INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

# Artificial Intelligence for (AI) Nuclear Security: Expert Perspectives on AI Priorities for the Office of International Nuclear Security

September 2025

Office of International Nuclear Security

National Nuclear Security Administration

PNNL-38324

## 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**

# ARTIFICIAL INTELLIGENCE FOR (AI) NUCLEAR SECURITY: EXPERT PERSPECTIVES ON AI PRIORITIES FOR THE OFFICE OF INTERNATIONAL NUCLEAR SECURITY

September 2025

**Prepared by**
Jessica Baweja (PNNL)
Prashant Jain (ORNL)
Alan Evans (SNL)

Pacific Northwest National Laboratory
Richland, Washington 99354

# CONTENTS

# ABBREVIATIONS, ACRONYMS, AND INITIALISMS

| | |
|---|---|
| AI | Artificial Intelligence |
| AI/ML | Artificial Intelligence and Machine Learning |
| AITF | AI Task Force |
| CCTV | Closed-Circuit Television |
| FY2025 | Fiscal Year 2025 |
| INL | Idaho National Laboratory |
| INS | Office of International Nuclear Security |
| LLM(s) | Large Language Model(s) |
| ML | Machine Learning |
| ORNL | Oak Ridge National Laboratory |
| PIDAS | Perimeter Intrusion Detection and Assessment System |
| SMEs | Subject Matter Experts |
| SNL | Sandia National Laboratories |
| SRNL | Savannah River National Laboratory |
| USG | United States Government |

# ACKNOWLEDGMENTS

The Artificial Intelligence (AI) Task Force (AITF) convened in the closing months of Fiscal Year 2025 to discuss the strategy for AI work for the International Nuclear Security (INS) program within the National Nuclear Security Administration. INS would like to thank the subject matter experts who dedicated their time and expertise to producing this roadmap. Laboratories and names are listed in alphabetical order:

Oak Ridge National Laboratory
Debraj De
Eric Hoar
Jason Karcz
John Landers
Scott Nelson
Linsey Passarella
Birdy Phathanapiron
Alisa Reasor
Scott Stewart
Idaho National Laboratory:
Christopher Chwasz
Christopher Spirito
Sandia National Laboratory
Remengton Pierce
Adam Williams
Savannah River National Laboratory
Mike Brisson
Tom Danielson
Glenn Fink

# 1. INTRODUCTION

Artificial intelligence (AI) has the potential to transform nuclear security operations, offering opportunities to enhance effectiveness while simultaneously introducing new challenges. As AI technologies rapidly evolve, agencies across the United States Government (USG) are researching, implementing, and evaluating various AI models and systems. Given the broad capabilities and applications of these technologies, it is essential for each agency to identify and articulate those areas where it can make meaningful contributions aligned with its mission and expertise.

To address this need for strategic focus, in late Fiscal Year 2025 (FY2025), the Office of International Nuclear Security (INS) established an AI Task Force (AITF) to gather input from subject matter experts (SMEs) regarding the most appropriate role INS could serve in researching, evaluating, or implementing AI for nuclear security. The AITF engaged 15 experts from national laboratories with backgrounds in cyber security, physical security, transport security, insider threat mitigation, nuclear engineering, human-systems engineering, and AI/ML development.

This white paper summarizes the insights gathered from these SMEs and presents a potential roadmap for INS engagement with AI technologies. The recommendations outlined here are intended to inform INS leadership as they make strategic decisions about resource allocation and program direction in this rapidly evolving technological domain.

# 2. METHODOLOGY

To solicit SME input, the AITF developed a questionnaire addressing key aspects of AI in nuclear security, including definitions, valuable capabilities, implementation barriers, appropriate levels of autonomy, and potential INS roles. This questionnaire was distributed to subject matter experts from multiple national laboratories, including Oak Ridge National Laboratory (ORNL), Sandia National Laboratories (SNL), Savannah River National Laboratory (SRNL), and Idaho National Laboratory (INL).

Fifteen experts with backgrounds in cyber security, physical security, transport security, insider threat mitigation, nuclear engineering, human-systems engineering, and AI/ML development provided responses. Some experts responded individually, while others collaborated to provide group responses from their respective laboratories. After collecting the questionnaire responses, the AITF conducted two facilitated discussions with the SMEs in August 2025. The task force then integrated insights from both the questionnaire responses and discussions to develop the findings and suggestions presented in this white paper.

# 3. UNDERSTANDING AI FOR NUCLEAR SECURITY

SMEs characterized AI for nuclear security as technologies and approaches that augment rather than replace human capabilities. The goal of AI in nuclear security, according to expert input, is to provide insights for human decision-makers rather than to conduct autonomous operations. In addition, AI should enhance threat detection by analyzing data “in ways humans alone can't” to identify potential security concerns faster and more accurately. AI for nuclear security was also described, ideally, as a means to increase productivity, decrease response time, and enhance resilience in protecting nuclear material.

One other function of AI in nuclear security, according to experts, is to integrate diverse data sources. Connecting information across different systems and modalities can identify patterns not visible through single-source analysis. Finally, experts also highlighted the need to address both defensive

and offensive security considerations. Although AI can enhance nuclear security effectiveness, it can also serve as an additional threat vector that must be considered.

# 4. INS'S STRATEGIC ROLE

Rather than suggesting that INS should be directly involved in AI technology development, experts generally viewed INS's contribution through the lens of its established strengths in knowledge exchange and guidance development.

Facilitating dialogue between key stakeholders emerged as the most widely supported role, endorsed by nearly all responding experts. SMEs suggested that INS could serve as a valuable bridge between AI technology developers, nuclear security practitioners, and regulatory authorities. This "translator" function would help security practitioners better understand AI capabilities and limitations and also help technology developers understand the unique requirements of nuclear security applications.

Developing guidance and evaluation frameworks was identified as another key role for INS. Several experts suggested that INS could help establish frameworks for evaluating AI technologies in specific nuclear security contexts. SMEs emphasized that such frameworks should focus on performance considerations and evaluation approaches rather than prescriptive requirements, understanding that regulatory standards remain the purview of each state's competent authority.

Adapting commercial solutions for nuclear security applications was suggested by many experts, who saw value in INS helping partners evaluate and adapt existing commercial AI solutions to meet nuclear security requirements. Building international capacity received support from several experts, particularly in the context of knowledge sharing and training, though some cautioned against extensive international partner training before operational AI use is established.

Only one expert suggested that INS should develop proprietary AI tools, indicating minimal support for INS entering the technology development space directly. This aligns with the general view that INS's strengths lie in facilitating dialogue, developing evaluation guidance, and knowledge sharing.

# 5. PRIORITY APPLICATION AREAS

Physical security monitoring emerged as one of the top priority areas, selected by a majority of experts. SMEs highlighted AI's potential to enhance video surveillance systems, perimeter intrusion detection, and alarm assessment. This application area directly addresses persistent challenges in maintaining vigilant security monitoring while managing false alarm rates.

Cyber security for nuclear facilities received similar levels of support from the experts, with recognition of the growing cyber threat landscape facing nuclear facilities and the potential for AI to enhance threat detection, network monitoring, and incident response.

Insider threat detection was identified as a high-priority application by many SMEs. Several highlighted this as their foremost concern, with one stating it is "one of the most severe concerns to nuclear security globally." They noted that current approaches relying primarily on badge access data and CCTV footage have significant limitations, as demonstrated in incidents like the Doel-4 sabotage from 2014.

# 6. LLMS AND FOUNDATION MODELS IN NUCLEAR SECURITY

SMEs offered varying perspectives on large language models (LLMs) and foundation models in nuclear security, revealing both potential applications and significant cautions.

Several experts identified document processing as a promising application, with one describing LLMs as "information assistants" that could summarize complex documents and highlight key points from incident reports or regulations. Training applications were also discussed, with suggestions that LLMs could generate realistic exercise scenarios including novel attack vectors that security personnel might not anticipate.

Some experts saw potential for insider threat detection through analysis of logs, emails, and databases, while others suggested operational support roles where LLMs could provide quick access to procedures and guidance. One expert proposed that emerging technologies could enable operational technology devices to communicate with LLMs, allowing operators and managers to dialogue with the plant as a whole.

However, SMEs also expressed significant caution. One expert stated, "I see no clear use case for LLMs at this point." Others emphasized the need for careful evaluation before deployment, with one warning that models would need to be "benchmarked for INS missions" rather than used with default settings. Several experts raised concerns about hallucinations and accuracy in security contexts, where false information could have serious consequences. Security considerations were also highlighted, with one expert cautioning against using models "trained by a potentially hostile country or organization" and recommending specific open-source alternatives.

An important distinction emerged regarding implementation: near-term applications might be more practical for internal INS use—developing training materials or generating scenarios—rather than partner deployment of LLMs, which could present significant challenges related to infrastructure, security, and maintenance.

Overall, SMEs suggested LLMs could serve valuable supporting roles—particularly for information processing tasks—but emphasized the need for careful evaluation and appropriate human oversight in security-critical contexts.

# 7. RECOMMENDED ACTIVITIES AND IMPLEMENTATION APPROACHES

Based on these priority areas, SMEs identified several high-value activities for INS engagement.

## 7.1 DOMAIN-SPECIFIC TESTING FRAMEWORKS

Several experts noted the need for standardized approaches to evaluate AI-enabled systems for specific applications. While there was general agreement that INS should not become a product certification body, experts recognized that limited testing activities might be necessary to develop effective evaluation frameworks and identify limitations in commercial technologies.

One expert with direct experience described leading an effort to evaluate commercial video analytics vendors against simulated intrusion tests in a PIDAS environment. This expert noted that while certain aspects are straightforward to test, detection capabilities—specifically the true positive

versus false positive rates—require careful methodology to enable meaningful comparison across platforms.

Several experts emphasized the importance of focusing on specific security domains rather than attempting to address all AI applications simultaneously. Areas frequently mentioned included perimeter intrusion detection, access control, alarm assessment, and insider threat detection. By narrowing the scope to particular applications, INS could develop more practical and immediately useful evaluation tools.

Rather than conducting extensive product assessments, experts suggested that INS's testing activities should focus on:

- Developing methodologies that partners can use for their own evaluations
- Identifying gaps between commercial AI capabilities and nuclear security requirements
- Creating realistic testing scenarios that reflect actual security challenges
- Providing insights on how commercial technologies might need to be adapted for nuclear security

As one expert noted during discussions, educating partners is a better focus than doing extensive testing directly. However, this expert also acknowledged that to educate effectively, “we need to do the work, but not in a way that produces a matrix of acceptable or unacceptable things.”

## 7.2 KNOWLEDGE EXCHANGE ON USE CASES

Given that nuclear security organizations often operate with limited visibility into peers' experiences with emerging technologies, INS could facilitate targeted knowledge exchange. During the August discussions, SMEs suggested documenting case studies on successful AI implementations, including concrete examples of security improvements and operational efficiencies.

## 7.3 DOMAIN-SPECIFIC TRAINING RESOURCES

Many organizations lack personnel who understand both AI capabilities and domain-specific security requirements. One expert emphasized that all stakeholders, “even if some of them will not directly use the AI models… need to [have] an emphasis on broad AI literacy.” Several experts noted that training should be tailored to different audiences, such as security managers, regulatory personnel, and facility operators.

An important consideration, however, was the speed of AI development: training activities would need to focus on foundational concepts and knowledge building that will not be significantly altered by the pace of change in technology. However, there did seem to be agreement that there is foundational knowledge in AI for nuclear security that would be less subject to this rapid pace of change.

## 7.4 SCENARIO DEVELOPMENT FOR TESTING

Several SMEs suggested that INS could develop realistic scenarios specifically designed to test how AI-enhanced security systems perform under various conditions and against different threat vectors. One expert also proposed using AI itself to “generate diverse, realistic security scenarios for tabletop exercises” to help identify novel attack vectors.

Another expert suggested creating “scenarios where AI capabilities were tested against human capabilities” to “optimize and find balance for where AI can be leveraged more heavily and areas where it may add minimal benefit or even hinder security.”

### 7.5 GUIDANCE ON EVALUATION METHODS

As AI-enabled security systems become more common, nuclear security managers and regulators need approaches to evaluate whether these systems meet their specific requirements. Rather than setting performance benchmarks, INS could provide guidance on testing methodologies that partners could use to assess AI technologies against their own established requirements.

Several experts emphasized the importance of considering both security performance and cost-effectiveness in evaluation approaches. One SME specifically mentioned using “effectiveness increase or cost decrease” as key metrics for successful implementation.

## 8. ACTIVITIES THAT MAY FALL OUTSIDE CORE FOCUS

While SMEs identified numerous valuable activities for INS engagement with AI, they also highlighted several areas that may fall outside INS's core focus. Developing proprietary AI models or solutions received minimal support from experts, with most emphasizing leveraging existing commercial or academic solutions. Extensive product testing across multiple vendors was generally viewed as beyond INS's appropriate scope; efforts should focus on how the testing is conducted rather than testing and evaluation of large numbers of products. Data collection and hosting for AI systems raised concerns related to security, privacy, and data ownership. Leading fundamental AI research was seen as better left to research institutions and technology developers with more resources or deeper AI expertise. These boundaries reflect both practical limitations of INS's resources and strategic considerations about where the program can add unique value.

## 9. MEASURING SUCCESS IN AI PROJECTS

SMEs emphasized measuring success through quantifiable security improvements and cost-effectiveness, such as:

- **Workforce optimization**: Measuring reductions in staff hours required for routine monitoring activities
- **Faster threat detection and response times**: Comparing response times before and after AI implementation
- **Operational efficiency improvements**: Tracking metrics like productivity increases and decreased investigation time
- **Training cost reduction**: Achieving improved training results while potentially reducing delivery costs

These metrics help partners make business-case justifications for AI investments while ensuring that technology adoption serves genuine security needs rather than following technology trends.

# 10. IMPLEMENTATION CONSIDERATIONS

SMEs recommended a phased approach to implementation of AI efforts, starting with small-scale projects that demonstrate value before expanding to broader initiatives. One expert advocated for "starting small and scaling up: pilot projects or limited deployments can demonstrate value and uncover challenges on a manageable scale."

Strategic sequencing of activities was highlighted as important, with initial efforts focusing on foundational resources like evaluation frameworks and educational materials. Collaborative partner engagement approaches were suggested, including technical exchanges and even "hackathon" events to develop and immediately test AI concepts.

The rapidly evolving nature of AI technologies was acknowledged as both a challenge and opportunity, requiring implementation approaches that remain relevant despite technological change.

# 11. CONCLUSION

The expert input described here suggests that they believe INS should focus on enabling partners to identify and implement cost-effective AI applications that deliver measurable nuclear security benefits through knowledge exchange and evaluation guidance.

## 11.1 KEY ACTIVITIES FOR INS

Rather than developing technologies or leading the development of standards, INS can provide the greatest value for partners by serving as a knowledge broker and evaluation guide in this rapidly evolving domain. The highest-priority application areas identified by experts—physical security monitoring, cyber security, and insider threat detection—represent domains where AI technologies could potentially deliver significant security improvements with tangible cost benefits.

Six key activities emerged as particularly promising for INS engagement, arranged in order of priority:

1. **Developing targeted testing frameworks** for specific AI applications in nuclear security. By creating methodologies for evaluating AI-enabled systems in domains like perimeter intrusion detection or video analytics, INS can help partners assess whether these technologies enhance security capabilities in a cost-effective manner.
2. **Supporting the development of realistic testing scenarios** that help evaluate AI system performance under conditions relevant to nuclear security. These scenarios would allow partners to assess AI capabilities against their specific security requirements before making significant investments.
3. **Facilitating knowledge exchange on real-world implementations**. By documenting case studies and lessons learned from early AI adopters, INS can help partners avoid costly mistakes and identify high-value applications with demonstrated return on investment.
4. **Helping partners to build regulations or validation and verification processes** using evaluation frameworks as the guide. Given a deeper understanding of the evaluation processes for AI-enabled systems from these targeted activities, INS can help partners to develop validation and verification processes for integration of those systems into the nuclear security enterprise.

5. **Providing guidance on evaluation approaches**—not setting benchmarks—that help partners assess AI technologies against their own established requirements while respecting national regulatory frameworks.
6. **Building domain-specific training resources** that enhance AI literacy among nuclear security practitioners. Tailored educational materials would enable security managers, operators, and regulators to make more informed decisions about AI technologies without requiring extensive technical expertise.

## 11.2 A POTENTIAL INTEGRATED AI TESTBED FOR NUCLEAR SECURITY

Three of the activities above have a common theme – testing and evaluation (T&E) of AI systems: targeted testing methodologies, realistic testing scenarios, and evaluation approaches (along with benchmarking if desired). The synergy among these three activities suggests the potential for an additional, larger, activity that INS could spearhead in this space with the assistance of other DOE offices. An integrated testbed for demonstrating or evaluating in a standardized manner—the performance of selected AI systems (including, but not limited to, physical protection system components, such as cameras, video analytics, access control systems) would have multiple benefits. It can serve as a demonstration site for international partners for testing and evaluation (T&E) approaches and can also support other activities identified above in terms of knowledge exchange and training. It could also serve as a testing resource for US advanced reactor vendors. It could also potentially support regulators to execute their own evaluations of AI systems that may be part of license applications. In all of these situations, various AI systems and solutions can be evaluated for both the opportunities they provide to enhance security system effectiveness, consistency and reliability of performance, as well as the risks of potential adversarial use of such systems - all while allowing the DOE to learn and improve based on the evaluations of these systems.

In pursuing all AI activities, INS should maintain a clear focus on measurable security improvements and cost-effectiveness. Success metrics should emphasize tangible outcomes such as reduced false alarm rates, workforce optimization, faster threat detection, and other efficiency gains that translate directly to cost savings or security enhancement.

By focusing on practical guidance, knowledge exchange, and targeted training in specific application areas, INS can help partners navigate the complex landscape of AI technologies and make informed decisions that enhance nuclear security while delivering clear return on investment. This approach represents the most effective path forward for INS's engagement with artificial intelligence in support of its core mission to prevent nuclear theft and sabotage worldwide.