Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting

August 23–26 & August 30–September 1, 2021

PERSPECTIVES ON THE NEXT GENERATION OF TECHNICAL AND PROTECTIVE MEASURES FOR INSIDER THREAT MITIGATION: PREPARING FOR EXTREMIST ATTACKS

ABSTRACT

Insiders are commonly considered as the greatest threats to a nuclear security regime. Insiders pose a significant threat to nuclear and radiological security because of their privileges, authorities, and knowledge. Typically, insiders have access rights to and awareness of critical information; materials storage, usage, transport, and disposition; facilities layout, operations, and embedded systems (e.g., alarms, surveillance cameras); business operations (including transport plans); and personnel (job credentials and privileges, work schedules and assignments). Such rights give insiders an advantage to bypass and avoid dedicated security systems. In recent years, the use of emerging technologies (e.g., social media, biometrics, sensors, unmanned systems, cyber devices) have likely helped to further disguise, conceal, and advance insiders' adversarial activities. As insiders become more sophisticated with the evolution of technologies, it is necessary to develop more advanced administrative and preventive measures as first line of defense and pay greater attention to relevant technical and protective measures as a second line of defense to counter evolving or emerging insider tactics. The motivation for these countermeasures is the need for more advanced detection, delay, and deterrence methods to enhance response, recovery, and resilience to even extremist insider adversarial attacks.

INTRODUCTION

This paper provides a preliminary foundation for the development of technical measures for insider threat mitigation. The ideas presented in this paper are subject to full research and development and are offered to motivate the development of scientific and technological capabilities that may enhance prevention and protection measures for insider threat mitigation.

Insiders are usually considered to be the greatest threats to a nuclear security regime. Insiders pose a significant threat to nuclear/radiological security because of their privileges, authorities, and knowledge. Typically, insiders have access rights to, and awareness of, critical information related to materials management, facilities operations, security systems, and staff credentials and authorizations. Such rights give insiders an advantage to bypass and avoid dedicated security systems. Additionally, the use of emerging technologies (e.g., social media, biometrics, sensors, unmanned systems, cyber devices) have likely helped to further disguise, conceal, and advance insiders' adversarial activities.

As insiders become more sophisticated with the evolution of technologies, it is necessary to develop more advanced administrative and preventive measures as first line of defense and pay greater attention to relevant technical and protective measures as a second line of defense to counter evolving or emerging insider tactics. The motivation for these countermeasures is the need for more advanced detection, delay, and deterrence methods to enhance response, recovery, and resilience to even extremist adversarial attacks perpetrated by insiders.

INSIDER THREAT: MOST DANGEROUS NUCLEAR SECURITY PROBLEM

An insider is an individual with authorized access to computer and cyber-physical systems, materials, facilities, and/or transportation information and resources. Insiders pose a significant threat to nuclear and radiological security, as they generally possess access rights that combined with their authority and knowledge allow them far greater opportunities than outsiders to bypass dedicated nuclear and radiological security elements. Insiders are regarded as the most dangerous nuclear security problem (Bunn 2017).

Table 1 lists the types of insiders and how they may undermine security. This paper will focus on insiders who pass all administrative measures and function undetected in their roles and responsibilities. Such persons may likely have no administrative red flags. Nevertheless, undetectable incidents may occur after an insider becomes radicalized, coerced, disgruntled, a hacker, covetous or desperate for fame and fortune, or just unintentionally careless or unable to support his/her tasks.

Table 1. Types of Insiders and Perceived Behavioral Patterns

Types of insiders	Behavioral patterns	Likely attack strategy
Radicalized	• Cultic • Ideological • Crazed • Act out of the ordinary	Active—Violent
Disgruntled	• Angry • Displeased • Dissatisfied • Frustrated	
Greed (desperate)	• Love for fame & fortune • Covetous • Craving • Gluttony • Ravenous	
Coerced	• Compelled • Forced/pressured	Active—Nonviolent
Gamers (enthusiasts)	• Hackers • Thrill seekers	
Inadvertent	• Accidental • Careless acts • Chance • Unintentional • Unplanned	Passive

LESSONS LEARNED FROM INSIDER THREAT CASE STUDIES

Table 2 list a few insider threat case studies at nuclear and radiological facilities summarized from a paper by Pope and Hobbs (2015). These case studies occurred between early 1990s and 2015. Two notable weaknesses that insiders took advantage of were (1) weak access controls and (2) faculty detection systems for materials, tampering, and falsified documents. These case studies suggest that more advanced controls and detection systems throughout the security paradigm are measures that can be accommodated by scientific and technological tools. Nevertheless, more case studies are

needed to validate this proposition. This is especially true because of recent and emerging technologies that can be used by insiders to execute more sophisticated attacks.

Table 2. Case Studies of Insider Attacks

Case study	Where	When	Perpetrator	Notable security weaknesses
Theft of UO_2 powder at GE low enrichment uranium plant	Wilmington, NC USA	January 1979	Chemical technician—temporary employee of a GE subcontractor	Weak access controls
Theft of weapons-grade HEU, 90% of ^{235}U, at the Luch Scientific Production Association	Podolsky, Russia	1992	Chemical engineer with 25 years of service under financial hardship	Bypass nuclear material accounting and control (NMAC), no surveillance, faulty detection systems at entrances/exits
Stable isotope diversion at Elektrokhimpribor: theft of rare isotopes, ^{203}TI, ^{87}Rb, and ^{168}Yb	Russia	Early 1990s	Multiple insiders/ cooperatives (9)	Bypass NMAC - no processes to detect diluted isotopes
Theft of gold at Los Alamos National Laboratory	United States	2009	Technician with 10–20 years of service	None—Theft was detected by a radiation portal monitor, and the perpetrator was apprehended
Sabotage at Koeberg NPP	Cape Town, South Africa	December 18, 1982	Safety officer who was rehired as a temporary employee	Poor vetting procedures and weak access controls
Sabotage of Doel 4 NPP (destruction of reactor turbine)	Suez, Belgium	August 5, 2014	Unknown insider	Access to sensitive areas and tampering with turbine valves
Illegal export of ^{192}Ir from radioisotope factory of Mayak Production Association	Mayak, Russia	August 1994–1997	Factory director used falsified documents to export ^{192}Ir to the United Kingdom	Detection of falsified documents

INSIDER THREAT MITIGATION MEASURES

The International Atomic Energy Agency (IAEA) has published prevention and protection measures for insider threat mitigation. The measures are documented in *IAEA Nuclear Security Series No. 8-G (Rev. 1) – Implementing Guide – Preventive and Protective Measures against Insider Threats* (NSS 8-G Rev. 1). A brief synopsis of this implementing guide is given in Table 3. In general, the IAEA recommends implementing insider threat mitigation measures for prevention and protection of computer-based systems, materials, facilities, as well as during transport to protect against theft and sabotage. The following sections describe conventional methods used to implement the IAEA's guidance.

ADMINISTRATIVE/PREVENTION MEASURES

Administrative measures are the first line of defense against insider threats and are normally considered preventive measures. Behaviorial observation programs and human reliability programs are common platforms for implementing administrative or preventive measures. Such programs are used to establish trust and reliability of personnel and are meant to reduce the number of possible insiders. Figure 1 applies the NSS 8-G Rev. 1 to develop administrative measures designed to prevent adversarial attacks by insiders.

Administrative measures may include such things as (i) policies and procedures, (ii) access control rules, (iii) confidentiality rules, (iv) training, and (v) vetting. For the most part, administrative measures require human intervention and subjective assessments or judgments which may yield false negative results. On the other hand, they may allow insiders to bypass security practices given their knowledge and privileges.

Table 3. A Brief Synopsis of IAEA Nuclear Security Series No. 8-G (Rev. 1) *Implementing Guide: Preventive and Protective Measures against Insider Threats*

Paragraph	Guidance
3.8	A target identification process should consider all systems that could require additional protection from insider threats. Physical protection systems, NMAC systems and safety and process control systems (e.g., computer or cyber-physical systems) should be considered as potential targets for malicious acts, including those initiated by an insider adversary.
3.9	Depending on the facility or operation, computer based systems may be exploited by the insider adversary (e.g., office networks or communication computers might be used to acquire sensitive information).
3.10	The compromise of computer based systems in a facility could adversely affect safety, the security of nuclear materials or accident mitigation. The operator should evaluate and protect computer based systems that contain information related to safety or security in accordance with the risk and the potential consequences of the release of this information. This evaluation should aim to identify critical computer based systems that may be the most vulnerable to a malicious act and whose failure could result in a nuclear security event.
4.4	Nuclear security requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness and nature of the material, and the potential consequences associated with unauthorized removal of nuclear material or sabotage of nuclear material or nuclear facilities.
4.5	Implementing nuclear security measures to protect against insider threats involves selecting a combination of preventive and protective measures and implementing them in accordance with a graded approach. It is important that the measures selected be implemented and evaluated effectively so that they perform as desired. Not all measures are appropriate for every facility or operation.
4.6	Layers of preventive and protective measures should be implemented in accordance with the concept of defence in depth, such that insider adversaries would need to overcome or circumvent multiple layers of measures or technologies to achieve their objectives. These layers may consist of administrative measures (e.g., procedures, instructions, access control rules, confidentiality rules), technical measures or a combination of both. Both types of measures should integrate people and equipment.

Preventive Measures Against Malicious Acts	INSIDER THREAT MITIGATION	Mission Elements (Nuclear Security Targets for Malicious Acts)			
		Materials (NMAC Systems)	Facilities (Physical Protection Systems)	Computers & Controls Systems (Cyber Security)	Transport Systems (Transport Security of Nuclear Materials)
	Threat Assessment (Design Basis Threat)	Apply Graded Approach Based on Targeted Materials	Apply Graded Approach Based on Theft or Sabotage Scenarios Involving One or More Insider Threats at Targeted Facilities	Apply Graded Approach Based on Targeted Computers and Control Systems	Apply Graded Approach Based on Targeted Transport Systems Including Modes, Materials, Packaging, Routes, etc.
	Reduce the Number of Insiders and Minimize Insiders' Opportunities **(PERHAPS MOSTLY COVERED BY ADMINISTRATIVE MEASURES BASED ON IAEA NSS No. 8-G)**	Written Procedures for Movement or Removal of Materials from Storage Vault to Processing	***Before Employment*** • Identity verification • Personal document verification • Trustworthiness assessments ***After Employment (Graded)*** • Escorting procedures • Periodic assessment of trustworthiness • Record of persons assessing sensitive and confidential information • Strict need-to-know and need-to- access rules • Access controls using government issued ID documents or biometrics • Compartmentalized areas and times • Standard operating procedures and policies • Security awareness program • Fitness for duty program • Reporting and investigation of incidents of security ***Upon Termination of Employment*** • Terminate and revoke all access privileges	• Application of the Principle of Least Privilege to Computer Based Systems • Compartmentalized Information • Reporting and Investigation of Incidents of Information/Computer Security and Cyber-Attacks • Information Security Measures for the Acceptable Use of Computer Based Systems	
	Response				
	Training		Continuous Security Awareness Training	Cyber-Security Training	
	Evaluation	Scenario Analysis – Mod/Sim or Serious Gaming (TTX)	• Effectiveness of Security Awareness Training • Processes for Continuous Improvement • Scenario Analysis – Mod/Sim or Gaming (TTX)		

Figure 1. Preventive measures for insider threat mitigation. Green text represents science and technology opportunities for application of S&T capabilities such as those at Oak Ridge National Laboratory (ORNL).

TECHNICAL/PROTECTION MEASURES

In this paper, technical measures are considered as the second line of defense to protect against insider attacks. Assuming all administrative measures have been bypassed, the insider may now have obtained access to materials, facilities, or information. The security posture at this point would be to delay the adversary, detect when an incident has occurred as well as detect the perpetrator, and deter the completion of the attack through effective response. Technical measures for delay tactics may include restraint mechanisms such as tie-downs and locks; and secure storage compartments. Technical measures for detection may include biometrics and electronics for advanced access controls; visual analytics for surveillance and situational awareness; embedded sensors to detect tampering and location; and embedded artificial intelligence to detect suspicious human behavior. Technical measures for effective deterrence enhance response through alarm systems and intelligence developed through modeling/simulation, tabletop exercises, and cognizance training. Sound technical measures are commonly deployed to protect materials, facilities, and information against an adversarial attack. These defense measures can help to reduce the consequences of an adversarial attack. Figures 2a and 2b suggests technical measures designed to protect against insider attacks based on NSS-8G Rev 1.

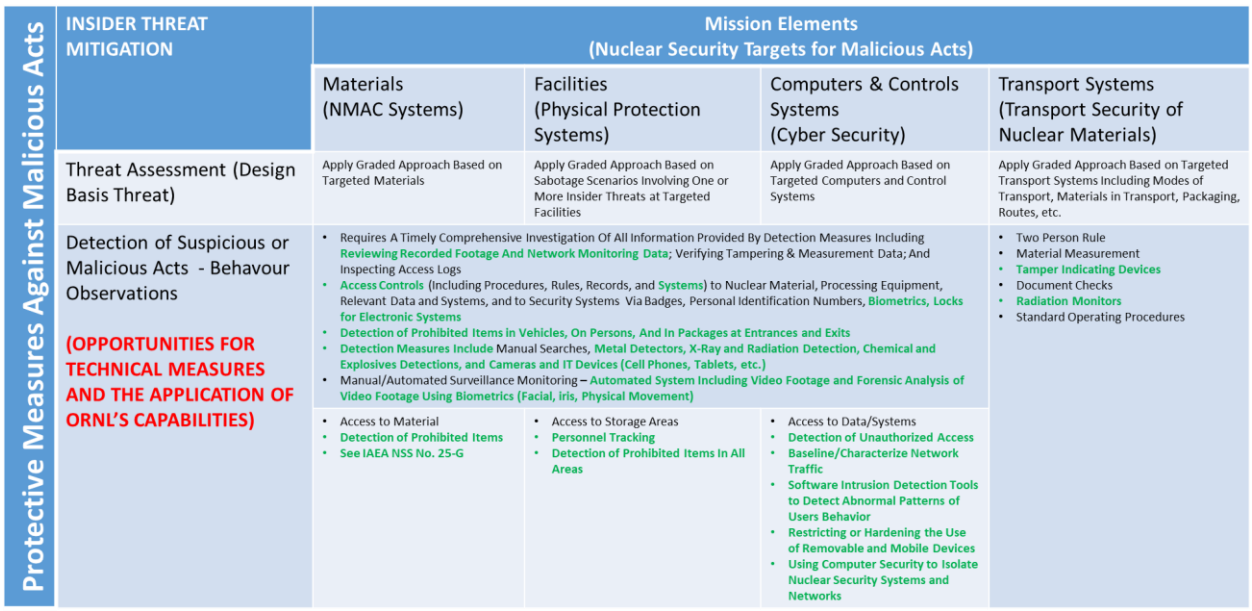

Figure 2a. Protective measures for insider threat mitigation. Green text represents science and technology opportunities for application of S&T capabilities such as those at Oak Ridge National Laboratory (ORNL).

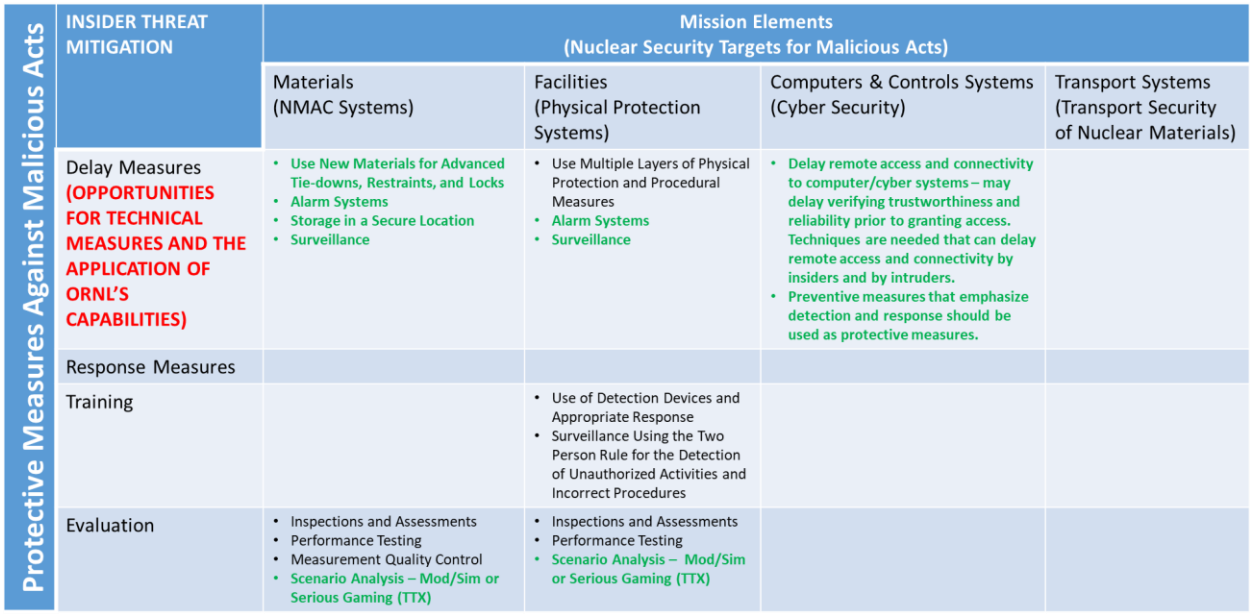

Figure 2b. Protective measures for insider threat mitigation. Green text represents science and technology opportunities for application of S&T capabilities such as those at Oak Ridge National Laboratory (ORNL).

REIMAGING TECHNICAL MEASURES FOR PROTECTION AGAINST INSIDER THREATS

The general perspective or framework for nuclear security often tends to be singularly focused on a particular risk, threat, and target. Nevertheless, consideration should be given to multiple adversaries, as well as to multiple, simultaneous, and recurring adversarial attacks. According to Bunn (2017), multiple insiders is a particularly challenging problem as the cyber age multiplies what insiders might do. Such considerations emphasize the need to develop technical measures that enhance administrative measures and that adequately and rapidly detect, delay, and deter attacks by insiders while also supplementing response, recovery, and resilience should an adversary or adversaries implement a successful attack.

Developing effective and efficient technical measures is challenging and complex. The operations of technical measures can be uncertain because insider protection is inherently difficult and is an emerging science (Bunn 2017). Nevertheless, technical measures offer the advantage of being customizable while providing the benefit of enhancing human reliability programs. Moreover, as more data become available and more insider cases are studied, technical measures can be enhanced to become more predictable and reliable in protecting against insider threats.

Table 4 summarizes some of the technical measures that are used to protect against insider threats through detection, delay, and deterrence measures. These are normally single or self-contained tactics. Although this is effective to a degree, a more effective approach would be to develop tools that integrate these three technical tactics, as shown in Figure 3. The integration of detection, delay, and deterrence should result in more advanced technical measures for insider threat mitigation.

Table 4. Technical Measures for Insider Threat Mitigation

Detection measures	Delay measures	Deterrence measures
Biometrics for access privileges	Alarms	Analytics
Behavioral pattern recognition	Communications	Decision support systems
Surveillance of suspicious activities	Fasteners	Law enforcements tools for: • Forensics • Interdiction
Tamper detection of: • Materials • Locks and alarms • Facilities access media • Surveillance cameras • Information systems • Control systems	Locks	
	Seals	
	Tie-downs	

The proposed integration is intended to improve denial and defeat. Denial could include restricting access or restricting exit upon detection of an incident. Defeat could include early identification of the adversarial insider, rapid restriction of access privileges, and instant notification to law enforcement to respond to an incident before the theft or sabotage is completed.

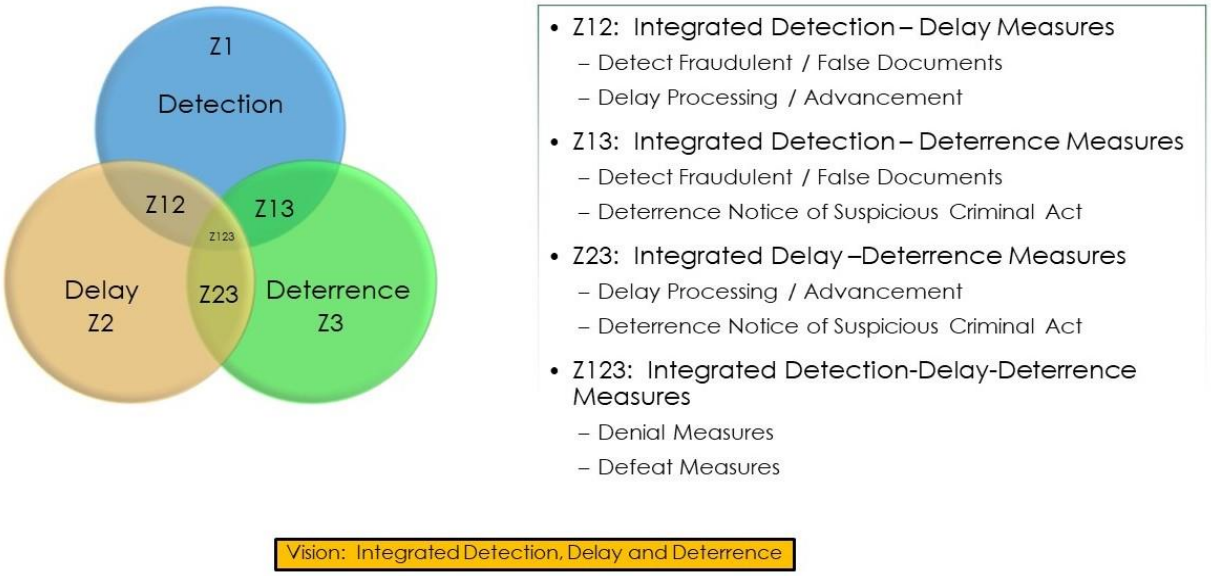

Figure 3. Integration of technical/prevention measures for insider threat mitigation.

PROPOSED RESEARCH AND DEVELOPMENT

The next generation of insider threat mitigation tactics should consider concepts and tools to defend against combinations of multiple, simultaneous, and recurring risks, threats, and targets. It is a challenging undertaking to understand the tools required by the nuclear community to ensure rapid response, recovery, and resilience after an adversarial attack perpetrated by insiders. Nevertheless, this challenge is a worthy research and development effort because the tactics used by insiders are certain to become more sophisticated with the use of new and emerging technologies. Moreover, the increasing use of social media must never be overlooked as insiders learn countermeasures based on documented case studies and insights developed from studying both successful and unsuccessful incidents as well as by collecting lessons from acts of extremism.

The ideas presented in this paper are unproven recommendations to improve insider threat mitigation. To test and evaluate these ideas for nuclear security, it is necessary to develop insider threat vulnerabilities assessments for nuclear power plants, research reactors, and advanced reactors. Indeed, the entire nuclear fuel cycle (present and future) should be assessed, especially advanced fuel cycles.

Additional cases studies of insider attacks should also be studied for at least the past decade. Case studies should focus on understanding how insiders' tactics are changing based on present and emerging technologies (e.g., cyber-physical systems, social media, mobile devices, AI tools, biometrics, remote/embedded sensors, unmanned vehicles). In addition, these technologies should be viewed with respect to the rise in global extremism, especially as it relates to the storage, use, and transport of weapons of mass destruction.

Counterintelligence offices at US Department of Energy national laboratories are perhaps a good resource for collecting a variety of information on insiders. They can also provide information about

schemes used by outsiders to coerce insiders at these facilities, especially at facilities with a wealth of knowledge and experience in the research, storage, use, transport, and disposal of nuclear and radiological materials. Information collected from counterintelligence offices throughout the Department of Energy complex may pave the way for more advanced tools that include embedded artificial intelligence.

SUMMARY AND CONCLUSIONS

According to Bunn and Sagan (2014), insider threats are perhaps the most serious challenges that nuclear security systems face. They suggest that there is a need for more in-depth, empirically grounded research on insider threats to nuclear security, as well as understanding what works best in protecting against them, especially because genuinely empirical work on nuclear security is in its infancy.

As more empirical work is developed on insider threats, it should lead to more advanced studies on recovery and resilience for complex nuclear security attacks, which may include a combination of multiple insiders with multiple targets occurring simultaneously.

Finally, note that IAEA Nuclear Security Series No. 8-G (Rev. 1) *Implementing Guide: Preventive and Protective Measures against Insider Threats* makes the following recommendations:

> "Implementing nuclear security measures to protect against insider threats involves selecting a combination of preventive and protective measures and implementing them in accordance with a graded approach (taking into account the current evaluation of the threat, the relative attractiveness and nature of the material, and the potential consequences associated with unauthorized removal of nuclear materials or sabotage of nuclear facilities)."
>
> "Layers of preventive and protective measures should be implemented in accordance with the concept of defense in depth. These layers may consist of administrative matters (e.g., procedures, instructions, access control rules, confidentiality rules), technical measures or a combination of both."

This paper has proposed integrating techniques for technical and protection measures, which should also enhance administrative and prevention measures.

REFERENCES

Bunn, Matthew, and Scott D. Sagan. 2014. A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes. Cambridge, MA: American Academy of Arts and Sciences.

Bunn, Matthew. 2017. Scenarios of Insider Nuclear Threats – And Steps to Strengthen Protection. Nautilus Institute for Security and Sustainability. https://scholar.harvard.edu/files/bunn_scenarios-of-insider-threats-to-japans-nuclear-facilities-and-materials-and-steps-to-strengthen-protection_01.pdf.

International Atomic Energy Agency. *Implementing Guide – Preventive and Protective Measures against Insider Threats*. Nuclear Security Series No. 8-G (Rev. 1). International Atomic Energy Agency, Vienna, Austria.

International Atomic Energy Agency. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*. Nuclear Security Series No. 13. INFCIRC/225/Revision 5. International Atomic Energy Agency, Vienna, Austria.

Pope, Noah Gale, and Christopher Hobbs. 2015. *Insider Threat Case Studies at Radiological and Nuclear Facilities*. LA-UR-15-22642. Los Alamos National Laboratory, Los Alamos, NM.