implement robust TID programs that include strict controls over the acquisition, procurement, storage, issuance, removal, and destruction of TIDs.

Moreover, the plant operations organization should be included in the critical group, given that operations positions often involve access to material, sensitive areas, and essential security protocols.

2.6.2. Plant Operations Organization Knowledge/Skills

Plant operations organization personnel should be trained in ITM techniques to deter, detect, and respond to potential insider threats.

2.6.3. Plant Operations Organization Behaviors

Plant operations organization personnel are leaders within an organization and are ultimately responsible for all operational decisions. Plant operations organization personnel should understand the role they play in mitigating insider threats. Plant operations organization employees should also understand that their roles may be stressful and have high-stakes consequences and that they should seek help when they need it.

2.6.4. Plant Operations Organization Resources

Plant operations organization personnel should have all the insider threat resources needed to identify, report, investigate, and mitigate potential insider threat activities. The resources available should include but are not limited to the BOP, a "safe to say" program, an employee concerns program, security department resources, and the EAP.

2.7. SYSTEM EVALUATION AND PERFORMANCE ASSURANCE

Although regulatory requirements and oversight are essential for establishing and maintaining security standards, security personnel must conduct nuclear security assessments to ensure that security systems and measures effectively counter insider and outsider threats as outlined in the state DBT/RTS. These assessments help identify vulnerabilities that necessitate corrective actions and offer insights into the residual risks that facility security personnel and competent authorities face. Furthermore, they provide valuable feedback regarding the adequacy of regulatory requirements. Assessments can be applied throughout all phases of the facility life cycle, optimizing physical protection during the design phase and ensuring the effectiveness of the PPS during operations and decommissioning [5].

System evaluation and performance assurance involve establishing performance monitoring criteria to measure the effectiveness of security measures, elements of the physical security system, and personnel (e.g., assessments of incident response times and adherence to protocols). Various evaluation methods, such as self-assessments, audits, and inspections, should be used to systematically assess security systems. Furthermore, a continuous improvement approach should be implemented so that organizations can use lessons learned from evaluations to enhance security measures in response to emerging threats and vulnerabilities. Regular training and exercises should be conducted to test the readiness and responsiveness of protective forces, ensuring that they are adequately prepared for potential threats. Comprehensive documentation and reporting should be maintained to provide transparency and facilitate oversight of security performance. Finally, management should routinely review evaluation reports and performance metrics to support strategic decision-making regarding security enhancements and resource allocation. Through these efforts, security personnel can ensure that nuclear facilities maintain robust security postures that effectively address insider and external threats.

Security personnel are encouraged to review the system evaluation and performance assurance capabilities recommended in **Appendix J.**

2.7.1. System Evaluation and Performance Assurance Processes/Tools

Security personnel should implement processes for conducting routine assessments, a crucial part of ensuring the ongoing effectiveness of ITMP measures. Security personnel should use internal and

external assessments to evaluate vulnerabilities and address identified deficiencies. Assessment findings should guide continuous improvement initiatives aimed at ensuring that ITMPs remain dynamic and responsive to emerging threats. Assessments and inspections should be conducted during various operational phases to provide assurance of an ITMP's effectiveness during operations. All assessments and inspections should be documented to verify that systems are functioning as intended. Additionally, security personnel should establish processes for carrying out internal investigations of incidents and developing corrective actions.

2.7.2. System Evaluation and Performance Assurance Knowledge/Skills

Security personnel should be knowledgeable and competent individuals who are trained in ITM evaluation techniques.

2.7.3. System Evaluation and Performance Assurance Behaviors

Management should acknowledge the significance of system evaluation, performance assurance, and continuous improvement of the ITMP. This commitment should be reflected in words and actions. Management must foster an environment in which individuals feel comfortable sharing information with assessors and evaluators without fear of reprisal. In such environments, individuals recognize the value of system evaluation and performance assurance and demonstrate their commitment by openly providing information to support the assessment process.

2.7.4. System Evaluation and Performance Assurance Resources

Security personnel should allocate resources to perform ITMP evaluations and implement recommendations.

2.8. CONTINUOUS IMPROVEMENT

Continuous improvement leverages findings from system evaluation and performance assurance to foster an ongoing cycle of enhancement, thereby reinforcing sustainability and optimizing overall ITMP performance. Together, these elements of continuous improvement create a cohesive framework that supports an organization's ITMP and effectively addresses risks, challenges, and changing threats.

Findings from evaluations and assessments should directly inform continuous improvement efforts to ensure that mitigation programs remain dynamic and responsive to emerging threats. To support continuous improvement efforts, continuous improvement personnel should continually update ITMP plans in accordance with regulatory guidance or as a result of updates to the DBT/RTS, train staff on insider threat response, and consistently monitor and evaluate program effectiveness.

Continuous improvement personnel are encouraged to review the continuous improvement capabilities recommended in **Appendix K**.

2.8.1. Continuous Improvement Processes/Tools

Continuous improvement personnel should adopt tools and methodologies widely used in the nuclear industry to promote continuous improvement. Root cause analysis, failure mode and effects analysis, performance metrics, key performance indicators, and benchmarking can help continuous

improvement personnel systematically enhance operations, ensure regulatory compliance, and cultivate a culture of security, safety, and excellence.

Additionally, continuous improvement personnel must establish postincident procedures for reviewing incidents, identifying gaps, and implementing lessons learned. Continuous improvement personnel should use corrective action programs to identify, evaluate, and address adverse conditions and stipulate procedures that set timely requirements for taking corrective actions.

2.8.2. Continuous Improvement Knowledge/Skills

Continuous improvement personnel should be knowledgeable, competent, and trained in continuous improvement methods and tools.

2.8.3. Continuous Improvement Behaviors

Management must recognize the significance of continuous ITMP improvement. Management's commitment to continuous improvement should be reflected in both words and actions. Management should foster an environment in which individuals feel comfortable reporting concerns and recommending improvements without fear of reprisal. In such an environment, individuals recognize the value of continuous improvement and demonstrate their commitment to it through consistent actions, behaviors, and practices that indicate dedication to enhancing processes, knowledge, and resources over time.

2.8.4. Continuous Improvement Resources

Continuous improvement personnel should allocate resources for implementing continuous improvement recommendations.

2.9. ITMP SUSTAINABILITY

ITMP sustainability involves a comprehensive approach to managing processes, tools, knowledge, skills, behaviors, and resources to preserve an ITMP's functionality and integrity over time. ITMP sustainability also involves adapting to changes in management, operational conditions, and potential threats. To enhance ITMP sustainability, a defense-in-depth strategy should be implemented. Organizations should ensure that all ITMP components are robust and that the failure of any single element does not expose the organization to insider threats. Sustainability measures for each element are discussed in the following sections.

2.9.1. System Sustainability: National Legal and Regulatory Framework

Recognizing and using up-to-date threat information is essential for sustaining an ITMP because up-to-date threat information allows operating organizations to uphold the effectiveness of their preventive and protective measures. Security personnel should implement systematic processes to ensure that threat information from competent authorities and local threat insights are promptly and effectively incorporated into preventive and protective measures.

2.9.2. System Sustainability: ITMP Plan

The ITMP plan provides a foundational framework for ITMP sustainability by establishing procedures and defining roles and responsibilities. Although an ITMP plan maintains a consistent commitment to an ITMP despite changes in management at a facility, reaffirming this commitment when

management changes occur is a top priority for any site. Leadership plays a crucial role in providing vision and fostering the culture within an organization. Effective management systems are vital leadership tools that enable leaders to articulate their vision and shape organizational culture by establishing and maintaining effective management practices, including quality management, operational procedures, human resource management, and training.

Managing and planning for sustainable operations at the operational level supports ITMPs by continuously allocating resources for the effective design, operation, and maintenance of ITMP measures. Senior managers are responsible for setting priorities and ensuring that long-term financial resources are available for operational expenses such as staffing, training, exercises, performance testing, procurement, and equipment maintenance.

Building and maintaining commitment to an ITMP is essential for sustaining the nuclear security regime because doing so empowers and motivates organizations and individuals to meet their nuclear security responsibilities. A strong commitment ensures that the necessary resources and capacities for fulfilling ITMP roles and responsibilities are consistently available. This kind of organizational and individual commitment relies on continuous recognition of insider threats as credible risks. Developing and maintaining nuclear security competencies at the operational level is vital for sustaining an ITMP because it ensures that a motivated, skilled, and experienced nuclear security workforce is available. Sustainability hinges on an operating organization employing staff with the competencies needed for the effective operation and maintenance of the organization's nuclear security systems and measures as defined by the competent authority.

Organizations should establish systems and processes for recruiting qualified personnel and providing training that enables personnel to gain these competencies. Furthermore, the development of human resources contributes to ITMP sustainability by ensuring that an adequate number of employees have the required expertise and fostering a nuclear security workforce with core competencies.

2.9.3. System Sustainability: NSC

A strong NSC is essential for sustaining an ITMP because it ensures that all individuals understand and promote the attitudes and behaviors necessary for enhancing nuclear security. The effectiveness of an ITMP relies on the commitment and actions of personnel, especially those in leadership roles.

NSC is inherently dynamic and requires ongoing attention to prevent its deterioration over time. Leadership plays a vital role in nurturing and maintaining this culture by visibly supporting security initiatives, setting a positive example, and fostering open lines of communication. Unless an organization engages in continuous monitoring and improvement efforts, NSC may weaken, creating vulnerabilities within the organization. Beliefs and attitudes formed over time influence individual behaviors and shape responses to security issues. A robust NSC program identifies and addresses employees who may be disengaged from a security-focused mindset and reinforces positive behaviors to sustain an effective ITMP and nuclear security system.

To maintain a strong NSC, managers must demonstrate commitment to it, encourage open dialogue, and foster a collective sense of responsibility for security. Organizations should establish systems for positively reinforcing behaviors and performance that contribute to nuclear security, such as reporting concerns or suggesting improvements.

2.9.4. System Sustainability: Preventive Measures/Personnel Security

The sustainability of preventive measures relies on regular reviews and adjustments of procedures and methods to incorporate the latest information regarding current threats. Additionally, sustainability is achieved through ongoing monitoring that ensures the trustworthiness and reliability of personnel throughout their employment. This monitoring may include periodic reassessments of criminal history, financial stability, medical status, psychological well-being, and self-reported changes.

2.9.5. System Sustainability: Protective Measures—Physical Security

The sustainability of physical security measures depends on continuous reviews and adjustments of procedures, methods, and equipment to reflect the most current threat information. Management should establish priorities, identify long-term financial resources, and clearly define roles, responsibilities, and accountabilities related to physical security to ensure the effectiveness of an organization's ITMP.

Implementing a robust maintenance program at the operational level is crucial for sustaining an ITMP because it ensures that associated systems and equipment operate reliably and effectively over time. Security personnel should be equipped to conduct timely maintenance using their own personnel, contractors, or a combination of the two.

2.9.6. System Sustainability: Protective Measures—NMAC

Ensuring the ongoing effectiveness of NMAC measures requires periodic reviews and adjustments to incorporate updated information regarding current threats. To support these efforts, a sustainability program should be established to maintain key elements of the NMAC program, including NMAC documentation and procedures, configuration management, staffing, training, quality control, and performance testing. Additionally, to enhance an organization's ability to detect unauthorized removal of nuclear material, the sustainability program must ensure that the facility's NMAC systems remain robust and effective over the long-term because their sustainability is crucial for maintaining overall nuclear security.

2.9.7. System Sustainability: Protective Measures—Cybersecurity

The sustainability of cybersecurity refers to the ongoing capacity to safeguard information systems and data from intentional and unintentional cyber insider threats and adapt to the constantly changing technological environment and threat landscape. Cybersecurity sustainability relies on continuous reviews and adjustments of procedures, methods, and equipment to align with the latest threat information.

To ensure the effectiveness of nuclear security systems and measures, organizations must periodically review and adjust these systems in response to updated information on current threats. Regular updates and audits maintain necessary delay mechanisms that must remain effective against evolving insider tactics.

2.9.8. System Sustainability: Protective Measures—Protective Forces

The sustainability of protective forces capabilities relies on ongoing reviews and adjustments of procedures, methods, training, and equipment to incorporate the latest threat information. Effective nuclear security necessitates the development and maintenance of capabilities that align with the

national threat landscape. A clearly defined threat, established through a national threat assessment, specifies what the nuclear security regime must protect against.

2.9.9. System Sustainability: Plant Operations Organization

To have sustainable processes that ensure integration between security and safety, all departments under the oversight and command of operations must focus on sustainability. This focus is ensured through security's active participation in all aspects of plant operations and interfacing with departments to meet all safety and security requirements. Operations has an overview of plant activities, including security; therefore, operations should have an active role in communication between all departments. The management system structure should include guidance, through protocols and procedures, that provides an effective road map for sustainability and continuous improvement.

Advisory Group on Nuclear Security/International Nuclear Safety Advisory Group (AdSec/INSAG) Report No. 1, *A Systems View of Nuclear Security and Nuclear Safety: Identifying Interfaces and Building Synergies*, highlights the importance of maintaining integration within operating organizations by means of sustainable mechanisms for success. Senior leadership has an overview of the implementation process for all activities and is therefore in a position to provide guidance to ensure sustainable ITM/NSC regimes.

CHAPTER 3

3. CONCLUSION

In conclusion, ITM requires a multifaceted approach that integrates technical and human-centric strategies. This paper has explored the key pillars involved in creating, implementing, and maintaining a successful ITMP. An effective ITMP must include technical controls and continuous behavioral observation and foster a well-balanced security culture. Creating a culture in which plant personnel feel empowered to identify and report suspicious activities without fear of retaliation is a key component of any ITMP. Through technical training, clear communication of site policies and procedures, and clear standards of ethical behavior, facilities can reduce the chances of adverse events stemming from ignorance or lack of awareness.

Continuous improvement plays a critical role within an ITMP, ensuring that as the threat landscape evolves, a facility's ITMP adapts to the changes and remains effective and efficient. Proper oversight from facility's leadership and stakeholder buy-in will drive a culture of shared responsibility for the successful implementation and long-term sustainability of an ITMP.

CHAPTER 4

4. REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, "Building Capacity for Nuclear Security", IAEA Nuclear Security Series No. 31-G, IAEA, Vienna, 2018.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, "Convention on the Physical Protection of Nuclear Material", INFCIRC/274/Rev. 1, IAEA, Vienaa, 1979.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, "Amendment to the Convention on the Physical Protection of Nuclear Material", INFCIRC/274/Rev. 1/Mod. 1, IAEA, Vienna, 2005.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, "Communication Dated 22 December 2016 Received From the Permanent Mission of the United States of America Concerning a Joint Statement on Mitigating Insider Threats", INFCIRC/908, IAEA, Vienna, 2017.

[5] International Nuclear Security, "Insider Threat Mitigation Program: Facility Implementation Handbook," 2020.

[6] C. F. Noonan, J. A. Baweja, M. P. Dunning and H. L. Day, "Security Self-Assessment Toolkit for Nuclear Materials Facilities," 2021.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, "Nuclear Security Culture", IAEA Nuclear Security Series No. 7, IAEA, Vienna, 2008.

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, "Preventive and Protective Measures against Insider Threats" No. 8-G, IAEA, Vienna, 2020.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, "Objective and Essential Elements of a State's Nuclear Security Regime, Nuclear Security Fundamentals", IAEA Nuclear Security Series No. 20, IAEA,, Vienna, 2013.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, "Physical Protection of Nuclear Material and Nuclear Facilities" NSS No. 27-G, IAEA, Vienna, 2016.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, "A Systems View of Nuclear Security and Nuclear Safety: Identifying Interfaces and Building Synergies," IAEA AdSec/INSAG, Vienna, 2023.

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, "Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities" NSS No. 25-G, IAEA, Vienna, 2015.

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, "Computer Security for Nuclear Security" No. 42-G, IAEA, Vienna, 2021.

[14] "Skill vs Capability vs Competency: How to Differentiate the Three," [Online]. Available: https://acorn.works/enterprise-learning-management/skill-vs-capability-vs-competency#:~:text=A%20capability%20is%20a%20combination,development%2C%20capabilities%20drive%20business%20outcomes..

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, "Sustaining a Nuclear Security Regime", IAEA Nuclear Security Series No. 30-G, IAEA, Vienna, 2018.

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities" (INFCIRC/225/Revision 5), IAEA NSS 13, IAEA, Vienna, 2011.

APPENDIX A

Table A.1 and **Table A.2** present suggested organizational and individual national legal and regulatory framework capabilities.

Table A.1. Organizational national legal and regulatory framework capabilities

Organizational national legal and regulatory framework capabilities	Capability area
The organization develops meaningful and useful policies and procedures based on the national legal and regulatory framework.	Processes/tools
The organization has knowledgeable and competent individuals that - understand roles and responsibilities delineated in the law, - understand compliance with the law, and - understand the boundaries within which facilities must operate (e.g., personal privacy laws).	Knowledge/skills
The organization has knowledgeable and competent individuals who can develop provisions for inspections, audits, and performance evaluations to ensure that compliance with established measures is continuously monitored and enforced [1].	Knowledge/skills
Collaborating organizations (operators, regulators, and law enforcement) have knowledgeable and competent individuals to oversee information sharing protocols for sensitive information.	Knowledge/skills
The organization participates in regulator peer groups such as International Atomic Energy Agency peer groups, the European Nuclear Safety Regulators Group, or the Forum of Nuclear Regulatory Bodies in Africa.	Knowledge/skills
The organization allocates resources for inspection preparation and performance.	Resources
The organization prioritizes resource allocation to provide sufficient human, financial, and technical resources for compliance with the national legal and regulatory framework.	Resources

Table A.1. Individual national legal and regulatory framework capabilities

Individual national legal and regulatory framework capabilities	Capability area
Individuals acknowledge that laws and regulations form the foundation of policies and procedures.	Behavior
Individuals involved in activities related to nuclear safety or security are responsible for supporting the organization's success. Supportive actions include ensuring compliance with regulations, fostering a questioning attitude, actively reporting, and addressing deficiencies.	Behavior

APPENDIX B

Table B.1 and **Table B.2** present suggested organizational and individual insider threat mitigation program (ITMP) plan capabilities.

Table B.1. Organizational ITMP capabilities

Organizational ITMP capabilities	Capability area
Management understands the importance of an ITMP and supports ITMP implementation. Management demonstrates commitment through words and actions.	Behavior
The organization establishes the ITMP as a core organizational value.	Behavior
The organization establishes that security and insider threat mitigation (ITM) are joint responsibilities.	Behavior
The organization employs knowledgeable and competent individuals who understand - threat assessment and the design basis threat/representative threat statement; - insider threat, target identification, vulnerability, and consequence assessments; - preventive and protective measures (including access control and trustworthiness assessment); - administrative, operational, physical, and technical measures; - incident investigations; and data analysis; and - program effectiveness/performance assurance.	Knowledge/skills
Appropriate individuals are trained for threat assessment and on the design basis threat/representative threat statement.	Knowledge/skills
The organization employs knowledgeable and competent individuals who are capable of developing an ITMP plan. - The Office of International Nuclear Security's *ITMP Handbook*, Appendix A, provides a sample ITMP plan outline. - Appendix 1 of the International Atomic Energy Agency's Nuclear Security Series No. 27-G provides a suggested structure for incorporating an ITMP into a security plan.	Knowledge/skills
Appropriate individuals are trained to recognize insider characteristics so they can identify potential insider threats and differentiate between categories of insiders and their possible motivations.	Knowledge/skills

Table B.1. Organizational ITMP capabilities (continued)

Organizational ITMP capabilities	Capability area
Appropriate individuals are trained to identify targets within a facility (e.g., nuclear material, supporting safety and security equipment, and sabotage that could result in unacceptable radiological consequences).	Knowledge/skills
The organization employs knowledgeable and competent individuals who understand the components of an ITMP plan.	Knowledge/skills
The organization employs knowledgeable and competent individuals who understand the design, evaluation, implementation, and maintenance of a physical protection system and contingency plans.	Knowledge/skills
The organization participates in international initiatives such as Information Circular (INFCIRC)/908–related engagements.	Knowledge/skills
Organizations allocate sufficient human, financial, and technical resources to develop, implement, and maintain an ITMP.	Resources
The facility has organizations that support the implementation of the ITMP (e.g., legal, HR, security, safety, facilities/operations, technical staff, IT).	Resources
The organization establishes processes and procedures to implement the ITMP.	Processes/tools
The organization employs knowledgeable and competent individuals who understand facility-specific ITM policies and procedures based on requirements set by the state/regulatory authority within the state's legal framework. These individuals can - identify targets within the facility (e.g., nuclear material, supporting safety and security equipment, and sabotage that could result in unacceptable radiological consequences); - identify insider threats, including different categories of insiders and their possible motivations; - identify the individuals (based on job function) who need unescorted access to vital areas to ensure that access to risk-significant materials, systems, or information is limited as much as possible; - define criteria for determining trustworthiness; and - maintain a list of positions with unescorted access to vital areas and nuclear or other radioactive material.	Knowledge/skills
The organization holds the effective implementation of policies, security measures, and procedures to manage internal threats as a core organizational value.	Processes/tools

Table B.1. Organizational ITMP capabilities (continued)

Organizational ITMP capabilities	Capability area
The organization's workforce is trained in processes and procedures for implementing the ITMP.	Knowledge/skills
The organization integrates ITM into operating standards, special procedures, and directives.	Processes/tools
Management enforces ITM policies and procedures.	Behavior
The organization integrates ITM into contingency, response, and emergency plans.	Processes/tools
Personnel are trained in contingency, response, and emergency plans.	Knowledge/skills
Personnel are trained to recognize signs of insider threats and understand the layered protections in place. Training programs foster a culture of vigilance, empowering employees to identify and report potential risks before they escalate.	Knowledge/skills
Security plans and programs (including ITM) are updated regularly to reflect changes in threats, operations, legislation, and regulations.	Processes/tools
The organization creates short-, medium-, and long-term workforce plans to determine overall human resource needs and associated requirements [1].	Resources
The organization offers feedback to the government regarding specific gaps or deficiencies identified in current capability building arrangements [1].	Behavior
The organization promotes awareness of nuclear security issues and associated capacity-building initiatives throughout the organization [1].	Processes/tools
The organization creates and executes a systematic approach to capability building within the organization as an integral part of the management system [1].	Processes/tools
The organization implements mechanisms to monitor and evaluate individual and organizational performance and encourages feedback to identify necessary improvements in personnel training, organizational structure, or procedures [1].	Processes/tools
The organization creates comprehensive training programs that include regular exercises to enhance and sustain skills, evaluate plans, and foster attitudes and behaviors that support a strong nuclear security culture [1].	Processes/tools
The facility's organizational-level coordination entails the ability to plan, conduct operations, and communicate effectively across relevant organizations to thwart nuclear security threats from criminals or unintentional unauthorized actions involving nuclear material, other radioactive substances, associated facilities, or related activities. It also focuses on detecting and responding to nuclear security incidents [1].	Processes/tools

Table B.2. Individual ITMP capabilities

Individual ITMP capabilities	Capability Area
Individuals are trained and understand their roles in insider threat mitigation (ITM).	Knowledge/skills
Individuals understand and internalize the fact that security and ITM is a joint responsibility.	Behavior
As a core organizational value, individuals support effective implementation of policies, security measures, and procedures to manage internal threats.	Behavior
Individuals maintain qualifications and training.	Knowledge/skills
Individuals pass on knowledge by mentoring and training others.	Knowledge/skills

APPENDIX C

Table C.1 and **Table C.2** present suggested organizational and individual nuclear security culture (NSC) capabilities.

Table C.1. Organizational NSC capabilities

Organizational NSC capabilities	Capability area
The organization improves the facility's NSC to ensure that individuals and organizations remain vigilant and maintain effective measures to counter insider threats. The cornerstone of NSC lies in the recognition—by all stakeholders involved in the regulation, management, or operation of nuclear facilities and activities and by those who may be affected by these activities—that credible threats exist and that nuclear security is paramount.	Behavior
Managers promote NSC by demonstrating their commitment to it, facilitating open communication, and cultivating a collective sense of responsibility for security.	Behavior
The organization offers an employee assistance program that addresses personal stressors and provides resources to mitigate the risk of insider threats.	Processes/tools
Personnel are encouraged to report security concerns and suspicious behavior.	Processes/tools
The organization has an anonymous method for employees to report concerns.	Processes/tools
The organization has a formal process for handling employee grievances.	Processes/tools
Management ensures that experiences and events that affect security, including events in other locations, are thoroughly analyzed and that appropriate enhancements or corrective actions are enacted.	Processes/tools
The organization ensures that employees have time and a method to report concerns.	Resources
Employees are allotted time to complete NSC surveys and participate in NSC assessments.	Resources

Table C.2. Individual NSC capabilities

Individual NSC capabilities	Capability area
Employees at all levels possess a strong conviction of the credibility of threats posed by insiders (and outsiders), prioritize nuclear security, and take proactive responsibility for fostering nuclear security through their actions.	Behavior
Individuals recognize that nuclear security is important.	Behavior
Individuals follow security procedures.	Behavior
Individuals reinforce positive nuclear security behaviors among their colleagues.	Behavior
Individuals receive NSC training.	Knowledge/skills
All personnel are accountable for their behavior and motivated to ensure nuclear security.	Behavior
Individuals abide by a staff code of conduct that covers the needs of nuclear security.	Behavior

APPENDIX D

Table D.1 and **Table D.2** present security organization and individual personnel security capabilities.

Table D.1. Security organization personnel security capabilities

Security organization personnel security capabilities	Capability area
Management personnel typically exhibit behaviors commensurate with their job responsibilities. They are grounded, reliable, and meticulous. They follow directions and communicate well.	Behavior
The security organization employs knowledgeable and competent individuals who understand how to align personnel security programs with the state's national legal requirements.	Knowledge/skills
The security organization has processes and procedures in place to conduct preemployment screening: background checks, drug testing, identity verification, work and educational history, and criminal record checks to identify any potential risk factors.	Process/tools
The security organization has processes and procedures in place to define sensitive job functions and establish clear criteria for positions requiring unescorted access to risk-significant areas to limit exposure to sensitive materials and systems.	Process/tools
The security organization creates separation-of-duties processes and procedures to divide responsibilities among multiple personnel to prevent any individual from having unchecked control over critical tasks.	Process/tools
The security organization has a duress program for personnel to signal coercion, enabling rapid intervention.	Process/tools
The security organization has processes and procedures in place to monitor trustworthiness and reliability via a behavior observation program; this program provides for the ongoing evaluation of personnel to detect changes in behavior, physical health, or other factors that may affect security.	Process/tools
The security organization has processes and procedures in place to monitor trustworthiness and reliability via a fitness-for-duty program; this program includes physical, psychological, and substance screening to confirm that individuals are mentally and physically fit for their roles.	Process/tools
The security organization employs knowledgeable and competent individuals who understand how to implement trustworthiness and reliability programs.	Knowledge/skills

Table D.1. Security organization personnel security capabilities (continued)

Security organization personnel security capabilities	Capability area
Management personnel are trained to recognize fatigue, stress, and other factors that may impair judgment or performance in safety-sensitive roles.	Knowledge/skills
The security organization has processes and procedures in place for escorting visitors or individuals who have not undergone full trustworthiness assessments but require periodic access.	Process/tools
Access revocation policies and procedures are documented and applied to potential insider threats, individuals changing job roles/functions, and individuals who are separating from the facility/organization (e.g., retirement, termination).	Process/tools

Table D.2. Individual personnel security capabilities

Individual personnel security capabilities	Capability area
Individuals self-report incidents and anomalies that may affect trustworthiness (e.g., financial difficulties, foreign contacts). Self-reporting requirements for legal medication, use of illegal substances, arrests, travel (business and personal) outside the country, and marriage issues may provide indications of physical or mental impairment by obligating individuals to self-report.	Behavior
Individuals recognize the existence of unintentional and malicious insider threats and their potential consequences.	Behavior
Individuals are trained to recognize and report aberrant behavior that may indicate a security concern.	Knowledge/skills
Individuals are trained to understand their responsibilities related to adherence to fitness-for-duty requirements.	Knowledge/skills
Individuals are trained to recognize coercion and foster a culture of safety in which they can report threats without fear of reprisal.	Knowledge/skills

APPENDIX E

Table E.1 and **Table E.2** present security organization and individual physical security capabilities.

Table E.1. Security organization physical security capabilities

Security organization physical security capabilities	Capability area
Management understands the importance of protection against theft and sabotage. Management demonstrates its commitment through words and actions.	Behavior
Management views physical security equipment as important. Management demonstrates its commitment through timely equipment repairs.	Behavior and resources
The security organization employs knowledgeable and competent individuals who understand protective measures against insider threats.	Knowledge/skills
The security organization employs knowledgeable and competent individuals who understand what equipment and areas should be protected from insiders.	Knowledge/skills
The security organization implements measures to protect against theft and sabotage.	Processes/tools
The security organization implements measures to control access to nuclear material, related operations, and security equipment and implements measures to detect, delay, and respond to malicious insider actions.	Processes/tools
The security organization implements processes to detect and investigate prohibited items: - Vehicle and personnel search procedures - Search and seizure procedures	Processes/tools
Personnel performing searches or using equipment to detect prohibited items are trained to use the equipment and appropriately respond after identifying prohibited items.	Knowledge/skills
The security organization uses tie-downs, restraints, anchors, in-device delay kits (device hardening), high-security locks, and other barriers to minimize unauthorized removal.	Processes/tools
The security organization creates multiple layers of physical protection and procedural measures to provide additional time and opportunity for detection (e.g., two-person rule).	Processes/tools

Table E.1. Security organization physical security capabilities (continued)

Security organization physical security capabilities	Capability area
The security organization implements detection measures and a process to investigate suspicions or unauthorized activities.	Processes/Tools
The security organization employs knowledgeable and competent individuals who are capable of designing and implementing security and safety measures in an integrated manner. This integration ensures that the measures do not adversely affect facility operations and overall safety.	Knowledge/skills
The security organization employs knowledgeable and competent individuals who are capable of operating and maintaining relevant nuclear security equipment.	Knowledge/skills
The security organization employs knowledgeable and competent individuals who are capable of effectively inspecting and evaluating the protective equipment necessary to provide sufficient protection and regulatory compliance.	Knowledge/skills
The security organization implements multifactor authentication to permit access to the facility, vital areas, and risk-significant material only to authorized individuals.	Processes/Tools

Table E.2. Individual physical security capabilities

Individual physical security capabilities	Capability area
Employees at all levels possess a strong conviction regarding the credibility of threats posed by insiders and outsiders, prioritize nuclear security, and take proactive responsibility for fostering nuclear security through their actions.	Behavior
Individuals understand their roles in maintaining the integrity of access control (e.g., not allowing others to use their badges).	Knowledge/skills
Individuals understand what items are prohibited and the consequences of violating policies.	Knowledge/skills
Individuals understand the use of the two-person rule and their responsibilities related to it.	Knowledge/skills

APPENDIX F

Table F.1 and **Table F.2** present suggested nuclear material accounting and control (NMAC) organization and individual NMAC capabilities.

Table F.1. NMAC organization capabilities

NMAC organization capabilities	Capability area
The NMAC organization cultivates a strong working relationship between the NMAC department and other departments, such as physical protection, operations, radiation safety, and the analytical laboratory or other measurement groups.	Behavior
The NMAC organization implements an NMAC system that provides technical and administrative measures that serve as detection triggers that require the facility to promptly investigate and resolve irregularities involving nuclear material, thus reducing detection time.	Process/Tools
The NMAC manager is trained to recognize insider threats and is fully aware of NMAC's contributions to nuclear security.	Knowledge/Skill
The roles and responsibilities of the NMAC manager and NMAC personnel are clearly defined and documented.	Process/Tools
Sufficient resources are provided to ensure an effective NMAC system.	Resources
The NMAC organization develops facility-specific procedures that convey NMAC requirements to operations personnel.	Process/Tools
The NMAC organization provides appropriate NMAC training to all facility personnel to ensure that all NMAC requirements are properly implemented.	Knowledge/Skill
The NMAC organization implements a policy of separation of functions and responsibilities for nuclear material, whenever possible; separation of duties is sufficient to deter and detect malicious acts by insiders or the misuse of nuclear material.	Process/Tools
The NMAC organization implements a configuration management program that controls all activities that have the potential to degrade the NMAC system.	Process/Tools
The NMAC organization establishes an effective records system capable of quickly listing the current inventory; the list is used for locating items and quantifying nuclear material in process.	Process/Tools
The NMAC organization establishes additional material control measures for locations where nuclear material is particularly vulnerable to malicious insider activities.	Process/Tools

Table F.1. NMAC organization capabilities (continued)

NMAC organization capabilities	Capability area
The NMAC organization implements an effective tamper-indicating device program.	Process/Tools
The NMAC organization implements a system to analyze alarms generated by the different elements of the NMAC system and initiate appropriate responses.	Process/Tools

Table F.1. Individual NMAC capabilities

Individual NMAC capabilities	Capability area
All personnel involved with nuclear material are aware that their actions contribute to the effectiveness of accounting and control.	Behavior
All personnel internalize the importance of NMAC to nuclear security.	Behavior
NMAC personnel are aware of the importance of accuracy and the timeliness requirements of the NMAC records system.	Behavior
Appropriate individuals are trained and able to detect unusual occurrences that may indicate unauthorized removal of nuclear material.	Knowledge/Skill
All facility personnel are trained on the importance of NMAC to nuclear security and how their roles and responsibilities may affect NMAC.	Knowledge/Skill
All facility personnel exhibit an awareness of the potential consequences associated with loss of control over nuclear material and understand the sensitivity of NMAC information.	Behavior

APPENDIX G

Table G.1 and **Table G.2** present suggested cybersecurity organization and individual cybersecurity capabilities.

Table G.1. Cybersecurity organization capabilities

Cybersecurity organization capabilities	Capability area
Management develops, fosters, and maintains a robust nuclear security culture.	Behavior
The cybersecurity organization cultivates a strong working relationship between the cybersecurity department and other departments such as physical protection, operations, radiation safety, and engineering.	Behavior
The cybersecurity manager is trained to recognize insider threats and is fully aware of cybersecurity's contributions to nuclear security.	Knowledge/Skill
The cybersecurity organization implements a cybersecurity plan that includes measures against insider threats.	Process/tools
The cybersecurity organization implements measures to secure computer-based systems that are specifically intended to mitigate risks associated with cyber insider threats.	Process/tools
The cybersecurity organization implements a cybersecurity program with a graded approach to identify and protect critical digital assets.	Process/tools
The cybersecurity organization implements defense-in-depth cybersecurity mitigation strategies.	Process/tools
The cybersecurity organization employs knowledgeable and competent individuals who understand national threat assessment, the national legal framework that applies to cyber insider threats, and system design.	Knowledge/Skill
The cybersecurity organization has a process for responding to cyber-related incidents.	Process/tools
The cybersecurity organization allocates financial resources for the acquisition of cybersecurity defense equipment and software and allocates sufficient personnel to carry out cybersecurity activities.	resources

Table G.1. Individual cybersecurity capabilities

Individual cybersecurity capabilities	Capability area
Individuals are aware of their potential to be unwitting insiders.	Knowledge/Skill
Individuals understand their computer security responsibilities and the importance of these responsibilities, particularly with regard to nuclear security and safety.	Behavior
Individuals receive education and training in computer security commensurate with their roles and responsibilities.	Knowledge/Skill

APPENDIX H

Table H.1 and **Table H.2** present suggested security organization and individual protective force capabilities.

Table H.1. Security organization protective force capabilities

Security organization protective force capabilities	Capability area
Management establishes a culture in which the protective force is valued and respected.	Behavior
The security organization employs knowledgeable and competent individuals who are able to - deter, detect, and respond to potential insider threats; - conduct randomized patrols, badge verifications, and personnel searches to increase uncertainty and deter insider actions; and - implement unannounced inspections of tamper-indicating devices and sensitive areas.	Knowledge/Skills
The security organization integrates the protective forces into the overall security system and defines clear roles and responsibilities for managing insider-related incidents.	Processes/Tools
The security organization implements enhanced screening for protective forces personnel.	Processes/Tools
The security organization provides regular training and exercises to ensure preparedness for mitigating malicious insider actions.	Knowledge/Skills
The security organization implements scenario-based training programs that focus on situational awareness, response tactics, and behavioral observation, preparing protective forces for routine and high-stress situations.	Knowledge/Skills
The security organization provides adequate personnel, training, and equipment to the protective force.	Resources

Table H.1. Individual protective force capabilities

Individual protective force capabilities	Capability area
Individuals understand the roles they play in mitigating insider threats.	Behavior
Individuals understand that their roles may be stressful and may have high-stakes consequences. They seek help when they need it.	Behavior

APPENDIX I

Table I.1 and **Table I.2** present suggested plant operations organization and individual plant operations capabilities.

Table I.1. Plant operations organization capabilities

Plant operations organization capabilities	Capability area
The plant operations organization integrates the plant operations organization into the overall security system and defines clear roles and responsibilities for managing insider-related incidents.	Processes/Tools
The plant operations organization implements enhanced screening for the plant operations organization.	Processes/Tools
The plant operations organization uses various processes and tools as part of an insider threat mitigation program, such as standard operating procedures, the two-person rule, plan of the day, critical position identification, and a tamper-indicating device program.	Knowledge/Skills
The plant operations organization employs knowledgeable and competent individuals who are able to deter, detect, and respond to potential insider threats.	Knowledge/Skills
Plant operations organization personnel are seen as leaders within the organization and are ultimately responsible for all operational decisions.	Behavior
Plant operations organization personnel have the insider threat mitigation resources needed to identify, report, investigate, and mitigate potential insider threat activities.	Resource

Table I.1. Individual plant operations capabilities

Individual plant operations capabilities	Capability area
Plant operations personnel understand the roles they play in mitigating insider threats.	Behavior
Plant operations personnel understand that their roles may be stressful and may have high-stakes consequences. They seek help when they need it.	Behavior

APPENDIX J

Table J.1. and **Table.J.2** present suggested performance evaluation organization and individual system evaluation and performance assurance capabilities.

Table J.1. Performance evaluation organization system evaluation and performance assurance capabilities

Performance evaluation organization system evaluation and performance assurance capabilities	Capability area
Management recognizes the importance of system evaluation, performance assurance, and continuous improvement of the insider threat mitigation program (ITMP). Management demonstrates this commitment through words and actions.	Behavior
Management creates an environment in which individuals feel comfortable providing information to assessors/evaluators without fear of reprisal.	Behavior
The performance evaluation organization and support organizations allocate resources to perform ITMP system evaluations and implement recommendations.	Resources
The performance evaluation organization has processes for performing routine assessments of the ITMP.	Processes/Tools
The performance evaluation organization has processes for carrying out internal investigations of incidents and developing corrective actions.	Processes/Tools
The performance evaluation organization employs knowledgeable and competent individuals who are trained in evaluation techniques and insider threat mitigation.	Knowledge/Skills

Table J.2. Individual system evaluation and performance assurance capabilities

Individual system evaluation and performance assurance capabilities	Capability area
Individuals value system evaluation and performance assurance. They demonstrate their commitment to these endeavors by openly providing information to assessors/evaluators.	Behavior

APPENDIX K

Table K.1 and **Table K.2** present suggested continuous improvement organization and individual continuous improvement capabilities.

Table K.1. Continuous improvement organization capabilities

Continuous improvement organizational capabilities	Capability area
The continuous improvement organization adopts tools and methodologies that are widely used in the nuclear industry to promote continuous improvement.	Processes/Tools
The continuous improvement organization establishes postincident procedures for reviewing incidents, identifying gaps, and implementing lessons learned.	Processes/Tools
The continuous improvement organization establishes a corrective action program.	Processes/Tools
The continuous improvement organization employs knowledgeable and competent individuals who are trained in continuous improvement methods and tools.	Knowledge/Skills
Management acknowledges the significance of continuously improving the insider threat mitigation program.	Behavior
Management fosters an environment in which individuals feel comfortable reporting concerns and recommending improvements without fear of reprisal.	Behavior
The continuous improvement organization allocates resources to implement continuous improvement recommendations.	Resources

Table K.2. Individual continuous improvement capabilities

Individual continuous improvement capabilities	Capability area
Individuals recognize the value of continuous improvement.	Behavior