Pacific Northwest
NATIONAL LABORATORY

PNNL-37214

Advancing INFCIRC/908 Insider Threat Mitigation International Working Group

Activity Roadmap, 2025-2027

January 2025

Christine F. Noonan
John Landers
Jessica A. Baweja
Allison D. Irwin
Jessica K. Snider

U.S. DEPARTMENT of ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

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

Printed in the United States of America

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

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

PNNL-37214

Advancing INFCIRC/908 Insider Threat Mitigation International Working Group

Activity Roadmap, 2025-2027

January 2025

Christine F. Noonan
John Landers
Jessica A. Baweja
Allison D. Irwin
Jessica K. Snider

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Advancing INFCIRC/908 Insider Threat Mitigation International Working Group

Activity Roadmap, 2025-2027

Contents

Acronyms

ICS – Industrial Control Systems

ITM – Insider Threat Mitigation

IWG – International Working Group

OT – Operational Technology

SC – Steering Committee

Work Plan Overview

At the conclusion of the 2nd International Symposium on Insider Threat Mitigation, the Advancing INFCIRC/908 International Working Group (IWG) agreed to explore two major topics, human factors and impacts from technology, each of which is influenced by global trends and events.

The insider threat is, at its core, a human problem resulting from complex interactions among and between individual, social, political, technological, and environmental factors. To advance and support the IWG and the international community of practice, this work plan defines the scope and limitations of the two topical areas, human factors and impacts from technology; identifies tactical activities; and highlights specific opportunities to showcase regional impacts on global nuclear security.

This 2-year work plan provides a roadmap for activities the IWG and other stakeholders will undertake between 2025 and 2027. Members of the IWG Steering Committee (SC) are responsible to (1) engage the broader insider threat mitigation community of practice to inform and promote work plan activities, (2) track progress towards goals, and (3) provide updates to the IWG at regular intervals. This work plan is a living document and will be updated periodically to assess progress towards goals and will be revised as needed to address emergent and exigent areas of concern identified by the IWG.

Topical Focus Areas

Human Factors

We define *Human Factors for Insider Threat Mitigation* as

> The integration of human behavior, capabilities, and limitations into comprehensive security measures to reduce risks to nuclear and other radioactive materials and associated facilities. This involves ensuring personnel trustworthiness and reliability, minimizing human error, fostering a strong security culture, and optimizing human performance to prevent both unintentional and deliberate insider threats.

Activities in this topical area address the international community's need to understand, measure, and reduce risks associated with human behavior throughout the employee lifecycle.

Impacts from Technology

We define *Impacts from Technology* as

> The benefits and challenges enabled by technological advancements in security systems, personnel monitoring, and response protocols, which can enhance or compromise the ability to prevent, detect, and respond to insider threats.

The constant evolution of technology presents both opportunities and challenges for ITM within nuclear security contexts. Activities in this topical area will support the international community navigate the risks and rewards of technology on specific ITM measures.

Proposed Activities

Focused on Human Factors

Activity 1

Sub theme: Risk Reduction. The presence of behavioral indicators of concern (e.g., absenteeism) and other personal risk factors (e.g., recent bankruptcy) does not always result in an insider threat. But, for individuals deemed high-risk (e.g., history of substance abuse), research suggests increasing mitigators and protective factors have a positive impact on reducing poor decision making.

> **Activity Title:** Regional Workshop on Risk Reduction Measures for High-Risk Behaviors
>
> **Description**: Security personnel from across an organization may contribute to an organization's insider threat mitigation program. These various disciplines (e.g., human resources, line management, cyber security, physical security, etc.) require a common framework to detect and address high-risk behaviors, particularly those linked to mental health stressors and burnout. The workshop will focus on identifying and mitigating high-risk behaviors through proactive mental health strategies, addressing burnout predictors, and provide actionable recommendations for reducing risks. The workshop will improve an organization's ability to prevent insider threats through early intervention and support.
>
> **Audience**: Regulators, facility operators, security personnel, radiation safety officers, human resources managers, and front-line managers. Participants will be chosen based on age criteria to ensure representation from multiple generations.
>
> **Output**: Key takeaways from the workshop will be presented at the 2026 Practitioner Workshop.

Activity 2

Sub-theme: Privacy and Trust. Traditional preventive security measures (e.g., personnel vetting, continuous observation, and behavior observation programs) are effective in early detection of concerning behaviors but, if not implemented well, can jeopardize the trust between employee and employer, leading to lower morale and counterproductive workplace behaviors.

> **Activity Title:** Virtual Regional Roundtable on Personnel Vetting Challenges and Opportunities
>
> **Description**: Organizational controls used to determine trust and reliability (e.g., pre-employment screening, continuous evaluation, and workplace monitoring) can facilitate or hinder employees' trust in their organization. In this roundtable series, participants will identify strategies to implement security vetting requirements and processes while minimizing intrusiveness, explore the impacts of data and privacy regulations, and discuss the positive and negative effects of controls on the employee-employer relationship.
>
> Regions with specific materials or facility concerns and/or legal and regulatory drivers (e.g., GDPR) should be considered during the event planning process. To ensure robust dialog during the event, participants should have general knowledge about privacy legislation and vetting procedures implemented in their home country.

Audience: Regulators, facility operators, security personnel, radiation safety officers, human resources managers, and front-line managers. Participants will be chosen based on age criteria to ensure representation from multiple generations.

Output: Participants will contribute to a good practices document to equip facility leaders with tools to enhance employee trust and program compliance while maintaining robust security.

Activity 3

Sub-theme: Cultural Factors. Shared beliefs, values, and attitudes in the workplace (i.e., organizational culture) are insufficient to address subcultures, national and regional cultures, and a multigenerational, multicultural workforce.

Activity Title: Interactive Workshop Series on Adapting Security Culture for a Multigenerational, Multicultural Workforce

Description: This workshop series examines the impact of cultural dynamics on insider threat mitigation that are not currently addressed by the IAEA NSS guides on security culture.[1] The first workshop will draw speakers and participants from around the globe to explore how generational differences affect trust, communication preferences, and engagement with security protocols, particularly in settings where cultural expectations for privacy and authority vary.

Subsequent workshops will be conducted at the national or regional level. During these workshops, participants will examine how global events positively or negatively influence security culture, reporting behaviors, and adherence to security protocols. Strategies for building resilience in times of uncertainty

Audience: Regulators, facility operators, security personnel, radiation safety officers, human resources managers, and front-line managers. Participants will be chosen based on age criteria to ensure representation from multiple generations.

Outputs: Following the global dialogue, key insights to increase engagement across diverse cultural and generational groups will be documented as a flier or infographic. Practical strategies to enhance security culture resilience during times of uncertainty will be documented and shared at future regional and international 908-sponsored events.

Focused on Impacts from Technology

Activity 4

Sub-theme: Artificial Intelligence (AI) and Machine Learning (ML). AI/ML has the potential to deliver many benefits to the nuclear sector, including efficiencies and risk reduction to people and the environment. However, challenges remain using AI/ML safely, securely, and ethically. Key areas of inquiry for ITM include impacts to regulatory frameworks, trustworthiness and continuous monitoring, and physical protection systems.

[1] NSS Publications focused on security culture include: NSS 7 – Nuclear Security Culture, NSS 28-T – Self-Assessment of Nuclear Security Culture in Facilities and Activities, and NSS 38-T – Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material.

Activity Title: Regional Workshop to Explore Interfaces of AI/ML and Insider Threat Mitigation

Description: Based on regional needs and interests, topics explored will vary. Near-term topics identified by the SC include AI/ML impacts on personnel security background investigation processes; implementation of the EU Directive on AI (i.e., the AI Act); integration with existing physical protection systems; and the privacy, cybersecurity, and regulatory challenges regarding the collection, curation, and protection of long-term storage of large volumes of data. Longer-term topics identified by the SC include development and implementation of regulatory frameworks; insider adversary exploitation of AI/ML; the use of AI to enhance Behavioral Observation Programs (BOP); and advanced sensor fusion for situational awareness and latent pattern anomalies.

Audience: Regulators, operators, security personnel, cyber-security experts.

Output: A compendium of good practices when considering, introducing, and operating AI for ITM in nuclear and radiological facilities.

Activity 5

Sub-theme: Addressing Evolving Operational Technology (OT) on ITM and Supply Chain Security**.** OT systems combine hardware and software to control and automate physical processes in industry. Nuclear and radiological facilities increasingly rely on sophisticated OT for precise control and monitoring of industrial processes. Disruption to these systems can have serious consequences, because the complexity and evolution of OT systems broadens the attack surface, introducing new vulnerabilities that can be exploited by both insider and external threats.

Activity Title: Regional Workshop on Addressing Evolving OT Impacts for ITM and Supply Chain Security

Description: Based on regional needs and interests, topics explored will vary. Near-term topics identified by the SC include supply chain risk management; supply chain standards development; and risk-based approaches to vulnerability management of OT for enhanced security and reliability. Longer-term topics identified by the SC include advanced performance testing and evaluation of OT systems to enhance insider resilience.

Audience: Regulators, operators, security personnel

Output: A compendium of good practices for ITM when considering, introducing, and using OT at nuclear and radiological facilities from an ITM perspective

Highlighting INFCIRC/908 Subscriber Activities

In alignment with the IWG goals, all INFCIRC/908 subscribing nations are encouraged to identify, share, and promote best practices, training materials, practical tools, or associated resources developed within their respective countries. If shareable with the international community of practice, the SC recommends hosting such resources on the INFCIRC/908 website in a curated repository.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov