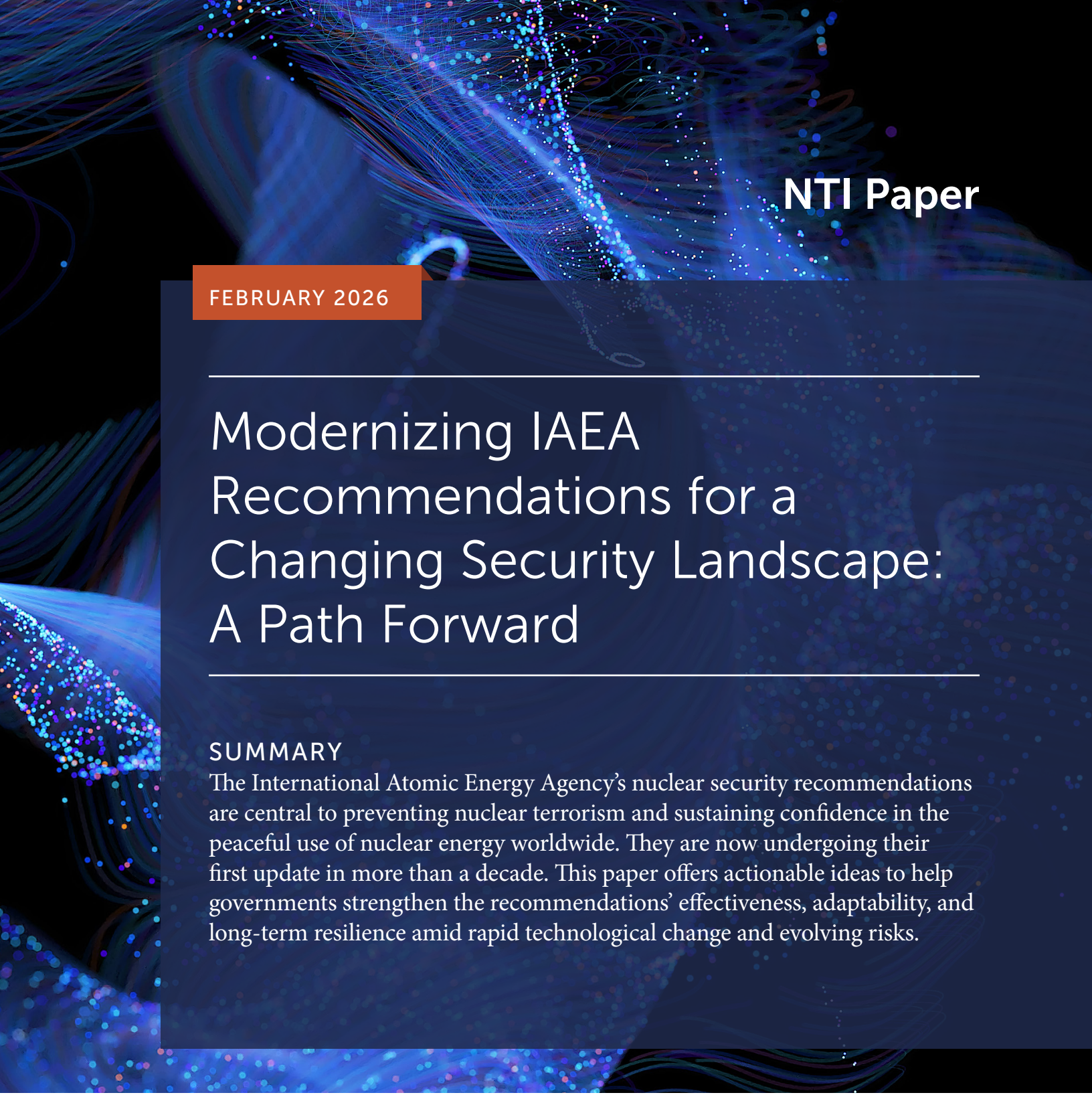

NTI Paper

FEBRUARY 2026

Modernizing IAEA Recommendations for a Changing Security Landscape: A Path Forward

SUMMARY

The International Atomic Energy Agency's nuclear security recommendations are central to preventing nuclear terrorism and sustaining confidence in the peaceful use of nuclear energy worldwide. They are now undergoing their first update in more than a decade. This paper offers actionable ideas to help governments strengthen the recommendations' effectiveness, adaptability, and long-term resilience amid rapid technological change and evolving risks.

NTI
BUILDING A SAFER WORLD

Contents

Acknowledgments

NTI would like to express its gratitude to the participants in the most recent meeting of the Global Dialogue on Nuclear Security Priorities and to those who contributed to the workshop at the Institute of Nuclear Materials Management Annual Meeting. Their insights were invaluable in identifying key areas of the guidance that should be revised.

We are especially grateful to Dr. Sarah Case Lackner for her excellent paper, which provided thoughtful recommendations and helped launch this effort. We also thank Nickolas Roth for his tireless leadership in developing this working paper, and Scott Roecker, Ross Matzkin-Bridger, Maegon Barlow, and Sophia Brown for their careful review and constructive edits.

Introduction

As the internationally recognized benchmark for physical protection standards, the International Atomic Energy Agency's (IAEA) *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (NSS No. 13 (INFCIRC/225/Rev. 5)), published in 2011, has played a critical role in shaping national regulations, facility-level practices, and international cooperation on nuclear security.[1]

More than a decade later, however, the nuclear security landscape has shifted. National regulations and practices have matured, international institutions and norms are stronger, countries have made new political commitments, and legally binding agreements are adhered to more widely. At the same time, global threats—intensified by rapid technological change—pose new challenges to physical protection systems. In response, the IAEA has initiated a revision of this foundational guidance.

The revision process offers a timely opportunity to ensure that the recommendations reflect today's threat environment and the realities of growing interest in nuclear energy.

The revision process offers a timely opportunity to ensure that the recommendations reflect today's threat environment and the realities of growing interest in nuclear energy; incorporate lessons from more than a decade of implementation; and remain relevant, inclusive, and actionable for all Member States and nuclear industry. This paper focuses on many of the priority areas identified in the revision process:

1. Insider threats
2. Emerging threats
3. Information and computer security
4. New and emerging technologies
5. The sustainability and resilience of nuclear security regimes.

To keep pace with evolving challenges—and to benchmark against advances in security practices from non-nuclear sectors—Member States should support the adoption of the measures recommended in this paper in the IAEA's updated nuclear security guidance.[2] Our recommendations, however, are intended to be the beginning of the conversation. Stakeholders should treat the following recommendations as both practical guidance and food for thought—using them as a foundation for continued improvement, innovation, and leadership in nuclear security.

[1] For the remainder of this paper, this document is referred to as INFCIRC/225/Rev. 5.

[2] This paper draws upon Dr. Sarah Case Lackner's contribution to the 2025 Global Dialogue on Nuclear Security Priorities, as well as the earlier multi-author report on the future of IAEA physical protection guidance. See Sarah Case Lackner, "Recommendations for the Ongoing Revision of IAEA NSS No. 13 (INFCIRC/225/Rev. 5)," Paper presented at the Global Dialogue on Nuclear Security Priorities, Addis Ababa, 2025, https://www.nti.org/wp-content/uploads/2025/08/Recommendations-for-the-ongoing-revision-of-IAEA-NSS-21.pdf and Matthew Bunn, Laura Holgate, Dmitry Kovchegin, Nickolas Roth, and William H. Tobey *IAEA Nuclear Security Recommendations* (INFCIRC/225): *The Next Generation* (Cambridge, MA: Harvard University Belfer Center for Science and International Affairs and Nuclear Threat Initiative, 2013), https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/IAEA%20225%20Recommendations.pdf.

The Appropriate Level of Detail for IAEA Guidance

As the IAEA undertakes revisions to INFCIRC/225/Rev. 5, it will be important to preserve the character of the document as a *guidance* standard—one that establishes meaningful expectations for physical protection while leaving space for Member States' implementation to be flexible and evolve over time. Guidance should be sufficiently clear and specific to convey the essential attributes of effective physical protection systems; set a baseline for implementation; and support consistent interpretation by regulators, operators, and peer review mechanisms. Without this level of specificity, the document risks appearing aspirational rather than practical, reducing its value as an international benchmark.

At the same time, guidance should avoid becoming so prescriptive that it constrains innovation or fails to accommodate the wide variation in national regulatory frameworks, technical infrastructures, and threat environments. Detailed technical methods, procedural steps, and specific implementation pathways are more appropriately housed in IAEA Implementing Guides and Technical Guidance, where they can be updated more rapidly and tailored to differing national contexts.[3]

Accordingly, the updated INFCIRC/225/Rev. 5 should:

- Articulate clear, outcome-oriented guidance and specific roles and responsibilities that define what effective physical protection should achieve, not merely high-level principles.
- Identify essential programmatic elements where consistency is required across all states that engage in nuclear activities.
- Provide enough detail to serve as a meaningful benchmark for international cooperation, peer review, and capacity building.
- Ensure flexibility so that states can choose appropriate methods and technologies suited to their legal frameworks, resources, and threat environments.

This balance—between robust expectations and adaptable implementation—is central to keeping INFCIRC/225/Rev. 5 both authoritative and durable. By defining clear standards while preserving space for country-specific approaches, the revised guidance can remain relevant as technologies evolve, new threats emerge, and Member States expand and mature their nuclear security regimes.

[3] For more on IAEA Implementing Guides and Technical Guidance, see International Atomic Energy Agency, Nuclear Security Series, https://www.iaea.org/resources/nuclear-security-series.

An Overview of Global Changes Impacting Nuclear Security

Since 2011, international consensus on nuclear security implementation has advanced significantly. Senior-level meetings, international institutions, multilateral agreements, and national actions have all contributed to strengthening nuclear security regulations and practices, and the broader international architecture.

Key milestones during this period were the Nuclear Security Summits, held from 2010–2016. At these four summits, more than 50 world leaders recognized nuclear terrorism as one of the "most challenging threats to international security" and affirmed that robust nuclear security is the most effective safeguard against terrorists or criminals acquiring nuclear materials. Each summit produced consensus communiqués and generated national, bilateral, and multilateral commitments—some of which were formalized as IAEA Information Circulars (INFCIRCs).[4]

These commitments, framed as "house gifts" and "gift baskets," advanced practical measures in areas such as the mitigation of insider threats, the minimization and elimination of civilian highly enriched uranium (HEU), transportation security, and certified training for nuclear security management. This senior-level engagement has continued through the IAEA's International Conferences on Nuclear Security (ICONS), where ministers meet every four years to discuss nuclear security implementation, and through the process to review the Amended Convention on the Physical Protection of Nuclear Material.

Several commitments from the Nuclear Security Summits built on the principles outlined in INFCIRC/225/Rev. 5, whereas others went further. For example, the Mitigating Insider Threats Gift Basket—endorsed by more than 30 countries and later codified as INFCIRC/908—committed states to establish programs addressing insider risks. Likewise, the Civilian HEU Minimization Gift Basket, published as INFCIRC/912, brought together more than 20 countries that pledged not to use HEU in new civilian facilities and to convert or shut down existing HEU reactors as soon as feasible. Two participating countries have since eliminated their HEU stocks altogether.[5] This call to minimize HEU has continued in international meetings, including in the 2024 ICONS co-president's statement endorsed by dozens of countries. Notably, INFCIRC/225/Rev. 5 contains no explicit guidance on minimizing or eliminating HEU.[6]

Peer review also became an area of growing international consensus. Since the publication of Rev. 5, the IAEA has conducted more than half of the more than 100 International Physical Protection Advisory Service (IPPAS) missions carried out since the program began in 1996. In addition, the IAEA has steadily strengthened nuclear security through the publication of new Implementing Guides and Technical Guidance documents covering insider threats, security culture, computer security at nuclear facilities, and development of a design basis threat, among others.

[4] Seoul Communiqué 2012 Seoul Nuclear Security Summit, https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjfywj_665252/202406/t20240606_11405355.html.

[5] Nigeria and Poland.

[6] International Atomic Energy Agency, Statement by the Co-Presidents of the International Conference on Nuclear Security 2024: Shaping the Future 20-24 May 2024, https://www.iaea.org/sites/default/files/24/05/joint_statement_of_the_co-presidents_icons_2024.pdf.

At the same time, the threat landscape has changed dramatically. During this same period, terrorist activity underscored new dimensions of vulnerability and nuclear risk. In 2011, months after Rev. 5 was issued, Anders Breivik committed an attack in Norway that claimed the lives of dozens. His 1,500-page manifesto included roughly 30 pages on radiological and nuclear terrorism, with a particular focus on insider attacks. In 2017, a Nevada National Security Site guard, Jessica Glover, reported enduring sexual harassment, sexual assault during training, and reprisals for speaking out—revealing a failed security culture and insider threats. Protective forces cannot possibly have the requisite trust in each other to defeat dangerous threats when team members are attacking each other.

Other insider threats have manifested in high-profile nuclear incidents. In 2014, an insider sabotaged the Doel-4 nuclear power plant in Belgium. Although the perpetrator was never identified, the subsequent investigation revealed that two employees with access to vital plant systems had previously left Belgium to fight for terrorist groups in Syria. In response, Belgium substantially strengthened its defenses against insider threats, expanding surveillance measures and mandating broader application of two-person and three-person rules and has played an important leadership role in strengthening international insider mitigation practices.

Protective forces cannot possibly have the requisite trust in each other to defeat dangerous threats when team members are attacking each other.

Although effective nuclear security is largely about the people responsible for implementation, the evolution of technology has seen important change. Emerging technologies have created both new opportunities and new vulnerabilities for nuclear security. Advances in cyber capabilities, uncrewed systems, and artificial intelligence (AI) are reshaping the threat landscape in ways that were scarcely anticipated when INFCIRC/225/Rev. 5 was issued.

Cybersecurity is now one of the most prominent areas of concern. In 2019, the Kudankulam Nuclear Power Plant in India was targeted by a sophisticated cyberattack against "mission-critical" systems, highlighting the potential for malicious actors to disrupt operations or compromise sensitive data. Similar cyber intrusions have been reported at nuclear-related facilities in other countries, demonstrating that both state and non-state actors view nuclear infrastructure as a strategic target. The growing digitalization of nuclear facilities expands the attack surface for cyber adversaries.

Uncrewed aerial vehicles (UAVs, or drones) represent another major emerging threat. Drones have been used in attempted attacks on nuclear facilities, including incidents in Ukraine, France, and the Middle East. Their relatively low cost, ease of acquisition, and ability to bypass traditional physical protection systems make them particularly concerning. A well-coordinated UAV attack could distract, surveil, or directly damage nuclear facilities.

On the one hand, AI offers promising tools for anomaly detection, insider threat monitoring, and predictive security analysis. On the other, AI compounds these risks by creating opportunities for adversaries to launch more sophisticated cyber intrusions, disinformation campaigns targeting nuclear facilities or operators, and automated swarm drone attacks that overwhelm existing defenses. The dual-use nature of AI creates significant policy and regulatory challenges.

Taken together, these developments illustrate how far international nuclear security consensus has advanced since INFCIRC/225/Rev. 5—and how profoundly the threat environment has shifted.

More recently, state-sponsored terrorism and the deliberate targeting of energy infrastructure—including nuclear facilities—have become notable concerns. Armed conflict and geopolitical competition are blurring the line between civilian and military targets, as seen most starkly in attacks and coercive actions affecting nuclear power plants and associated infrastructure. These developments underscore that, although outside the traditional IAEA purview, nuclear security can no longer be viewed solely through the lens of non-state terrorist threats. Instead, it must account for heightened state-level risks, hybrid threats, and sustained crisis environments in which facilities may be deliberately targeted, personnel placed under extreme stress, and normal security assumptions disrupted.

These risks are growing as the global civil nuclear landscape is pursuing renewed growth and diversification. Potentially dozens of nuclear newcomers are expressing interest in nuclear energy for the first time, while established nuclear energy states are advancing first-of-a-kind deployments of advanced and small modular reactor (SMR) designs. These developments introduce novel security challenges alongside their potential benefits. New entrants may face gaps in regulatory capacity, institutional experience, and security culture, while SMR deployments raise questions related to transportable reactors, novel fuel forms, multi-module sites, co-location with non-nuclear infrastructure, and expanded reliance on digital systems and remote operations. Many of these issues were not anticipated when INFCIRC/225/Rev. 5 was finalized, underscoring the need for updated guidance that reflects both the scale and diversity of today's civil nuclear expansion as well as the more complex, contested, and technologically enabled risk environment.

Opportunities for Action

The following recommendations identify priority areas where updates to INFCIRC/225/Rev. 5 would strengthen its relevance and effectiveness in today's nuclear security environment. They focus on addressing evolving and emerging threats, reinforcing the human and organizational dimensions of security, integrating digital and technological risks, and ensuring that nuclear security regimes remain resilient, adaptive, and sustainable over time. Together, these recommendations are intended to provide clearer, more actionable guidance that reflects both the expanding diversity of civil nuclear activities and the increasingly complex threat landscape.

Insider Threats

Strengthening Approaches to Insider Threats

Insider threats remain among the most serious and complex challenges to nuclear security, yet their treatment in INFCIRC/225/Rev. 5 is limited. Nearly every documented case of nuclear theft or sabotage, in which details are known, has involved some insiders. Insiders possess inherent advantages: authorized access that can circumvent multiple layers of protection, detailed knowledge of systems and their vulnerabilities, trust from colleagues that reduces suspicion and eases recruitment, and the ability to plan and act over extended periods. Rev. 5 recognizes that insiders "could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures." However, the current text does not sufficiently reflect the scale or evolving nature of this threat.

Recommendations

The revised INFCIRC/225/Rev. 5 should strengthen and expand guidance on insider threats within the threat assessment section. Although paragraph 3.36 acknowledges insider risks, it does not convey the depth of the challenge or the distinct measures required to address it. The revision should clearly articulate that effective protection against insiders requires approaches beyond those developed for external adversaries and should recommend the establishment of national and/or site-level Insider Threat Mitigation Programs with clearly defined fundamental requirements.

Building on existing language, the document could include a new paragraph on "Requirement for Insider Threat Mitigation Programs."

New paragraph 3.36 bis or 3.37 could read:

> States should establish and maintain national and/or facility-level Insider Threat Mitigation Programs, proportionate to the threat and risk, as an integral component of the nuclear security regime. Such programs should be systematic, documented, subject to regular reviews and focused on continuous improvement.

To define insider threat program requirements, INFCIRC/225/Rev. 5 should—where relevant in paragraphs 3.47, 4.48, 5.14—highlight recommendations from both the Mitigating Insider Threats Gift Basket (INFCIRC/908), endorsed by more than two dozen countries—including most with weapons-usable material—and IAEA Nuclear Security Series No. 8-G, *Preventive and Protective Measures against Insider Threats*.[7]

Strengthening the treatment of insider threats in these ways would align INFCIRC/225/Rev. 5 with contemporary risks, reflect internationally endorsed best practices, and provide states with clearer and more actionable expectations for addressing one of the most consequential threats to nuclear security.

Security Culture

The human dimension of nuclear security is a key element of preventing insider threats that governments have made significant progress on strengthening since the publication of Revision 5. These efforts have had a particular emphasis on fostering and sustaining robust security culture.[8] INFCIRC 225/Rev. 5 emphasizes important elements of security culture, including:

The recognition that threats exist.

- The importance of collaboration between governments, organizations, managers, and individuals to maintain security culture.
- The benefit of promoting and encouraging security culture.
- The value of regularly updating all personnel about physical protection.
- The document states, "[a]ll organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization," but could further build upon this idea.

Recommendations

A revision of INFCIRC/225/Rev. 5 could recommend establishing a comprehensive nuclear security culture program that engages the entire enterprise, incorporates effective motivation techniques, and minimizes complacency—a concept endorsed in Nuclear Security Series 7, *Nuclear Security Culture*.[9] Strengthening the treatment of security culture in this way would help ensure that personnel at all levels recognize their role in sustaining robust protection measures.

[7] See International Atomic Energy Agency, *Preventive and Protective Measures Against Insider Threats*, Nuclear Security Series No. 8-G (Rev. 1) (Vienna: IAEA, 2022), https://www.iaea.org/publications/12354/preventive-and-protective-measures-against-insider-threats, and IAEA, *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* (Vienna: IAEA, 2017), https://www.iaea.org/publications/documents/infcircs/communication-dated-22-december-2016-received-from-the-permanent-mission-of-the-united-states-of-america-concerning-a-joint-statement-on-mitigating-insider-threats.

[8] Security culture defined here as the assembly of characteristics, attitudes, and behaviors of individuals, organizations, and institutions that serves as a means to support, enhance, and sustain nuclear security.

[9] International Atomic Energy Agency, *Nuclear Security Culture*, Nuclear Security Series No. 7 (Vienna: IAEA, 2008).

Since the publication of INFCIRC/225/Rev. 5, the IAEA has issued technical guidance on how to conduct nuclear security culture self-assessments. Incorporating this into the revised text would provide states and operators with a practical tool for evaluating and improving their programs.

Such additions would build naturally on the existing section on nuclear security culture (paragraphs 3.48–3.51):

> Paragraph 3.50: The State should require comprehensive security culture programs that promote a nuclear security culture and encourage all security organizations to establish and maintain one. A nuclear security culture should be pervasive in all elements of the physical protection regime. *The importance of this culture should be promoted from the very top management of organizations, as an essential part of an overall organization culture.*
>
> Paragraph 3.51: All organizations that have a role in physical protection should make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management's commitment to provide guidelines to the staff and to set out the organization's security objectives. All personnel should be aware of and regularly educated about physical protection. *These organizations should also undertake regular self-assessments of nuclear security culture.*

Other possible additions could focus on the importance of cybersecurity in the modern world as part of a nuclear security culture and highlight the links between new and emerging technologies and nuclear security culture:

> (new) Paragraph 3.51: Nuclear security culture in the organization should include due attention to cybersecurity and account for novel challenges at the interface between nuclear security culture and new and emerging technologies.

Moreover, given the growing consensus and data on the need for diverse perspectives to recognize a range of threats, additional language within these paragraphs should emphasize the concept of "bias minimization" as a critical component of security culture:[10]

> (new) *Nuclear security culture programs should seek to minimize structural bias and exclusion that can degrade threat recognition, reporting, decision quality, and insider threat defenses.*

Emerging Threats in the Design Basis Threat or Threat Assessments

In a new era of rapidly emerging and increasingly unpredictable threats posed by adversaries using emerging technologies, physical protection should be based on the state's current and ongoing evaluation of the threat. INFCIRC/225/Rev. 5 provides a good definition for a process of identifying threats that nuclear facilities should protect against (known as a design basis threat or DBT), but it does not highlight the importance of maintaining a continuous process of monitoring threats, communicating them to operators, and ensuring protection against them, which are essential for keeping physical protection systems up to date.

[10] Sneha Nair, *Converging Goals: Examining the Intersection Between Diversity, Equity, and Inclusion and Nuclear Security Implementation*, NTI Global Dialogue on Nuclear Security Priorities, Vienna, Austria, April 14–15, 2023, https://www.nti.org/wp-content/uploads/2023/07/GD-Paper_Converging-Goals-Examining-the-Intersection-Between-Diversity-Equity-and-Inclusion-and-Nuclear-Security-Implementation.pdf.

Threat evaluation should also address emerging threats, which are more relevant than ever. States should have processes for anticipating disruptive changes in the threat environment requiring innovative approaches. In recent years, these changes have included emerging technologies like cyber threats, uncrewed aerial systems, and additive manufacturing.

Recommendations

Paragraph 3.2 should be strengthened by emphasizing continuous analysis, communication, and monitoring:

> *The State's physical protection regime should include continuous analysis of threats and their implications for DBT and physical protection measures, timely communication of threat information to operators, and monitoring of operators' responses to changes in threat. The regime should be updated regularly to reflect changes in threats and advances in physical protection systems, including those due to new and emerging technologies…The DBT should include capabilities and tactics adversaries have demonstrated in the country or nearby regions.*

IAEA nuclear security Implementing Guides should emphasize that nuclear power plants and Category I nuclear materials should be protected against at least a baseline level of threat.

Related, IAEA nuclear security Implementing Guides should emphasize that nuclear power plants and Category I nuclear materials should be protected against at least a baseline level of threat, including:

- A well-placed insider.
- A modest group of well-trained, well-armed outsiders (operating as more than one team).
- Collaboration between insiders and outsiders.
- Evolving threats such as cyber and unmanned aerial vehicles.
- Plausible but not yet demonstrated capabilities and tactics.

Paragraph 3.39 should be amended to include: "…evaluate the implications of any changes in the threat assessment or DBT, *with particular attention to changes due to new and emerging technologies.*"

Paragraph 3.40 should be broadened to include:

> …against possible stand-off attacks *or those involving new and emerging technologies, digital and otherwise*, as specified in the State's threat assessment or DBT.

The revision should encourage the use of emerging technology for nuclear security implementation, adding references in the General sections of Chapters 4, 5, and 6 to highlight the importance of emerging technologies for security. For example, "*Operators should consider the use of emerging technologies to improve security systems and strengthen cybersecurity capabilities.*"

Adapting to rapidly evolving threats requires countries to learn from each other by sharing non-sensitive nuclear security information. Provisions on international cooperation (Articles 3.31–3.33) should recommend non-sensitive threat-related exchanges between states. Related, a brief reference to

the importance of encrypting communications and considering the implications of misinformation in emergency response could be helpful.

Information and Computer Security

Cybersecurity

In 2011, the importance of cybersecurity was growing rapidly, but today, digital systems are far more widespread throughout nuclear operations than they were 15 years ago. INFCIRC/225/Rev. 5 highlights protecting nuclear material accountancy and control against cyberattacks. The advent of sophisticated AI models and systems that can rapidly process open-source information and write computer code or text that could assist an attacker means that security of sensitive information and computer systems will only increase in importance in the coming decades.

Computer security should be integrated throughout the text as a cross-cutting element of physical protection, rather than treated in a stand-alone section. This reflects the reality that digital systems are embedded in nearly all aspects of modern life, including nuclear facilities and activities. Although creating a separate section might underscore its importance, it risks implying that computer security is optional or peripheral. In practice, given the pervasive use of digital systems in both business processes (sensitive information management) and operational technologies, such an interpretation would be counterproductive.

Recommendations

Given the growing importance of data security and information protection, the guidance under Fundamental Principle G: Legislative and Regulatory Framework (paragraphs 3.9–3.17) should explicitly call for the establishment of regulations and requirements addressing computer, data, and information security. Including such provisions would both reinforce the central role of information security within nuclear security frameworks and strengthen the authority of lower-level publications that provide more detailed recommendations and technical guidance. For example:

> Paragraph 3.10 (add at end): *These requirements should include those for the security of computer systems, networks, and data associated directly or indirectly with the physical protection of nuclear material in use, storage, and during transport, and for nuclear facilities, using a graded approach.*

In or directly after paragraph 3.28, which addresses security by design, it would be useful to note that computer security by design, taking a systems view across the entire facility, is needed, particularly given the trend toward increasing digitization in all parts of nuclear facilities. For example:

> Paragraph 3.28 (add at end): *Further, cybersecurity should be taken into account when designing the facility, using a systems approach and including any networked devices and other digital systems planned for use in the facility.*

In paragraph 3.42, which addresses managing risk, computer and data security measures should be explicitly called out. For example:

> Risk can be managed by: (new bullet) *Improving the effectiveness of computer and data security. Ensuring that malicious actors are unable to access or manipulate computer systems used in nuclear facilities and that confidential data, including digital data, remains confidential, will increase the difficulty of organizing an effective attack on material or a facility.*

Explicit references to digital and computer-based data and information security should be included in paragraphs that address confidentiality. This would create clear linkages to more detailed guidance in lower-level publications. Security-relevant information extends beyond sensitive security procedures to encompass a wide range of data critical to facility operations, including information collected through electronic means (e.g., Internet of Things devices) and data stored remotely (e.g., in the cloud).

At the outset of the recommended requirements, or in another early section of the document, the growing reliance on automation and digital systems in nuclear facilities and related activities should be explicitly recognized. This recognition should emphasize the importance of securing both the systems themselves and the data they generate, process, and store. Although paragraphs 4.10 and 5.19 address computer-based systems, their scope is too narrowly focused on physical protection, nuclear safety, and nuclear material accountancy and control. This does not reflect the full range of digital applications now embedded in both operational technologies and business processes. Accordingly, the current text could be replaced with language such as:

> Paragraph 4.10 (alt) and 5.19: *Digitized systems used in facilities as well as those accessing sensitive digital data related to nuclear facilities should be protected against compromise (e.g., cyberattack, manipulation or falsification), consistent with the design basis threat.*

The examples provided illustrate only a few of the many opportunities to emphasize how cybersecurity has become an indispensable element of nuclear security. A comprehensive revision could go further by carefully reviewing the text in Chapters 4, 5, and 6 to ensure that additional references to cybersecurity are incorporated wherever appropriate.

New and Emerging Technologies That Could Be Used to Strengthen Nuclear Security Systems

INFCIRC/225/Rev. 5 should account for the growing production, transport, and use of high-assay low-enriched uranium (HALEU). As HALEU becomes more common in a range of forms, especially for advanced reactors, updated guidance on the appropriate level of security—particularly for its transport and for insider threat mitigation at locations where it is present—will be essential. DBTs should also be revisited to reflect the specific risks HALEU presents for theft or sabotage.

Recommendations

The document should clearly define HALEU and provide guidance for how its protection would differ from other types of nuclear material within Chapters 4, 5, and 6.

To support clearer material categorization and proportionate protection requirements for HALEU, the IAEA should consider establishing a Coordinated Research Project (CRP) involving regulators, technical support organizations, and operators to conduct scenario-based analyses of theft, diversion, and sabotage risks across different enrichment ranges, material forms, and quantities. The CRP should assess material attractiveness and potential consequences across the HALEU fuel cycle, including fabrication, storage, and transport, and identify facility- and activity-specific vulnerabilities that may warrant differentiated protection objectives.

Findings from the CRP should be used to inform revisions to INFCIRC/225/Rev. 5, including guidance on material categorization, graded application of protection measures, and DBT considerations in Chapters 4, 5, and 6, as well as the development of supporting technical guidance and regulator-focused training and topical meetings to promote consistent national implementation.

Sustainability and Resilience of Nuclear Security Regimes

Continuous Improvement

A process of continuous improvement is indispensable to effective nuclear security. Because threats, vulnerabilities, and operating environments evolve over time, nuclear security systems must remain adaptive, ensuring that protective measures remain robust against emerging risks. Continuous improvement rests on three core elements:

1. The systematic collection and assessment of information on evolving threats, vulnerabilities, and operating experience.
2. Regular evaluation of the adequacy and effectiveness of physical protection systems.
3. Timely planning, implementation, and review of enhancements.

Importantly, this process does not conclude once a specific upgrade or corrective action is completed; rather, it represents an ongoing discipline essential to sustaining resilience over time.

Although INFCIRC/225/Rev. 5 and subsequent guidance documents reference sustainability programs and quality assurance, they do not explicitly identify continuous improvement as a foundational principle of nuclear security. Embedding continuous improvement more clearly in a future revision—alongside its inclusion as a core element of Nuclear Security Series No. 20, *Objective and Essential Elements of a State's Nuclear Security Regime*—would strengthen the guidance and better align it with contemporary risk management and safety and security management practices. Sustainability should be clearly defined not as a static end state, but as the capacity of states and operators to maintain effective nuclear security indefinitely, in the face of evolving threats, for as long as nuclear materials and facilities exist.

Recommendations

A revision of INFCIRC/225/Rev. 5 should recommend that states establish and maintain ongoing processes of continuous improvement as a fundamental principle of their nuclear security regimes. These processes should include:

- Systematic collection and analysis of information related to threats, vulnerabilities, and operating experience.
- Regular evaluation of the adequacy and effectiveness of physical protection systems.
- The planning, implementation, and review of enhancements to sustain performance over time.

Sustainability programs at both the national and operator levels should explicitly incorporate continuous improvement as a central objective, beginning at the earliest stages of regime development and reinforced continuously throughout the lifetime of nuclear materials and facilities.

Continuity of Operations

The COVID-19 pandemic underscored the importance of ensuring continuity of nuclear security operations during major, sustained disruptions. These experiences highlight the need for nuclear security regimes that are not only effective under normal conditions, but resilient under compound and prolonged crises, including pandemics and other beyond-DBT scenarios.[11] Revisions to INFCIRC/225/Rev. 5 should clearly reflect these lessons.

The COVID-19 pandemic underscored the importance of ensuring continuity of nuclear security operations during major, sustained disruptions.

Governments and operators should establish and maintain comprehensive continuity of operations and business continuity plans aimed at reducing security risks during such crises. These plans should address issues including the maintenance of off-site power and cooling; the continued effectiveness of backup and redundant systems; staffing shortages and workforce protection; the secure management of fresh and spent nuclear fuel, including the timely transfer of spent fuel to dry storage where feasible; and the resilience of supply chains critical to nuclear security. Planning should explicitly consider scenarios in which normal regulatory, inspection, training, and emergency response activities are disrupted for extended periods.

The pandemic also demonstrated the importance of adaptive regulatory and oversight approaches under exceptional circumstances. States should ensure that continuity planning encompasses mechanisms for maintaining effective regulatory oversight and coordination when in-person activities are constrained, including through the use of remote tools and alternative oversight arrangements, while preserving security effectiveness.

[11] For the IAEA's analysis on COVID-19, see International Atomic Energy Agency, *The IAEA and the COVID-19 Pandemic: GC(65)/INF/7, GC(65)/INF/8, GC(65)/INF/9*, (Vienna, IAEA, August 26, 2021), https://www.iaea.org/sites/default/files/gc/gc65-inf7-8-9_0.pdf.

Preparedness for extended national or regional crises would be further strengthened by the establishment or use of nuclear operations or security centers of excellence. Such centers could support joint training and preparedness exercises for operators, regulators, first responders, and policymakers focused on prolonged disruptions affecting nuclear facilities. At the regional level, they could also facilitate cross-border coordination and joint response planning, helping neighboring states practice information sharing and cooperative response under crisis conditions.

Finally, lessons learned from the pandemic underscore the value of institutionalizing effective information-sharing mechanisms and virtual tools—including remote training, exercises, peer exchanges, and advisory services—as complements to in-person activities, strengthening resilience without diminishing security standards.

Recommendations

Although formally capturing these objectives in a future revision of INFCIRC/225/Rev. 5 would provide useful strategic direction, many of these lessons could be incorporated through targeted textual refinements that emphasize sustainability, resilience, and continuity of operations.

For example, paragraph 3.56 could be revised as follows:

> The State should establish a sustainability program to ensure that its physical protection regime is sustainable and effective in the long term, as well as resilient, including in short-term and extended unplanned situations for which continuity of operations is needed. This includes ensuring the regime is sufficiently robust to withstand such situations, maintaining effective coordination and oversight, and committing the necessary resources to support both sustainability and resilience.

Peer Review

As an essential component of sustainability, peer reviews should be recommended in a revision of INFCIRC/225/Rev. 5. The IAEA's International Nuclear Security Advisory Service and the IPPAS, both offered at the request of Member States, are two of the best-known and most established peer review mechanisms. However, uptake has been limited—only one-third of countries with nuclear materials and/or nuclear facilities have requested an IPPAS mission in the past five years—indicating that this valuable tool remains underused.

Recommendations

Although INFCIRC/225/Rev. 5 includes a section on international cooperation and assistance, it does not reference the role of advisory missions. Given their proven value, advisory services should be explicitly recognized in the revision. For example, a new paragraph could be introduced as follows:

> Paragraph 3.31: *International advisory missions, such as those provided by the IAEA, can provide States with valuable feedback on potential improvements to their physical protection regimes.*

Quality Assurance

INFCIRC/225/Rev. 5 states that quality assurance is to provide confidence that specified requirements for all activities important to physical protection are satisfied. Confidence building is important because it strengthens trust in the effectiveness of a state's nuclear security regime, both domestically and internationally, and helps demonstrate that appropriate measures are in place to prevent theft, sabotage, or other malicious acts. The state should therefore promote transparency and accountability in its nuclear security regime to reinforce public trust and international confidence.

Appropriate measures could include:

- The publication of nuclear security regulations, relevant policies, and associated budgetary provisions.
- The inclusion of nuclear security performance assessments and judgments in the annual reports of regulators and licensees.
- The public review of significant nuclear security incidents and remedial actions, undertaken with due care to avoid disclosing sensitive or site-specific information.
- Internal or external peer reviews, which can also play an important role in identifying areas for improvement and reinforcing a culture of continuous enhancement.

All such measures should be pursued in a manner that balances openness with the obligation to protect sensitive information, ensuring that efforts to build confidence do not inadvertently increase the risks of theft or sabotage.

Recommendations

After Paragraph 3.52, a revision could include the following:

> *Appropriate measures to engender confidence in domestic and international stakeholders that specified requirements for all activities important to physical protection are satisfied could include the publication of nuclear security regulations, relevant policies, and associated budgetary provisions; the inclusion of nuclear security performance assessments and judgments in the annual reports of regulators and licensees; and the public review of significant nuclear security incidents and remedial actions, undertaken with due care to avoid disclosing sensitive or site-specific information.*

Performance Testing

As part of the broader processes of continuous improvement and quality assurance, evaluating how protection system capabilities respond to changing threats is essential. Performance testing is a critical element of this evaluation.

In INFCIRC/225/Rev. 5, performance testing is defined as "Testing of the physical protection measures and the physical protection system to determine whether or not they are implemented as designed; adequate for

the proposed natural, industrial and threat environments; and in compliance with established performance requirements." Although this definition acknowledges the role of threats, it largely reflects a compliance-based approach. It emphasizes conformity with design and performance requirements rather than assessing the actual state of the system and how the combined functions of detection, delay, and response determine overall system effectiveness.

Recommendations

A strengthened approach to performance testing would be practice-oriented rather than solely document-based. Effective programs should draw on information from daily system operation, maintenance testing, and limited-scope component tests, with force-on-force exercises serving as the ultimate check of performance in countries with weapons-usable material or facilities whose sabotage could result in major radioactive release. These exercises should employ "attempt-to-defeat" scenarios grounded in real threat information. Results from such evaluations should be systematically fed back into the system, with identified weaknesses addressed through temporary compensatory measures and long-term upgrades. To ensure objectivity, performance testing should be managed by an organizational unit independent of the one responsible for operating the security systems.

Paragraph 4.35 could be revised as follows:

> Evaluations, including performance testing, of the physical protection measures and of the physical protection system, including timely response of the guards and response forces should be conducted regularly to determine reliability and effectiveness against the threat. *Such evaluations should be practice-oriented and draw on information from daily system operation, maintenance activities, and limited-scope component testing. Force-on-force exercises employing attempt-to-defeat scenarios based on credible threat information should be used as a comprehensive means of assessing system performance.* These should be carried out with full cooperation between the operator and response forces. *To ensure objectivity, performance testing should be managed by an organizational unit independent of those responsible for operating the physical protection system.* Significant deficiencies *identified through such evaluations, together with any temporary compensatory measures and longer-term corrective actions taken to address them,* and action taken should be reported as stipulated by the competent authority. *The results of evaluations should be systematically fed back into the physical protection system to support continuous improvement.*

Demonstrable Competence

Dozens of governments have endorsed the principle that management and personnel with responsibility for nuclear security should be demonstrably competent.[12] Yet no such expectation is currently established by IAEA nuclear security recommendations. Although some national nuclear establishments offer professional certification and training, these programs are not universally required.

[12] International Atomic Energy Agency, *Communication Dated 1 December 2016 Received from the Permanent Mission of Canada Concerning Certified Training for Nuclear Security Management Joint Statement on Certified Training for Nuclear Security Management* (Vienna: IAEA, 2016), https://www.iaea.org/sites/default/files/publications/documents/infcircs/2016/infcirc901.pdf.

Recommendations

The revision of INFCIRC/225/Rev. 5 could help close this gap by recommending that such certification and training programs become a standard expectation for nuclear security professionals. Doing so would help ensure that managers and personnel have the necessary skills to meet their responsibilities, while also fostering a common language, shared experiences, and professional standards across the nuclear sector. This, in turn, would improve the overall professionalism of nuclear enterprises and facilitate the effective sharing of best practices internationally.

Paragraph 3.31 could be revised to include:

> The State should ensure that evaluations include exercises to test the physical protection system, including the training and *certified* readiness of guards and/or response forces.

Consolidation and Minimizing Stockpiles

Security measures can never eliminate all risks. Every location where weapons-usable nuclear materials are stored or handled introduces some level of added risk that such material could be stolen or diverted through mistakes, insider actions, or failures of security. Countries can achieve higher security at a lower cost by protecting fewer places. Despite its importance, this issue has not been addressed in any version of INFCIRC/225.

Since 2011, international consensus in support of consolidation and minimization has grown significantly. The IAEA General Conference has repeatedly endorsed HEU minimization, and the Agency has facilitated numerous efforts to repatriate HEU to its country of origin. A series of international meetings have reinforced these commitments, and more than 20 countries have now joined INFCIRC/912, pledging to minimize HEU.

Recommendations

Within Sustainability Program, paragraphs 3.56–3.57, a revised INFCIRC/225/Rev. 5 should explicitly recommend that states reduce both the number of sites and transports involving weapons-usable nuclear material, and the overall stockpiles of such material, to the minimum necessary to meet national requirements. Countries with HEU or separated plutonium should commit to regular reviews of each location where such materials are stored or used, assessing whether the benefits of maintaining the material at that site outweigh the risks. Where they do not, the material should be eliminated or removed and consolidated elsewhere.

Nearly all known thefts of HEU or separated plutonium have involved bulk material, most often in powder form. This highlights the particular risks at bulk processing facilities, where diversion may be more difficult to detect. Accordingly, the revision should recommend that states keep bulk processing of weapons-usable material, and the number of facilities where it takes place, to the minimum necessary, while applying the most stringent standards of security and material accountancy.

Siting

The siting of nuclear facilities has direct implications for nuclear security and should be considered at the earliest stages of planning and development. With the emergence of new, smaller reactor designs, facilities may be increasingly located in densely populated areas to provide local power or district heating. Conversely, some advanced reactor projects envision siting in remote or isolated areas, closer to resource needs or industrial use. Both scenarios present distinct security challenges.

For reactors in densely populated areas, the potential consequences of a successful sabotage or theft attempt could be magnified due to proximity to large civilian populations and critical infrastructure.

For reactors in densely populated areas, the potential consequences of a successful sabotage or theft attempt could be magnified due to proximity to large civilian populations and critical infrastructure. In such cases, security requirements should emphasize robust physical protection, rapid response capabilities, and effective coordination with local law enforcement and emergency services.

For reactors in remote locations, the challenge lies in the reduced availability of nearby response forces, limited infrastructure, and greater logistical hurdles in sustaining protective systems. These sites may require enhanced self-protection measures, resilient communication systems, and contingency planning for extended periods without external support.

Recommendations

Siting decisions should integrate nuclear security considerations alongside safety, environmental, and economic factors. States should conduct comprehensive risk assessments for both population-dense and remote siting options, ensuring that physical protection measures are adapted to the specific context. Guidance in INFCIRC/225/Rev. 5 should explicitly recognize these considerations and encourage states to incorporate siting-related risks into design basis threat evaluations and overall physical protection planning.

Paragraph 3.28 could be revised to include:

> For a new nuclear facility, the site selection and design *should include, as early as possible, comprehensive risk assessments taking into account how environmental factors are likely to impact physical protection systems* and also address the interface between physical protection, safety and nuclear material accountancy and control to avoid any conflicts and to ensure that all three elements support each other.

Paragraph 5.10 could be revised to include:

> When defining scenarios, the operator should consider the location, *with particular attention to population density and remote siting,* of the nuclear facility and all nuclear material and other radioactive material, including radioactive waste, especially those at the same location inside a nuclear facility.

Improving Accessibility and Usability of the Nuclear Security Series

To maximize the impact of revised recommendations, states must be able to easily locate, interpret, and apply relevant NSS documents. At present, understanding the structure of the NSS—including the hierarchy between Fundamentals, Recommendations, Implementing Guides, and Technical Guidance—requires navigating multiple webpages and document lists. This can make it difficult for practitioners, regulators, and policymakers to identify the appropriate guidance and understand how documents relate to one another.

Recommendations

The IAEA should consider developing a user-friendly, centralized online platform for the Nuclear Security Series that:

- Provides a clear explanation of the hierarchy and purpose of each NSS category.
- Includes an interactive roadmap showing linkages between recommendations and Implementing Guides.
- Organizes documents by thematic area (e.g., insider threats, transport, cybersecurity).
- Highlights revisions or superseded editions.
- Offers search and filtering tools to support practitioners in identifying the most relevant documents.

Such a platform would significantly strengthen the accessibility, transparency, and practical utility of the NSS for Member States—particularly those with limited technical or regulatory capacity—and would facilitate more consistent implementation and training across the international community.

Conclusion

The revision of INFCIRC/225/Rev. 5 represents a critical opportunity for the international community to reaffirm its commitment to strong and adaptive nuclear security. By strengthening guidance on insider threats, embedding robust approaches to security culture, addressing emerging and evolving threats, integrating cybersecurity and data protection throughout, and promoting sustainability, resilience, and professional competence, Member States can ensure that the updated recommendations remain effective for decades to come.

Adopting these measures will not only align the recommendations with current realities but also help create a forward-looking framework that anticipates future challenges. A stronger, more comprehensive INFCIRC/225/Rev. 5 will reinforce international confidence in nuclear security systems, encourage continuous improvement, and support cooperation across borders and sectors. Ultimately, revising this foundational guidance is an investment in peaceful nuclear technology, reducing risks to nuclear materials and facilities worldwide and strengthening the collective ability to prevent catastrophic nuclear incidents.

About the Nuclear Threat Initiative

The Nuclear Threat Initiative (NTI) is a nonprofit, nonpartisan global security organization focused on reducing nuclear, biological, and emerging technology threats imperiling humanity.

1776 Eye Street, NW | Suite 1000 | Washington, DC 20006 | **www.nti.org**

facebook.com/nti.org @NTI_WMD NTI_WMD Nuclear Threat Initiative