

INCENTIVES FOR NUCLEAR SECURITY

Matthew Bunn

Harvard University

BCSIA, 79 JFK Street, Cambridge MA02138

matthew_bunn@harvard.edu

ABSTRACT

Effective systems and procedures to ensure security for nuclear warheads and weapons-usable nuclear materials are expensive and often inconvenient. Hence, strong incentives exist to cut corners on nuclear security – for states and ministries to provide fewer resources than needed, for facilities to invest what resources they have in activities directed toward generating revenue or fulfilling their principal missions, and for individuals not to follow burdensome security procedures. This paper outlines approaches under which U.S. policy and policies by other key governments could provide incentives to put in place effective nuclear security, at the state or ministry level, at the facility level, and at the individual level. Effective regulatory approaches, decisions not to provide lucrative U.S. government contracts to foreign facilities that have not demonstrated strong nuclear security, and steps to ensure that actions related to nuclear security are appropriately included in individual performance reviews and facility-level performance fees are among the kinds of incentives that could be considered. Ultimately, maintaining effective nuclear security should be part of the “price of admission” for doing business in the international nuclear marketplace. Without such incentives, current programs to cooperate in improving nuclear security worldwide may not succeed in putting in place nuclear security systems and procedures that provide genuinely effective security and will be sustained for the long haul.

INTRODUCTION

Effective nuclear security is expensive and often inconvenient. Every dollar that a facility manager spends on protection is a dollar *not* spent on revenue-generating production (“safeguards don’t make kilowatts,” as the saying goes). Every hour that an employee spends following security procedures is an hour *not* spent on activities more likely to lead to a promotion or a pay raise. For a state, every budget allocation for nuclear security is an allocation *not* made for other urgent priorities.

In short, the incentives to cut corners on nuclear security are strong. Most individuals and organizations tend to do what they have incentives to do. Hence, unless strong counter-incentives to maintain effective security and accounting for nuclear stockpiles can be put in place, the goal of ensuring that all nuclear weapons and weapons-usable nuclear materials worldwide are secure enough to defeat the threats that terrorists and criminals have shown they can pose is not likely to be achieved.¹ To date, programs such as the nuclear material protection, control, and accounting (MPC&A) program have provided equipment and training that have increased recipients’ *ability* to provide effective security, but have been less successful in arranging incentives that would give them the *motivation* to do so. The problem of incentives is among the most critical policy issues currently facing nuclear security efforts. It is a key issue in Russia, but it is also a key issue in the United States and everywhere else that nuclear stockpiles and facilities – or other particularly hazardous materials and facilities – have to be secured.

INCENTIVES AT THE INDIVIDUAL AND TEAM LEVEL

A common business saying is that performance equals ability times motivation. Even once appropriate training has been provided to make employees *able* to take the actions necessary to achieve effective security and accounting for nuclear stockpiles, it is crucial to motivate them to *want* to do so. Providing incentives for good security performance is difficult, because judging who is doing well and who is doing badly on security is not easy to do; as the saying goes, “you can’t reward what you can’t measure.” But measures of security performance do not have to be perfect to send the message that management takes

security seriously and expects employees to do the same. Simple approaches can do. One director of a U.S. lab, for example, made it a practice to ensure that whenever there was a security violation, there were consequences for the team responsible and all of those above them (including the director); and, when a team had gone for an extended period with no security violations, to reward them.² A variety of approaches might be pursued to strengthen security incentives at the individual and team level.

The “good citizen” incentive. Most people, if they understand that doing their job appropriately is critical to the security of their nation and the world, will do their best to do a good job. (Indeed, one in-depth study of factors affecting the probability that employees will violate rules concluded that employees are very unlikely to violate rules they think are important, even if the probability of being caught is very low.³) Hence, in-depth training on the dangers of nuclear theft and nuclear terrorism is an essential part of creating incentives for individuals and teams to take security seriously. Unfortunately, today such training is too often either not provided or of low quality. For example, the security manager at Seversk (among the largest plutonium and highly enriched uranium processing facilities on earth) recently reported that the guards guarding his facility are poorly trained, do not understand the importance of particular security procedures, and do not “recognize that security and perhaps not only his life, but the lives of his close ones – no matter how far they live from his place of service – depends on his actions or inaction.”⁴

Realistic performance tests – in which teams portraying outside attackers attempt to break into the facility, or people portraying insider adversaries attempt to remove material or sabotage the facility – can help remind employees of realistic threats to their facilities, and what steps are needed to defeat them, countering the complacency about security that is common at many facilities. Briefings on the seriousness of the threat – including documented terrorist interest in acquiring stolen nuclear weapons and materials and in sabotaging nuclear facilities – can also be a key element of a program to convince employees to make security a priority. As one part of training programs to rectify this problem, the Department of Energy should seek to work with Rosatom to produce a video highlighting the dangers of nuclear theft and terrorism – including footage from events such as Hiroshima, Chernobyl, and Beslan, to highlight the threat in clear and stark terms. In a Russian context, the power of such a video would be greatly increased if President Putin agreed to introduce it, emphasizing that he expected every one involved in securing these stockpiles to give their utmost, in the interest of Russia’s security. Such a video could then be adapted for use in other countries (including the United States), splicing in similar high-level statements from their leaders.

Reviewing and rewarding security performance. Facilities should seek to develop at least rudimentary measures of employee and team security performance, so that good performance can be rewarded as a regular element of performance reviews. (There is general agreement in the management literature that rewards are more effective than punishments in shaping employee behavior⁵ – and as discussed below, punishing modest errors and violations may make it impossible to convince employees to provide the data to management that is crucial to fixing the underlying conditions that cause them.) Management must send the message that security performance is a key element of what is expected from employees – and making security a part of performance reviews that feed into promotions and raises is an important part of making that message credible.

Rewarding reporting. Because major security incidents are extremely rare, tracking security progress or backsliding in between major inspections or performance tests requires mechanisms for identifying and analyzing modest incidents and near-misses – as in the case of safety. This in return requires convincing employees to report these events, in enough detail to be useful. Encouraging employees to report on all security-related issues and problems not only identifies issues to be addressed, but helps convince employees of the importance management attaches to continuously monitoring and improving security performance.

Convincing people to report incidents in which they or their colleagues made mistakes or broke the rules is not easy. But experience demonstrates that with the right approach, a culture of reporting can be forged within an organization.⁶ Doing so requires convincing employees that they and their colleagues will not be punished when such incidents are reported honestly (except in cases of egregious recklessness or intentional malfeasance), and that there may be consequences if such incidents are not reported. For example, in the U.S. nuclear navy, each commander of a nuclear vessel must file a report every month that

details every problem with the ship's nuclear system that arose, and how that problem was addressed; in the early days, if a commander reported no problems, nuclear navy founder Admiral Hyman Rickover would personally show up and demand to know what was going on.⁷ Regular operational reviews go over the ship's logs in detail, and there are serious consequences if reportable incidents were not reported.

The essential point is that in nearly all cases of near-misses, it is more important for management to hear about and understand the incidents and their underlying causes, so that they can be fixed, than it is to blame and punish particular individuals. In the safety area, some organizations, far from punishing those involved in near-misses, actively reward reporting of near-misses.⁸

Making good security easy. If it is easy to commit security violations, and inconvenient and time-consuming not to, employees will violate security rules. Hence, it is crucial to set up the basic structure of the work environment to make good security as easy as possible and to make it as inconvenient as possible to do anything that would seriously undermine security.⁹ Examples include “inherently sustainable” security upgrades such as the heavy concrete blocks placed on top of the plutonium canisters at Mayak and in front of the bunker doors at Pantex; DOE’s decision to move to a diskless environment for secure computing, rather than relying on all employees not to take classified disks out of secure areas; access control systems that require two individuals to swipe their cards and type in their codes at the same time at separate locations to open a security door, thereby making it very difficult *not* to abide by the “two-man rule”; and simple expedients such as making sure that nuclear material areas have no more entry and exit points that have to be guarded and monitored than they need to have.

“Security watchdog” awards. Ultimately, what governments should hope for from individuals and teams involved in guarding and managing nuclear stockpiles is not just compliance with security rules, but proactive efforts to improve security. Toward that end, it would be highly desirable to establish a program of significant awards for “security watchdogs” – individuals or teams who identify significant security weaknesses and propose feasible fixes for them.

INCENTIVES AT THE FACILITY LEVEL

Similar incentives apply at the level of an entire facility. In particular, facility managers want to be good citizens, too: if they are convinced that there is a serious threat of theft or sabotage at their facility, they are far more likely to make security one of their top priorities. Hence, realistic performance tests and threat briefings for senior management are important at the facility level as well. Some facility managers may also want their facility to be seen as a leader in security, and this could provide some incentive for security investments as well.

But ultimately, security is not the primary mission of a nuclear facility, and managers need to balance their allocation of scarce resources between security and other priorities. Most managers will not make major and costly investments in security unless they have to – which then highlights the importance of effective regulation.

Security regulation. Effective regulation of MPC&A is absolutely essential to a strong nuclear security and accounting system that will last for the long haul. Regulatory agencies need to put in place rules that require facilities with nuclear weapons or weapons-usable nuclear material (or those who transport these commodities), along with facilities or transports whose sabotage could result in a major catastrophe, to provide security able to defeat the insider and outsider threats that terrorists and criminals have demonstrated they can pose in that country (or that intelligence agencies judge to be realistic). They need to put in place systems of inspections and realistic tests to assess whether these rules are being adequately followed. And they need to put in place effective compliance programs to convince facilities to comply – with the power and willingness, in the worst case, to impose substantial fines or shut-downs if facilities prove unable or unwilling to provide adequate security. For this purpose, governments need to give the regulatory agencies not only the resources and expertise to do their jobs, but a substantial measure of power, independence, and high-level support when needed – and governments need to closely monitor the performance of the regulatory agencies themselves in addressing these security threats. In Russia, MPC&A regulation appears to have notably improved in recent years, with both more effective inspections and compliance programs by

Rostekhnadzor (the successor agency to Gosatomnadzor), and the recent advent of a program of in-depth Rosatom inspections of both physical protection and material accounting at Rosatom facilities – a major step, given Rosatom’s greater power to bring inspection resources to bear and to force its facilities to comply.¹⁰ But in Russia as in other countries, there is more to do to ensure that nuclear security regulation is effective.

In regulation, too, it is important to be constantly aware of where the incentives point. A security inspector, for example, who spends a large fraction of his time at one facility, becomes friendly with that facility’s management, and is hoping to convince the facility to give him a higher-paying job after his tour with the inspection agency, will have strong incentives to overlook problems that the facility’s management does not want to spend the money to fix. More broadly, a regulatory agency under political pressure not to interfere unduly with the nuclear industry, whose personnel primarily come from the industry and expect to return to it later in their careers, and whose personnel rely almost wholly on information and perspectives provided by the industry, can be expected in most cases not to impose rules that the industry believes are excessively costly or unwarranted – even if the rules are justified from a broader societal perspective.

It is also important that the rules be clear, their purpose understandable, and designed so that compliance with them will in fact lead to security sufficient to meet the threat. In general, this is likely to require regulatory systems that are primarily performance-based, rather than rule-based. Otherwise, one can often have the problem of “goal displacement” – facilities focusing on building a fence high enough to meet the rule, not a fence good enough to provide the needed level of security. To date, in many countries, nuclear security rules are far from models of clarity, and are more often primarily rule-based rather than performance-based. This is in part because of the inherent difficulty of regulating performance in protecting against events that virtually never occur – a problem that again emphasizes the importance, as one element of an overall regulatory system, of realistic tests of the performance of security measures at particular sites in defeating specified outsider and insider threats. The U.S. MPC&A program should reinvigorate its efforts to work with both Rostekhnadzor and Rosatom to put in place a regulatory system for nuclear security and accounting that continually comes closer to meeting these standards – and should step up efforts to strengthen the regulatory ability of the Ministry of Defense (MoD) group charged with regulating security and accounting for MoD’s materials, and providing independent regulation of those areas of Rosatom facilities involved in nuclear weapons and their components.

Industry self-help and self-regulation. After the accidents at Three Mile Island and Chernobyl, the nuclear industry realized that a major accident at the facility with the weakest safety program could have devastating effects on the entire industry, and that the industry therefore had a strong self-interest in putting in place measures that would bring the laggards up to the level of the best-performing facilities – to encourage facilities to shoot for excellence in safety, not just compliance with the minimum rules imposed by government regulators. Hence, the industry established the U.S. Institute of Nuclear Power Operations (INPO), and ultimately the global World Association of Nuclear Operators (WANO), whose missions are to share best practices, to provide industry-based inspections, peer reviews, and advice, and generally to help ensure that safety practices industry-wide are continually improved.¹¹ While these organizations do not have the power to fine or shut down facilities, they exert substantial peer pressure – few facilities want to be identified as safety laggards, and leave safety problems pointed out in such an industry review uncorrected.

Today, the nuclear industry has a similar self-interest in ensuring that all facilities provide adequate security. A terrorist sabotage that caused a Chernobyl-scale accident, or a theft of plutonium or highly enriched uranium (HEU) that led to a terrorist nuclear attack would be a gigantic disaster for the nuclear industry worldwide – almost certainly dooming prospects for substantial future growth of nuclear energy, and possibly leading to political calls for the shut-down of existing plants. Hence, the time is ripe for an industry initiative to establish a comparable organization – the “World Association for Nuclear Security” – to exchange best practices and conduct voluntary peer reviews of nuclear security. Doing so will be more difficult than in the case of safety, because of the secrecy surrounding security issues at individual facilities – but there is much that can be done without contradicting the legitimate demands of confidentiality.¹²

Security performance in management reviews. Another key element of providing incentives at the facility level is reviewing and rewarding good security performance in reviews of the management of a facility. In the United States, for example, the Department of Energy’s major facilities are managed by

contractors who receive award fees if they manage the facilities well, as judged by certain criteria. Compliance with security rules is already a contract requirement, and is among the criteria used in determining these awards – but it would be worthwhile to attempt to develop measures for assessing overall security performance that could be used to reward facilities for good, and improving, security. A wide range of related approaches could be found to encourage managers of facilities in different countries to make security performance a priority. The security manager for a major European nuclear firm, for example, reports that he has authorization from the board of directors to include security factors in the measures used to determine managers' bonuses, but has not yet managed to develop measures of security performance that are sufficiently accurate and quantifiable for that purpose. One measure that was considered and rejected was the absence of regulatory citations for violations of security rules at that facility (rejected because regulators, knowing that the manager's bonus would be affected if they did not give the facility a clean bill of health, might use that knowledge to toughen their demands). This firm, however, does maintain a set of security indicators for each of its facilities, which are rated either green, yellow, or red; the firm requires managers to take action to fix red indicators immediately. Moreover, having red indicators at their facility makes managers look bad at regular senior management reviews, motivating them to get those issues addressed promptly, and to address yellow indicators before they can become red.¹³ The MPC&A program should seek to negotiate contracts with facilities receiving MPC&A assistance that include contract rewards and penalties for good or bad performance in sustaining effective MPC&A; given the difficulty of assessing performance, the burden should be on facilities to demonstrate good performance in reviews and tests.

Contract preferences for sites with good security. If facilities needed to have good security and accounting measures in place to get lucrative contracts, their managers would be strongly motivated to invest in MPC&A. Today, however, few such incentives are in place. Under current U.S. policy, for example, a Russian nuclear facility will be sanctioned, and denied U.S. contracts, for cooperating with Iran on technologies related to HEU and plutonium – but if it maintains such poor security that Iranian agents could readily arrange to steal HEU or plutonium, it can still have all the contracts it wants. This should be changed. Establishing a preference in all U.S. contracts (not just those supporting the MPC&A program) for facilities that have positively demonstrated effective security performance in realistic tests would create a strong incentive for facilities to invest in MPC&A, and to participate in realistic tests of their performance. The United States should work with other leading nuclear states to convince them (and their state-owned firms) to establish similar preferences for sites with good security. Ultimately, effective nuclear security should become a fundamental “price of admission” for doing business in the international nuclear market.

A nuclear security matching fund. It would be highly desirable to create an international nuclear security matching fund, which would match funding from individual facilities when those facilities made a compelling case that a particular proposed project would substantially improve security. Such a fund would encourage facilities to identify projects that would improve security at their sites, and, by covering a substantial part of their cost and bringing in additional revenue that can help employ security experts at the sites, could substantially reduce facilities disincentive to invest in nuclear security.¹⁴

“Security leader” awards. As with individuals and teams, the standard governments should encourage facilities to pursue is not just compliance with security rules but excellence in security performance. Toward that end, it would be desirable to establish a system of awards (including significant bonuses for the managers of facilities and possibly for all security-related personnel) for facilities that were “security leaders,” demonstrating superior performance in nuclear security. Again, the burden should be on the facilities to demonstrate their superior performance, as judged by a panel of security experts, or reflecting (at least in part) the results achieved in realistic performance tests of facility security systems. In the United States, for example, there is an annual competition among protective forces at nuclear facilities, with an award to the force that gets the best cumulative score on tests during the competition. In Russia, in 2002 the Ministry of Atomic Energy (now Rosatom) launched a competition among its facilities for the highest-performing facility, judged by 17 criteria (none of which related to security). The employees of the winning facility each year split \$100,000 in bonuses.¹⁵ The United States should work with Russia to establish a parallel program to provide comparable bonuses to facilities that demonstrate superior nuclear security performance. This should not necessarily be limited to one facility per year, or facilities that expect that they

could do well but not be the first-place finisher might be discouraged from competing; if several facilities demonstrate performance worthy of reward, sufficient funds should be made available to reward them all.

INCENTIVES AT THE STATE OR MINISTRY LEVEL

National governments and ministries are large, complex organizations driven by a variety of competing political and bureaucratic imperatives, not unitary rational actors maximizing their utility. Nonetheless, incentives are an important element of convincing governments and ministries to accept new nuclear security agreements, make investments in nuclear security, put in place more effective nuclear security regulations, and the like.

Addressing a perceived security threat. Perhaps the most important reason for governments or ministries to take action to upgrade nuclear security is the equivalent of the “good citizen” incentive discussed above – a genuine belief among senior officials that there is a serious threat of nuclear theft or sabotage in their country, and that strengthened security measures are necessary to protect the country’s national security against that threat. Unfortunately, today the nuclear elites in Russia and many other countries around the world (including many in the United States) are convinced that the threat of nuclear theft and terrorism is overblown, and that existing security measures are adequate (or even excessive). Convincing governments that the threat to their own countries is real, and that action is urgently necessary to address it, is absolutely critical to a successful global effort to lock down nuclear stockpiles worldwide. Toward that end, the United States should (a) work with the leadership of key countries to convince them to put together teams of their own experts to do fast-paced assessments of security at all of their nuclear facilities, to find and propose fixes for vulnerabilities to specified outsider or insider threats; (b) work with nuclear technical experts in key countries to prepare joint briefings on the threats of nuclear theft and terrorism for senior leaders; and (c) help organize war games or similar exercises simulating nuclear theft or sabotage scenarios for senior leaders.¹⁶

Complying with agreements. Governments in general do seek to comply with their international obligations. Unfortunately, today there are few agreements that require governments to provide really effective security for nuclear stockpiles. There is a convention on physical protection, but even once the amendment now being approved goes into force for individual countries, it offers only general principles, not enforceable standards that countries must meet. It says, for example, that parties to the treaty should have rules concerning nuclear security that facilities are required to obey, but it does not indicate what those rules should say. The new nuclear terrorism convention – which has not yet entered into force – has no provisions requiring countries to provide high levels of security for their nuclear stockpiles or facilities. Many countries have entered into agreements with nuclear supplier states that include physical protection obligations – but often the obligation is only to “take into account” IAEA recommendations on physical protection.

The most important new development in this area is the unanimous passage of UN Security Council Resolution 1540, which creates a new, binding legal obligation on all 191 UN member states to provide “appropriate effective” security and accounting for any nuclear stockpiles they may have.¹⁷ If the words “appropriate effective” mean anything, they ought to mean that security measures must be put in place that can effectively defeat the threats that terrorists and criminals in that country have shown they can pose. There is now an urgent opportunity for the United States and other countries to work together to lay out what the essential elements of an “appropriate effective” nuclear security and accounting system are, and to help – and pressure – countries around the world to put those essential elements in place.¹⁸

Meeting “world standards”. Many countries want to be seen as meeting world standards in their management of nuclear technology, even if they are not required to do so; hence, international recommendations in a variety of areas (including physical protection) carry substantial influence. Many countries also do not consider themselves as particularly expert in physical protection, and therefore give considerable weight to the recommendations of authoritative international bodies such as the International Atomic Energy Agency (IAEA); some countries, for example, draw their domestic physical protection regulations largely from the IAEA’s physical protection recommendations, INFCIRC/225. But the INFCIRC/225 recommendations as they stand, while far more detailed than the physical protection

convention, still have major weaknesses: they are more rule-based than performance-based (suggesting, for example, that nuclear material be in a locked vault, but not how hard that vault should be to open), and do not require that facilities with potential nuclear bomb materials have armed guards. For this reason, with the amendment to the physical protection convention now largely completed, it would be worthwhile to prepare a revision to INFCIRC/225 (which has not been revised since 1999), redesigning them so that compliance with them would mean putting in place a genuinely effective security system, and including more significant provisions on protection against sabotage as well as theft.

There is also more that the IAEA can and should do to collect data on what different countries' national approaches to physical protection are, what their domestic legislation and regulations say, and whether they are generally in compliance with the physical protection convention and generally following INFCIRC/225 recommendations. Even the knowledge that such a report was being prepared might well motivate some countries to take additional steps, to avoid being publicly identified as laggards, failing to take nuclear safety and security measures that most other countries with comparable facilities had already taken.

Cooperating on a critical U.S. agenda. For better or for worse, today the United States is the world's only superpower, and many countries find it in their interest to cooperate in areas that the United States makes clear it considers very important to U.S. and world security. Given that President Bush has identified the danger that terrorists would get and use nuclear weapons as the single greatest danger to U.S. national security, security for nuclear warheads and their essential ingredients is a subject that should be at the top of the U.S. diplomatic agenda – an item to be addressed with every country with stockpiles to secure or resources to help, at every level, at every opportunity, until the job is done. Experience in related areas makes clear that a U.S. message that good relations depend on action can have the desired effect: China, for example, has established export control laws and a still evolving but much improved approach to enforcing them under persistent U.S. pressure over the years.

Creating commercial incentives. One important incentive for states to take necessary nuclear security measures is the fear that their firms will be denied access to lucrative nuclear markets or key technologies and supplies if they do not. (The Chinese desire for a peaceful nuclear cooperation agreement with the United States, for example, was a key element in convincing the Chinese government to take action on export controls.) For decades, the members of the Nuclear Suppliers Group (NSG) have required that recipients of key nuclear exports adequate physical protection for them. But the NSG physical protection requirements are extremely brief and vague – it would be easy to meet those requirements without having a secure system. Similarly, the U.S. requirements for physical protection of U.S.-origin materials essentially require states to take IAEA recommendations into account, not that security measures be put in place that can effectively defeat particular threats. It would be highly desirable to upgrade both the U.S. and NSG physical protection requirements. Again, ultimately effective security measures for dangerous nuclear stockpiles should be part of the price of admission to the international nuclear market.

Avoiding embarrassment. Oversight generally leads to improved government performance, and helps prevent backsliding. Most ministry heads are strongly motivated not to be confronted over security problems by the president of their country, or asked to testify on security weaknesses before a committee of their legislature, or be featured in the press as a facility with bad security. Avoiding embarrassment is itself a strong incentive – it is the flip side, in some respects, of the “good citizen” incentive. Strengthening this incentive requires putting in place oversight measures that increase the probability that embarrassing situations would be found and revealed – including spot inspections of nuclear facilities by groups with significant independence; engaged and informed legislatures willing to investigate and press for action; well-informed non-government organizations interested in monitoring progress in nuclear security; and an active and challenging press corps focused on this topic. Most of these means of oversight, however, are problematic in the area of nuclear security, which is often shrouded in secrecy; in many countries, there is precious little oversight of nuclear security matters beyond the facilities and the responsible government agencies themselves, until a major incident of some kind occurs. Nevertheless, in the United States in particular, investigations by Congress and exposés in the press and by non-government organizations have been crucial factors leading to major upgrades in security over the years.¹⁹ The United States and other

nations interested in promoting nuclear security should seek to build up an independent press, engaged legislatures, and informed non-government organizations focused on nuclear security.

INCENTIVES FOR NUCLEAR REMOVAL

For many sites around the world, the best answer is not to upgrade security for the nuclear stockpiles where they now are, but to remove them.²⁰ Many civilian research reactors, for example, could readily convert from HEU fuel to low-enriched uranium (LEU) that cannot support an explosive nuclear chain reaction. Many others are no longer needed, and should be convinced to shut down.

But facility managers often have strong incentives to keep their facility running, and to keep whatever weapons-useable nuclear materials they have. In Russia, for example, people who work at facilities with dangerous materials such as plutonium or HEU reportedly receive higher pay and benefits in return. Hence, convincing facilities to give up their nuclear material is likely to require offering substantial packages of incentives, targeted to the needs of each facility. Indeed, this is the overwhelming message from past successful removals of HEU from vulnerable sites: each case was unique, and required a different set of incentives to convince the facility and the country to allow the HEU to be removed. Some of these incentives related directly to the nuclear facility itself, such as the Nuclear Threat Initiative's help with managing the remaining nuclear waste on-site that proved to be crucial to getting a deal with Yugoslavia to remove the HEU from Vinca in 2002, but others were almost entirely unrelated, such as the broader threat reduction assistance provided to Kazakhstan as part of the arrangements for Project Sapphire, or the relief from sanctions provided to Libya as part of its agreement to abandon its weapons of mass destruction programs and allow the fresh, unirradiated HEU at its nuclear research institute to be removed.²¹

As a result, it is important, as the new Global Threat Reduction Initiative (GTRI) moves forward, to be creative and flexible in offering packages of incentives for countries and facilities to give up their nuclear material. This could range include help with converting to LEU or with shutting and decommissioning a reactor, contracts for other research by the scientists at a site after agreement is reached to shut the site's reactor, help with managing the wastes from a research reactor, and other steps, many of which will not even be thought of until a particular case arises.²² It appears that additional incentives are also likely to be needed to convince facilities to return even that portion of the U.S.-supplied HEU abroad that is covered by the current U.S. take-back offer.²³

In legislation sponsored by Senator Pete Domenici (R-NM) and Senator Dianne Feinstein (D-CA) in 2004, Congress took an essential step in the right direction, authorizing the provision of an enumerated list of incentives to convince facilities to give up their HEU; this year, Congress should consider broader language authorizing the secretary of energy to take such actions as may be necessary to implement GTRI effectively.

At the same time, as is the case with nuclear security more broadly, the issue of removals of weapons-useable nuclear material from vulnerable sites requires sustained high-level attention. If the United States is now to succeed in drastically increasing the pace of HEU removals around the world, it is likely to be necessary to put this issue on the agenda for senior officials, as one critical element of the global effort to keep nuclear bomb material out of terrorist hands and therefore a high priority for U.S. diplomacy.

REFERENCES

¹ For a classic discussion of how incentives pointing in the wrong direction prevent organizations from accomplishing their goals, see Steven Kerr, "On the Folly of Rewarding A, While Hoping for B," *Academy of Management Executive* 9, no. 1 (1995). For an earlier discussion of the crucial importance of incentives for nuclear security, see Oleg Bukharin, Matthew Bunn, and Kenneth N. Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union* (Washington, D.C.: Russian American Nuclear Security Advisory Council, 2000; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/mpca2000.pdf as of 10 March 2005), pp. 27-44.

² Glenn Schweitzer, remarks to "Third Russian International Conference on Nuclear Material Protection, Control, and Accounting," 16-20 May 2005, Obninsk, Russia.

³ The probability of violation was judged to be only 3% when employees assessed the situation as "compliance important, usually legally required, but probability of detection [of violation] low to moderate". Chances of that employees would violate a rule were far higher if the rule was considered unimportant or there was a personal benefit in violating it, even if the chances of being caught

were substantial. See James Reason, *Managing the Risks of Organizational Accidents* (Aldershot, UK: Ashgate Publishers, Ltd., 1997), p. 145.

⁴ Igor Goloskokov, "Refomirovanie Voisk MVD Po Okhrane Yadernikh Obektor Rossi (Reforming MVD Troops to Guard Russian Nuclear Facilities)," trans. Foreign Broadcast Information Service, *Yaderny Kontrol* 9, no. 4 (2003).

⁵ See, for example, Leslie Wilk Braksick, *Unlock Behavior, Unleash Profits: How Your Leadership Behavior Can Unlock Profitability in Your Organization* (New York, NY: McGraw-Hill, 2000).

⁶ See Reason, *Managing the Risks of Organizational Accidents*, pp. 195-213.

⁷ Interviews with former nuclear navy personnel.

⁸ This applies at some hospitals, for example, in cases that did not lead to a bad outcome for a patient but could have. Steven Kerr, personal communication, June 2005.

⁹ A huge fraction of safety problems in industry are attributable to work environments that make safe conduct harder for the employee than risky conduct. See discussion in Reason, *Managing the Risks of Organizational Accidents*. Much the same is likely to be the case for security.

¹⁰ In 2004, for example, Rosatom teams carried out physical protection inspections at eight facilities (including several large defense complex facilities), with teams of roughly 10 individuals spending up to two weeks inspecting a particular facility. Weaknesses requiring correction were found at all the facilities, and at two facilities, the problems were so extensive that a reinspection at a comparable scale was required to ensure that the necessary corrections had been made. This effort was summarized by Alexander V. Izmailov, Eleron, in remarks to the "Third Russian International Conference on Nuclear Material Protection, Control, and Accounting," 16-20 May 2005, Obninsk, Russia.

¹¹ For an insightful discussion, see Joseph V. Rees, *Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island* (Chicago: University of Chicago, 1996).

¹² For further discussion, see Charles Curtis, these proceedings.

¹³ Interview, July 2003.

¹⁴ This approach was suggested by my colleague Anthony Wier.

¹⁵ Igor Khripunov and James Holmes, eds., *Nuclear Security Culture: The Case of Russia* (Athens, Georgia: Center for International Trade and Security, The University of Georgia, Date 2004; available at <http://www.uga.edu/cits/documents/pdf/Security%20Culture%20Report%2020041118.pdf> as of 18 February 2005), pp. 55-56.

¹⁶ For a more extensive discussion of these ideas as they relate to building the sense of urgency in Russia in particular, see Matthew Bunn and Anthony Wier, *Securing the Bomb 2005: The New Global Imperatives* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/report_cnwmupdate2005.pdf as of 6 July 2005), pp. 96-97.

¹⁷ The full text of the resolution, reports that countries have filed on their progress in implementing it, and other information is available at the website of the committee established to oversee implementation. United Nations, "1540 Committee" (New York: UN, 2005; available at <http://disarmament2.un.org/Committee1540/meeting.html> as of 25 February 2005).

¹⁸ See discussion in Matthew Bunn, "Unsc 1540: Next Steps to Seize the Opportunity" in *A New Role for the United Nations Security Council: Criminalizing WMD Proliferation: the Impact of U.N. Security Council Resolution 1540* (Arlington, Va.: Institute for Nuclear Materials Management, 2005; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/UNSC1540.pdf as of 9 July 2005); Bunn and Wier, *Securing the Bomb 2005*, pp. 108-09.

¹⁹ For an example of an in-depth Congressional investigation that created serious pressure for change, see Committee on Energy and Commerce, *Nuclear Weapons Facilities: Adequacy of Safeguards and Security at Department of Energy Nuclear Weapons Production Facilities*, U.S. Congress, House of Representatives, 99th Congress, 2nd Session (6 March 1986). For a recent in-depth critique by a well-informed non-government organization, which contributed to new security initiatives by the Secretary of Energy, see Project on Government Oversight, "U.S. Nuclear Weapons Complex: Security at Risk" (Washington, D.C.: POGO, 2001; available at <http://www.pogo.org/p/environment/eo-011003-nuclear.html> as of).

²⁰ For discussion, see, for example, Bunn and Wier, *Securing the Bomb 2005*, pp. 99-107; Matthew Bunn, Anthony Wier, and John Holdren, *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2003; available at http://www.nti.org/e_research/cnwm/overview/report.asp as of 1 February 2005), pp. 115-18; Robert L. Civiak, *Closing the Gaps: Securing High Enriched Uranium in the Former Soviet Union and Eastern Europe* (Washington, D.C.: Federation of American Scientists, May 2002; available at <http://www.fas.org/ssp/docs/020500-heu/full.pdf> as of 15 March 2005); Philipp C. Bleek, *Global Cleanout: An Emerging Approach to the Civil Nuclear Material Threat* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, September 2004; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/bleekglobalcleanout.pdf as of 13 April 2005).

²¹ Bleek, *Global Cleanout*.

²² Where necessary, this should include help paying for the cost of new LEU fuel (especially in cases where reactor otherwise would not buy new LEU fuel because it already has HEU that will last for many years, or for the lifetime of the reactor).

²³ U.S. Government Accountability Office, *Nuclear Nonproliferation: DOE Needs to Consider Options to Accelerate the Return of Weapons-Usable Uranium from Other Countries to the United States and Russia*, GAO-05-57 (Washington, D.C.: GAO, 2004; available at <http://www.gao.gov/new.items/d0557.pdf> as of 2 February 2005).