IAEA Nuclear Security Recommendations (INFCIRC/225): The Next Generation

Matthew Bunn, Harvard University
Laura Holgate, Nuclear Threat Initiative
Dmitry Kovchegin, Independent Consultant
Nickolas Roth, Stimson Center
William H. Tobey, Harvard University

Abstract

In 2011, the International Atomic Energy Agency (IAEA) released the fifth revision of its Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225).[1] This update of IAEA nuclear security guidance was a significant improvement upon its predecessors, suggesting new and strengthened approaches to nuclear security in a range of areas. For the first time, it recommended protecting digital systems used for physical protection, nuclear safety, and nuclear material accountancy and control against cyber-attack; protecting against insider threats; prioritizing security culture within organizations involved in implementing physical protection; conducting regular force-on-force exercises as part of performance testing; and establishing programs to ensure that physical protection regimes are sustained over time. These recommendations represented a significant evolution in the international consensus on nuclear security.

Nearly a decade later, however, the global nuclear security landscape has changed. Nuclear security regulations and practices have improved. International institutions and norms supporting global nuclear security architecture are stronger. Countries have made new political commitments to strengthening their nuclear security. Legally binding agreements are more widely subscribed than they were before. Meanwhile, new global threats have surfaced, presenting new challenges to physical protection systems. A range of emerging technologies creates new opportunities, but also new risks.

In light of these evolving conditions, and to benchmark against security improvements in the non-nuclear realm, the IAEA nuclear security recommendations published nearly a decade ago should be updated. This paper will review changes in the nuclear security environment—including evaluations of consensus around physical protection practices, international agreements, and threats—since INFCIRC/225/Rev. 5 was published. It will then make recommendations for how to build upon existing IAEA nuclear security recommendations in a sixth revision of INFCIRC/225.

Introduction

The International Atomic Energy Agency's (IAEA) 2011 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225) revision five, improved significantly upon its predecessors. For the first time, the IAEA recommended protecting digital systems; protecting against insider threats; prioritizing nuclear security culture; conducting regular force-on-force exercises; and ensuring the sustainability of physical protection systems. Although many at the time recognized that this document did not go far enough, these recommendations represented a significant evolution in the international consensus on nuclear security.

Nearly a decade later, however, the global nuclear security landscape has changed. Nuclear security regulations and practices have improved. International institutions and norms supporting global nuclear security architecture are stronger. Countries have made new political commitments to strengthen their nuclear security. Legally binding agreements are more widely subscribed to. Meanwhile, new global threats have surfaced, presenting new challenges to physical protection systems. Emerging technologies create new tools, but also potential risks. Not only is there a need to update INFCIRC/225 to the evolving environment, but the need to address issues omitted in the fifth revision is increasingly compelling.

This paper reviews changes in the nuclear security environment—including evaluations of consensus around physical protection practices, international agreements, and threats—since INFCIRC/225/Rev. 5 was published. It then makes recommendations for revising INFCIRC/225.

Evolving Nuclear Security Consensus

International consensus surrounding nuclear security implementation has advanced considerably over the past decade. International summits, institutions, multilateral agreements, NGO initiatives, and national actions have significantly improved nuclear security regulations, implementation, and international architecture since the last revision of INFCIRC/225 was published.

The most significant factor in the recent evolution of nuclear security was the nuclear security summits. From 2010 through 2016, dozens of world leaders met at four summits focusing on strengthening nuclear security around the globe. Each of these summits produced consensus communiques recognizing that nuclear terrorism is one of the "most challenging threats to international security" and that nuclear security is the most effective means to prevent terrorists and criminals from acquiring nuclear materials. The summits also encouraged national, bilateral, and multilateral commitments to nuclear security action through "house gifts" and "gift baskets," which were later published as IAEA Information Circulars (INFCIRCs). These commitments covered many issues, including strengthening nuclear security implementation, certified training for nuclear security management, mitigating insider threats, enhancing transport security of nuclear materials, and minimizing and eliminating the use of civilian highly enriched uranium(HEU).

Some of these commitments advanced ideas mentioned in INFCIRC/225 Rev. 5, but many were never addressed. For example, the Mitigating Insider Threats Gift Basket, which was endorsed by 27 countries and is now INFCIRC/908, commits countries to develop and implement programs to mitigate insider risk. While Rev. 5 mentions protecting against insiders, it does not call for comprehensive programs to reduce the threat. Another area where there is a growing consensus beyond Rev. 5 recommendations is minimizing and eliminating the use of civilian HEU. This gift basket, now published as INFCIRC/912, commits more than 20 countries to refrain from using HEU in new civilian facilities and to convert or shut down all HEU civilian reactors as soon as it is economically and technically possible.[2] Several of the nations backing this commitment eliminated their HEU stocks over the past decade. There is nothing in Rev. 5 about minimizing or eliminating HEU or steps to achieving it.

Perhaps the most multilateral commitment from the summit process was Strengthening Nuclear Security Implementation Initiative, opened to all as INFCIRC/869. The more than 30 states participating in INFCIRC/869 commit to "meet the intent" of the IAEA's nuclear security recommendations on physical protection of nuclear material and facilities. They also commit to going beyond those recommendations by hosting periodic peer reviews of their nuclear security arrangements and ensuring that "management and personnel with accountability for nuclear security are demonstrably competent."[3]

The nuclear security summits also advanced norms on nuclear security information sharing. At each summit, countries would submit reports describing the progress they had made in strengthening their nuclear security systems. Additionally, at the last nuclear security summit, dozens of countries endorsed the Statement of Principles of the Nuclear Security Contact Group, now published as INFCIRC/899, which included a commitment to promoting and assessing implementation of nuclear security commitments made during the summit process.[4] As of 2020, 48 countries and four international institutions are part of that Contact Group, including five countries that were not summit participants.[5]

Another area where there was steady progress in international nuclear security consensus was peer review. Since Rev. 5 was published, through 2019, the IAEA organized 40 International Physical Protection Advisory Service (IPPAS) peer review missions—almost half of the 85 IPPAS missions conducted since they first began in 1996.

The IAEA has also advanced nuclear security through its supporting Implementing Guides and Technical Guidance Documents. For example, since 2011, the IAEA has published implementing guides on developing a Design Basis Threat; mitigating insider threats; and computer security at nuclear facilities. These were all ideas introduced in Rev. 5. IAEA ministerial events in 2016 and 2020 also advanced the international nuclear security consensus. Both events included declarations endorsed by dozens of countries and the 2020 declaration endorsed several key nuclear security concepts mentioned in this paper.[6]

NGO and industry-level initiatives have also made critical contributions to advancing nuclear security. The World Institute for Nuclear Security (WINS), for example, supports good practice exchanges, develops guidance on good practices in an array of areas of nuclear security, and established an online nuclear security training academy for education and certification. According to its 2018 annual report, 82 percent of those who participate in WINS activities say they have changed their security practices as a consequence.[7] The Nuclear Threat Initiative's biennial Nuclear Security Index tracks nations' progress on nuclear security and suggests ways countries can further improve. Moreover, non-governmental reports, legislative investigations, organized dialogues, and other activities, can inspire new ideas, educate policymakers, and encourage action.[8]

Partially as a result of all of the work by international organizations, groups, and NGOs, there are numerous examples where states have made remarkable progress in strengthening nuclear security.[9]

Nuclear Security Incidents

One of the strongest motivators for strengthened nuclear security stems from actual incidents.[10] Since 2011, there have been numerous major nuclear and non-nuclear security incidents, as well as terrorist attacks, that have either forced new thinking or reinforced the need for new guidance regarding nuclear security.

Numerous incidents at nuclear and non-nuclear facilities also provide important lessons for nuclear security.[11] [12] The 2012 break-in at the Y-12 HEU facility in Oak Ridge, Tennessee by an 82-year-old nun and two other protesters in their 60s revealed stunning failures in security culture. Worse, in 2017, Nevada National Security Site guard Jessica Glover suffered months of sexual harassment, sexual assault during a training exercise, and reprisal for reporting the abuse. Such behavior evinced a failed security culture. Protective forces cannot possibly have the requisite trust in each other to defeat dangerous threats when one group of the team is attacking other members of the team. This is the single most serious breakdown in nuclear security culture that has ever been publicly reported, and yet there is no public evidence that effective measures have been implemented to rectify it.[13]

There have also been major developments in terrorist threats over this period. Months after INFCIRC 225/Rev. 5 was published, for example, the terrorist Anders Breivik killed 77 people in Norway. Authorities found his 1,500-page manifesto, about 30 pages of which are devoted to carrying out acts of radiological and nuclear terrorism. In 2016, terrorists were caught spying on the highest ranking official of Belgium's principal nuclear research facility. At the same time, insider incidents in a range of industries have occurred in many countries since 2011, highlighting the threat; for the nuclear industry, perhaps the most notable events were the insider sabotage of the Doel-4 nuclear power plant in Belgium in 2014 (still unsolved), and the discovery in the course of the investigation that long before, two individuals with cleared access to vital areas of the plant had departed to fight for terrorists in Syria.[14] In response to the incident, Belgium significantly strengthened its protections against insider threats, requiring more cameras and more widespread implementation of two-person and three-person rules.[15] Perhaps the most significant terrorist threat since 2011 was the rapid rise of the Islamic State. In only a few months, right after the 2014 Nuclear Security Summit, the Islamic State had amassed more resources, controlled more territory and people, and had greater recruitment ability than any terrorist organization in history.

There have also been several nuclear security incidents in recent years highlighting the rapid evolution of nuclear security threats. For example, in September 2019, Kudankulam Nuclear Power Plant was the victim of a cyber-attack on "mission-critical targets." Unmanned aerial systems have also been a growing concern causing the commander of U.S. Strategic Command, Gen. John Hyten, to tell Congress in 2017 that recent incidents of unauthorized drones overflying both Navy and Air Force nuclear facilities "represent a growing threat to the safety and security of nuclear weapons and personnel."[16]

These incidents demonstrate the evolving threat nuclear operators face and the need to update international guidance to defeat it.

Recommendations

In light of evolving norms around nuclear security, as well as rapidly changing threats facing nuclear operators, several important updates should be included within a new revision of INFCIRC 225. Many of these recommendations fit within the Nuclear Security Fundamentals included in INFCIRC/225/Rev. 5, but some go well beyond. Some of the recommendations below provide more detail than what INFCIRC/225 has included in the past. These details are often included in implementation guides rather than INFCIRC/225. The authors of this paper believe, however, that these recommendations are important enough to rise to the level of this document.

Peer Review. Fundamental Principle A (Responsibility of the State) recommends regular review and updating of national security regimes, and Fundamental Principle J (Quality Assurance) notes the importance of programs that provide confidence in the effectiveness of security provisions.[17] Peer reviews can contribute to both fundamental principles. Moreover, over 30 states, including most of the states with nuclear power plants, highly enriched uranium, or plutonium, are participating in the Strengthening Nuclear Security Implementation initiative (open to all states as INFCIRC/869), in which they commit to "periodically" host peer reviews of their physical protection arrangements. Hence, peer reviews should be recommended in a revision of INFCIRC/225. The IAEA's International Nuclear Security Advisory Service and the IPPAS, provided upon request of member states, are two of the best known and regularized peer review approaches. These services involve on-site reviews by trained international experts of national legislation and regulations as well as implementation at the site level, compared against the relevant IAEA guidance, including INFCIRC/225. Hosts of such reviews gain valuable knowledge of areas for improvement and good practices gleaned from similar facilities. These reviews also contribute to the IAEA's collection of good practices to be shared with other member states through its secure NUSEC portal. Only one-third of countries with nuclear materials and/or nuclear facilities have requested an IAEA IPPAS mission in the last five years, indicating that this valuable tool is underutilized.

Other peer reviews can also contribute to state responsibility and quality assurance. Some countries with trusted relationships could exchange regular bilateral peer reviews of each other's regulations and facilities, perhaps identifying areas where bilateral or other assistance could be provided to improve security performance. Reflecting Nuclear Suppliers Group guidance that adequate security be a condition of supply of nuclear materials, the United States carries out on-site security reviews in connection with exports of nuclear material, which adds to the understanding that recipients of such material are equipped to secure it appropriately. Other exporters could follow this model. In countries with multiple nuclear sites, peer reviews could also be carried out between sites. Such exchanges promulgate best practices and allow for inadequate regulations or capabilities to be remedied before incidents occur. To have greatest effect, peer reviews should occur regularly to confirm that improvements identified in prior reviews are effectively incorporated.

Confidence Building. The increasing acceptance of the value of confidence building reflects the recognition that the behavior of one state regarding its nuclear materials can impact its own citizens, its neighbors, and even countries and populations far away. Lax security in one country can allow for theft of materials, sabotage of facilities, or the detonation of an improvised nuclear device with both local and global effects on economies and health. The 2019 IAEA Nuclear Security Resolution also took note of the benefits of good security for enhancing public confidence in peaceful nuclear applications. High-quality security provisions at the national level that can be discerned by others are therefore essential to building confidence. Such steps could include publication of nuclear security regulations and associated budgets, inclusion of nuclear security judgments in the annual reports of regulators and licensees, public review of nuclear security incidents and any remedial provisions, and internal or external peer reviews, with due care taken, of course, to avoid release of site-specific information that could increase risks of theft or sabotage.

Peer reviews also contribute to confidence building in nuclear security. The fact that a country has undergone a peer review indicates that they are taking nuclear security seriously and seeking out advice. Confidence is much greater when the results of such reviews are published, even partially, along with the plans for improving any shortcomings, but only five countries (Australia, Canada, Japan, Norway, and Sweden) have published all or part of the results of recent IPPAS missions.

Continuous Improvement. A process of continuous improvement is essential for effective nuclear security and is a core element of INFCIRC/869. To minimize risk, nuclear security systems must constantly adapt to changing threats. The foundation of this continuous improvement process is ongoing collection of information about changing threats, evaluation of the system capabilities to defend against them, and planning and implementing improvements necessary to ensure a nuclear security system is capable of addressing the threat. This process does not stop with implementation of a specific improvement – no matter how substantial or advanced. Still, continuous improvement as a fundamental principle for nuclear security is absent from IAEA Nuclear Security Series documents. Capturing continuous improvement as an essential element in the next revision of INFCIRC/225 would greatly strengthen the guidance.

Fundamental Principles F (Security Culture), J (Quality Assurance), and L (Confidentiality) are all focused on "Sustaining the Physical Protection Regime." Sustainability programs facilitate practical implementation of the continuous improvement process at the state level and at specific nuclear sites. INFCIRC/225/Rev. 5 first introduces the concept of sustainability into physical protection activity. In particular, it recommends that "The State should establish a sustainability programme to ensure that its physical protection regime is sustained and effective in the long term by committing the necessary resources".[18] It further recommends that "Operators, shippers and carriers should establish sustainability programmes for their physical protection system" and lists elements of sustainability programme. To elaborate on this recommendation IAEA issued an implementing guide "Sustaining a Nuclear Security Regime" (IAEA NSS No. 30-G).[19] This guide provides member states with valuable recommendations regarding the elements of sustainability programs at both the national level and the level of specific operator. Still, neither INFCIRC/225 nor NSS 30-G clearly defines sustainability program goals. INFCIRC/225 tautologically notes that a state's sustainability programs should ensure "that its physical protection regime is sustained and effective in the longer term". Nuclear Security Fundamentals document NSS-20 "Objective and Essential Elements of a State's Nuclear Security Regime," issued in 2014 and intended to serve as an overarching document for the IAEA Nuclear Security Series, also focuses on specific elements of sustainability programme rather than its fundamental goal.

The sustainability of a nuclear security regime should be established in INFCIRC/225 as one of a nuclear security regime's essential elements. The goal of a sustainability program should be defined as ensuring that states and operators are capable of ensuring security of nuclear facilities and materials over an indefinite period of time under changing threat environments as long as they have nuclear facilities and materials. Sustainability planning should start as early as possible, ideally with the nuclear security regime and nuclear energy program.

Protecting Against the Full Range of Threats. Fundamental Principle G states that "physical protection should be based on the State's current evaluation of the threat." Continuous monitoring of threats, their proper communication to operators, and reflection in protection systems are key to continuous improvement. Article 3.39 of INFCIRC/225/Rev.5 provides a reasonably strong definition of a design basis threat process, but it does not highlight the critical importance of having a continuous process of monitoring threats, communicating them to operators, and protecting against those threats. In particular, article 3.2 recommends that "The State's physical protection regime should be reviewed and updated regularly to reflect changes in the threat".[20] This principle should be revised to "The State's physical protection regime should include continuous analysis of threats and the changing threats implications for design basis threat and appropriate physical protection measures, timely communication of threat information to operators and monitoring of operators response to changes in threat". Further, the threat evaluation process needs to address emerging threats. In addition to analyzing and making "quantitative" changes, such as changes in potential intruder

strength, weaponry, and motivations, threat evaluation needs to include disruptive "qualitative" changes in the threat requiring innovative approaches to address them. Such disruptive changes now include cyber threats, unmanned aerial systems, or additive manufacturing. Tomorrow will bring new challenges.

Also, provisions related to international cooperation (Articles 3.31-3.33) should recommend the exchange of non-sensitive threat-related information between member states.

Providing protection against the full spectrum of capabilities and tactics that adversaries might employ is fundamental to an effective physical protection system. A revised INFCIRC/225 should recommend that states include in their DBTs or threat assessments the full set of capabilities and tactics adversaries have demonstrated in that country or nearby countries in its region, as well as plausible but not yet demonstrated capabilities and tactics. Moreover, a new revision of INFCIRC/225 should recommend that all countries protect nuclear power plants and Category I nuclear materials against at least a baseline level of threat. In an age of globalized threats, where all nuclear materials and facilities are potential targets of theft or sabotage, no country is so safe that it does not need to protect against a well-placed insider; a modest group of well-trained and well-armed outsiders, capable of operating as more than one team; and both an insider and the outsiders working together. The revision should also recommend that countries require protection against evolving threats such as cyber and unmanned aerial vehicles.

Insider Threats. Since 2011, there has been a substantial increase in international attention to the insider threat, widely acknowledged to be the most dangerous threat to nuclear materials and facilities.[21] While the IAEA's guide to preventing and protecting against insider threats was published in 2008, three years before INFCIRC/Rev. 5 was completed and published, the insider protection guide has come into much wider use since then.[22] Similarly, the first edition of the WINS best practice guide to managing internal threats was published in March 2010, but has come into much wider use since 2011.[23] A global meeting on protecting nuclear materials and facilities from insider threats in Belgium in 2019, pledged in INFCIRC/908, drew representatives from dozens of countries.

INFCIRC/225/Rev. 5 mentions the insider threat in several places, but provides no comprehensive treatment of the topic. More specific recommendations on implementing effective programs to protect against insider threats would be among the most important elements of a new revision. As noted in the IAEA's guide to preventing and protecting against insider threats, and in INFCIRC/908, effective protection against insider threats requires a comprehensive approach that is "integrated," "graded," and "risk-informed." INFCIRC/908 refers specifically to a range of measures, including, among others: (a) the need for both national-level and facility- or agency-level programs; (b) measures to "rigorously assess continually monitor human reliability"; (c) measures to "deter insiders from theft/diversion" (and, in the broader context of INFIRC/225, sabotage as well); (d) limit insiders' access to sensitive materials or locations; € measures to "provide prompt detection of theft/diversion," including strong nuclear material control and accountability (MC&A) measures; (f) regulatory approaches that encourage operators to take a "holistic" approach to protecting against insider threats; (g) training programs on mitigating insider risks; and (h) "programs to conduct performance tests, self-assessments, and peer reviews to enhance effectiveness of insider threat mitigation programs." [6] Incorporating elements such as these in a new revision of INFCIRC/225 would provide states with much stronger guidance on steps they should take to address insiderthreats.

In particular, INFIRC/225/Rev.5 recommends that states limit unescorted access to protected areas to individuals "whose trustworthiness has been determined," but it offers no guidance on how to make such a determination – and the need for ongoing monitoring after initial access has been granted.

Performance Testing. Fundamental Principle J emphasizes the importance of quality assurance programs to ensure that physical protection requirements are satisfied. Related to the continuous improvement process is evaluating how protection system capabilities respond to changing threats. Performance testing is one of the most critical components of such an evaluation. Coverage of performance testing in Rev. 5, however, is weak. The current definition describes performance testing 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". While it mentions protecting against the threat, this definition mostly follows a compliance-based, not a performance-based approach. It measures compliance against design and performance requirements, rather than evaluating the actual state of the system and how detection, delay, and response characteristics impact the system effectiveness. An appropriate performance testing program needs to:

- Be based on practice rather than documents ("design" and "performance requirements"). This means that an evaluation needs to be based on information obtained through daily system operation, maintenance testing, limited scope tests of the system components, and force-on-force exercises as an ultimate check of system performance.
- Employ limited-scope tests and force-on-force exercises using "attempt to defeat" scenarios based on actual threat information.
- Feed back into the system data obtained through the effectiveness evaluation process. If performance testing reveals weaknesses, these weaknesses should be addressed through temporary compensatory measures and upgrades providing long term fixes.
- Be managed by the site organization independent from the organization managing security systems.

Demonstrable Competence. INFCIRCs 869 and 901 record commitments by dozens of states at the 2016 Nuclear Security Summit to "ensuring that management and personnel with accountability for nuclear security are demonstrably competent."[24] No one would visit a lawyer, dentist, or accountant who had not been through a rigorous course of training *and examination* to manifest their mastery of their chosen field. Yet no such expectation is now created by IAEA recommendations. Such courses are offered by some national nuclear establishments and by the World Institute for Nuclear Security. They should be *de rigueur* for nuclear professionals, and such certification should be recommended by the IAEA. Not only would this ensure that nuclear managers have the necessary skills to do their jobs, it would also create a common language and set of shared experiences to improve the professionalism of nuclear enterprises and facilitate the sharing of best practices.

Security Culture. Another area of significant improvement since 2011 is nuclear security culture. Fundamental Principle F focuses on security culture. INFCIRC 225/Rev. 5 emphasizes important elements of security culture, including recognition that a threat exists, the importance of collaboration between governments, organizations, managers, and individuals to maintain security culture, the importance of promoting and encouraging security culture, and the importance of regularly updating all personnel about physical protection. As already noted, this is a critical element of sustaining strong nuclear security. 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 it does not elaborate on how.

States have made important progress in strengthening nuclear security culture since 2011. For example, Japanese regulations now require operators to have programs to strengthen security culture within their organizations. In January 2015, Japan's Nuclear Regulation Authority developed a "Code of Conduct on Nuclear Security Culture" for NRA staff. It emphasized, among other things, threat awareness, senior management commitment, education, and self-improvement. As one initiative, NRA commissioners themselves tour facilities with senior plant executives to discuss opportunities for strengthening security culture. The NRA has also distributed self-assessment questionnaires to all operators, who then develop their own self-evaluation procedures.[25]

A revision of INFCIRC/225 could recommend establishing a comprehensive security-culture program that engages the whole enterprise; developing effective motivation techniques; and addressing

complacency among senior managers. Moreover, given the 2019 incident at the Nevada National Security Site, the revision should also emphasize the importance of diversity, equity, and inclusion as a critical component of security culture. Additionally, since INFCIRC 225/Rev. 5 was published, the IAEA has published technical guidance on how to conduct nuclear security culture self-assessments.[26] WINS also provides culture self-assessment tools. Self-assessment should be recommended in a new revision.

Categorization. Fundamental Principle H emphasizes a graded approach to nuclear security that takes into account the "relative attractiveness" and "nature of the nuclear material." The treatment of how much operators should rely on modest radiation barriers to reduce the need for physical protection was an important step forward in INFCIRC/225/Rev. 5. The fifth revision did not alter the categorization table that also appears in the physical protection convention, which indicates material's categorization can be reduced one step if it is emitting a radiation field equal to or greater than one Gray per hour (Gy/hr) at one meter. But the fifth revision does suggest "if the *threat assessment* or *design basis threat* includes an adversary who is willing to perform a *malicious act*" – which surely almost any threat assessment or design basis threat would – then states should "carefully consider" reducing the categorization levels only if the radiation level is so high as to "incapacitate the adversary before the *malicious act* is completed."[27] Any revision should maintain this advice, and, if anything, make it stronger – perhaps rather than "carefully consider," it should affirmatively recommend that in most cases states should not reduce the categorization level unless the radiation level would be incapacitating in the time required to carry out the acts of concern.

Since 2011, there has been considerable international discussion of modifying material categorization based on chemical and other properties as well, as the U.S. Department of Energy does. No clear international consensus has developed, however. In general, it makes sense to have more stringent physical protection measures for material that is easier to process into forms that could be used in a bomb. Less stringent security measures for material in forms that would be difficult to turn into a bomb also give operators incentives to convert material into such forms whenever practicable, to save money on security. But it is important not to go too far. Given that chemically removing the plutonium from unirradiated plutonium-uranium mixed oxide (MOX) fuel is far simpler than enriching low-enriched uranium (LEU) to produce HEU, future revisions should reject ideas proposed by some in the United States, that MOX should require no more security than LEU, or that security plans could rely on simply detecting that a theft was occurring rather than stopping it, and relying on local law enforcement to recover the material.[28]

Consolidation and Minimizing Stockpiles. Security measures never reduce risk to zero. Every location with materials that could be used to make a nuclear bomb if they fell into hostile hands represents some level of added risk that material could be stolen or diverted as a result of a mistake or failure of security. Hence, efforts to consolidate stocks of weapons-usable nuclear material to the smallest practical number of locations, and to minimize the stocks themselves, should be a major part of an effective nuclear security program. But these topics are not mentioned at all in INFIRC/225, in any of its revisions.

The international consensus supporting consolidation and minimization of stocks has grown substantially since 2011. IAEA General Conference statements now actively support HEU minimization, and the IAEA has supported a range of efforts to ship HEU back to its country of origin. The communiqué of the 2014 nuclear security summit emphasized that all stocks of HEU and separated plutonium must be "appropriately secured, consolidated, and accounted for," and urged states both to consolidate stocks and to keep stocks of HEU and separated plutonium to "the minimum level" consistent with national requirements.[29] A series of international meetings have supported HEU minimization efforts, and over 20 countries have joined in a commitment to HEU minimization, now open to all as INFCIRC/912.[30]

A new revision of INFCIRC/225 should address this issue, recommending that states should reduce the number of locations and transports handling weapons-usable nuclear material, and the stocks of such material, to the minimum consistent with national requirements. In particular, countries with

HEU or separated plutonium should commit to regular reviews of each location where such materials exist to confirm that the benefits of having that material at that location continue to outweigh the costs and risks; if not, the material should be removed and consolidated at another location.

Nearly all the known thefts of HEU or separated plutonium have been of bulk material, generally in the form of powder. This suggests that bulk processing facilities, where material might be removed without detection, pose the greatest risks of theft and diversion. A new revision of INFCIRC/225 should recommend that states keep the scale of bulk processing of weapons-usable material and the number of locations where this occurs to the minimum consistent with national requirements, and maintain stringent standards of security and accounting for all such operations.

Conclusion

The preceding recommendations should not be viewed as a menu of items but as a cohesive group of mutually reinforcing measures that will strengthen physical protection systems. For example, peer review facilitates continuous improvement, and a healthy security culture and demonstrable competence are synergistic. Taken together, along with the rapidly evolving norms and threats, they indicate a strong need for a sixth revision of INFCIRC/225.

ENDNOTES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA, Vienna (2011), https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Communication dated 30 January 2017 received from the Permanent Mission of Norway concerning a Joint Statement on Minimising and Eliminating the Use of Highly Enriched Uranium in Civilian Applications, IAEA, Vienna (2017), https://www.iaea.org/sites/default/files/publications/documents/infcircs/2017/infcirc912.pdf.
[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Communication received from the Netherlands Concerning the Strengthening of Nuclear Security Implementation, IAEA, Vienna (2014), https://www.iaea.org/sites/default/files/publications/documents/infcircs/infcirc869.pdf.
[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Communication dated 24 October 2016 received from the Permanent Mission of Canada concerning the Statement of Principles of the Nuclear Security Contact Group, IAEA, Vienna (2016), https://www.iaea.org/sites/default/files/publications/documents/infcircs/2016/infcirc899.pdf.
[5] See NUCLEAR SECURITY CONTACT GROUP, "Nuclear Security Contact Group Members", http://www.nscontactgroup.org/members.php.
[6] NEAKRASE, S., "ICONS 2020: The Good, the Bad, and the Ugly ... Actually, Mostly Good," *Atomic Pulse*, March 5, 2020, https://www.nti.org/analysis/atomic-pulse/icons-2020-good-bad-and-ugly-actually-mostly-good/.
[7] WORLD INSTITUTE FOR NUCLEAR SECURITY, *Annual Report: Reaching the Tipping Point*, WINS, Vienna (2018), https://wins.org/document/annual-report-2018/.
[8] For example, see RAJAGOPALAN, R.P., et al., *Nuclear Security in India*, Observer Research Foundation, New Delhi (2016), https://www.orfonline.org/wp-content/uploads/2016/10/ORF_Monograph_Nuclear_Security.pdf.
[9] For more, see BUNN, M., et al., Revitalizing Nuclear Security in an Era of Uncertainty (Cambridge, Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, January 2019) and NUCLEAR THREAT INITIATIVE AND ECONOMIST INTELLIGENCE UNIT, *NTI Nuclear Security Index: Theft/Sabotage: Building a Framework for Assurance, Accountability, and Action, 4th Edition*, NTI, Washington, D.C. (2018), https://ntiindex.org/wp-content/uploads/2018/08/NTI_2018-Index_FINAL.pdf.
[10] One study published earlier in the decade identified foreign nuclear security incidents as a key driver of nuclear security improvements. See BUNN, M. AND HARRELL, E., *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey*, Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, Massachusetts (March 2014), https://www.belfercenter.org/sites/default/files/files/publication/surveypaperfulltext.pdf.
[11] For a summary, see BUNN, M., et al., Revitalizing Nuclear Security in an Era of Uncertainty, pp. 52-53, https://www.belfercenter.org/sites/default/files/2019-03/RevitalizingNuclearSecurity_Mar19.pdf.

[12] BUNN, M., et al., *Revitalizing Nuclear Security in an Era of Uncertainty*, pp. 27-28.
[13] BENNER, K., "A Nuclear Site Guard Accused Colleagues of Sexual Assault. Then She Was Fired," *New York Times*, January 25, 2019, https://www.nytimes.com/2019/01/25/us/politics/department-of-energy-sexual-assault.html.
[14] BUNN, M., et al*., Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?*, P. 29.
[15] SAYLES, R., "Belgian Regulator Sets New Security Steps After Suspected Sabotage," Inside NRC, December 29, 2014, from LexisNexis Academic database.
[16] MEHTA, A., "STRATCOM Issues Guidance for Anti-Drone Measures Near Nuclear Sites," *C4ISRNet*, April 4, 2017, https://www.c4isrnet.com/digital-show-dailies/space-symposium/2017/04/05/stratcom-issues-guidance-for-anti-drone-measures-near-nuclear-sites/.
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5), https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf, P. 5.
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*, IAEA, Vienna, P. 17.
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, *Sustaining a Nuclear Security Regime*, IAEA, Vienna (2018), https://www-pub.iaea.org/MTCD/Publications/PDF/P1763_web.pdf.
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5), https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf, P. 5.
[21] BUNN, M. and SAGAN, S.D., eds. Insider Threats, Cornell University Press, Ithaca, N.Y. (2017).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA, IAEA, Vienna (2008), https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1359_web.pdf.
[23] WORLD INSTITUTE FOR NUCLEAR SECURITY, WINS International Best Practice Guide 3.4: Managing Internal Threats, WINS, Vienna (2015).
[24] 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, IAEA, Vienna (2016), https://www.iaea.org/sites/default/files/publications/documents/infcircs/2016/infcirc901.pdf.
[25] Nobuaki Eguchi, "Efforts to Enhance Nuclear Security Culture in Japan, presentation to the Second International Regulators Conference on Nuclear Security, Madrid, Spain, May 11-13, 2016, and Satoru Tanaka, "A Nuclear Security Regime in Japan: Enhancement Efforts and Global Contributions," presentation to the IAEA International Conference on Nuclear Security: Commitments and Actions, Vienna, December 5-9, 2016.
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Self-assessment of Nuclear Security Culture in Facilities and Activities, IAEA Vienna (2017), https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf.
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf, P. 21.
[28] For a critique of one such U.S. proposal, see BUNN, M., Comment on Proposed Rule on Enhanced Security at Nuclear Fuel Cycle Facilities; Special Nuclear Material Transportation; Docket NRC-2014-0118. Nuclear Regulatory Commission, Rockville, Md. (2014).
[29] "Nuclear Security Summit Communiqué," Ministry of Foreign Affairs, the Netherlands, The Hague (2014).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Communication dated 30 January 2017 received from the Permanent Mission of Norway concerning a Joint Statement on Minimising and Eliminating the Use of Highly Enriched Uranium in Civilian Applications.