

The Human Factor and Security Culture: Challenges to Safeguarding Fissile Materials in Russia

**Preliminary Report
November 2002**

**Center for International Trade and Security
The University of Georgia
USA**

**Research Team Coordinator
and Center Director:** Gary K. Bertsch

Center Associate Director Igor Khripunov

Center Assistant Director Michael Beck

Editors: Igor Khripunov and James Holmes

Contributors: Nathan Busch
Maria Katsva
Igor Khripunov
Dmitriy Nikonov

For more information, please contact:

Center for International Trade and Security, 120 Holmes/Hunter
Academic Building, University of Georgia, Athens, GA 30602.

Tel.: 706-542-2985

Fax: 706-542-2975, 706-583-8292

E-mail: cits@uga.edu

Web site: www.uga.edu/cits.

The Center for International Trade and Security would like to thank the NATO Science Program for a linkage grant that supported joint research with the Atomenergo Institute for Professional Education (Moscow); the W. Alton Jones Foundation, for providing funding for a workshop on nuclear security culture in Moscow, November 2001; and the U.S. Department of Energy for supporting nonproliferation and nuclear security awareness training for Russia's MINATOM officials in 1999-2000. This is a preliminary report, which the authors intend to revise and update in 2003.

INTRODUCTION

Because it is extremely difficult to produce fissile materials such as highly enriched uranium and plutonium – the key ingredients for nuclear weapons – terrorists and rogue states will likely attempt to acquire stolen materials. The greatest potential source of stolen fissile materials is Russia, where hundreds of tons of nuclear materials are at risk of theft. Over the last decade, there have been numerous thefts and attempted thefts of these materials from Russian nuclear facilities. Moreover, there is evidence that the al Qaeda and countries such as Iran, Iraq, North Korea, and Syria have all attempted to obtain stolen fissile materials from Russia.

The United States has responded to these risks by funding several programs to help Russia improve its control over nuclear materials. The U.S. government has spent over \$1.5 billion on these programs since their inception. For both political and technical reasons, however, the bulk of U.S. efforts have been focused more on the technical side of this problem—installing or enhancing equipment for physical protection and material accounting at Russian nuclear facilities.

While these technical upgrades are critically important, their efficient use depends on the extent to which nuclear site personnel are not only trained in technical skills, but also motivated and willing to perform these functions. There is growing evidence that Russian security culture is inconsistent with the nature and magnitude of modern threats, with personnel often failing to recognize the importance of following all the procedures and using the technologies necessary for protecting nuclear materials. Unless this issue is directly and comprehensively addressed, the Western security upgrades to Russian facilities will not be as efficient as originally thought.

For example, U.S. scientists have often observed “exceptions” made to security procedures during their visits to Russian nuclear facilities in order to speed up access to a secure area. Worse still, even when the modern surveillance and alarm systems have been installed at Russian facilities, they are often not used properly. In one instance, a new infrared intrusion detecting system was reportedly rendered ineffective because the grass was not mowed. At other facilities, high-quality surveillance systems were made useless when the facilities shut off their electricity in order to reduce their electricity bills. There are also numerous reports of guards shutting off security and monitoring systems because they decided there were too many false alarms.

The root of this problem is that Russia is making a transition from an authoritarian system that effectively eliminated any risks of insider theft to a new society with different values, career requirements, and human ambitions. Many low-paid workers at Russian nuclear facilities believe that there are other more important priorities than investing scarce money in security upgrades. They simply are less convinced that strict and costly security procedures and accounting systems are necessary to prevent theft by insiders. In addition, the nation’s still-immature legal order, rampant crime and corruption, and continued economic disruptions make an adequately motivated workforce the key to nuclear security in Russia.

If the efforts of the United States and the international community are to be successful, they clearly need to focus on more than just applying technical fixes to Russian security systems. There is also a need for a well-funded campaign devoted to changing the perceptions and

mentality of mid-level managers and low-level technicians at Russian nuclear facilities. This is particularly important for sustaining what the United States has already contributed to enhancing nuclear security in Russia.

The Department of Energy has been doing a great deal to train Russian nuclear personnel and deserves high praise for its efforts. This report outlines additional steps that U.S. institutions can take to help Russia develop a security culture equal to today's challenges. It is designed to offer a better understanding of the security culture problem in Russia, which can enhance the effectiveness of the ongoing efforts to provide material protection, control and accounting (MPC&A) assistance to Russia.

The first step is to promote a genuine commitment to improving Russian security on the political level. Top-level officials up to the president and prime minister must follow relevant events and publicly prioritize any efforts aimed at enhancing security arrangements. Second, American experts need to work with the Ministry of Atomic Energy and top-level managers of Russian nuclear facilities to develop security procedures and regulations that are not only rigorous and enforceable but also understandable and acceptable to the personnel. Third, the U.S. government and non-governmental organizations can expand "security awareness" programs by making them more innovative and interdisciplinary. These programs would help train Russian technicians and mid-level managers not only in methods of using and maintaining security systems, but also in the more fundamental reasons why nuclear security is important and why they must be personally responsible for its efficiency. U.S. nuclear managers can share with their Russian counterparts their own experiences and standards in sustaining and reinforcing security awareness on a day-to-day basis. Fourth, efforts must be made to improve personnel testing and recruitment procedures in the nuclear sector with a view to increasing the reliability of new hires.

For any major assistance project to succeed, it is necessary to factor in differences in national culture and psychology. In Russia, the human dimension of safeguarding fissile materials is seen as much more important than in Western society because of the Russia's distinctive history and traditions, not to mention the ongoing, tumultuous post-Soviet transition. The objective is to promote a working environment in which Russia's security personnel could perform as efficiently as their counterparts in other countries.

This paper examines obstacles to enhancing nuclear security in Russia and draws attention to the need for both improved safeguards and a more vibrant security culture. We begin by defining security culture and the concept of the "human factor," which is widely used in Russia to explain the importance of workforce skills, knowledge, and motivation in the effort to deal with security threats. We then review the nuclear security environment at U.S. facilities as a baseline for evaluating attitudes and approaches to nuclear security in Russia. Sections 2 and 3 focus on the role of the human factor in Russia's professional culture in general, and in the nuclear sector in particular. Finally, we conclude by recommending steps that the West should take to strengthen Russia's security culture, underlining the importance of addressing personnel issues.

Definitions

The term *security culture* has become a common buzzword in nonproliferation and nuclear security circles, but it is rarely defined clearly. For example, in several recent reports, the International Atomic Energy Agency (IAEA) has stressed the importance of developing a nuclear security culture within its member states.¹ In addition, Potter and Wehling state that perhaps the most important part of building sustainable nuclear security in Russia is developing a safeguards culture to help transform “the mind-sets of nuclear workers, guards and administrators.” They also outline some useful steps that the United States might take to this end. But, to date, there have been few rigorous and detailed discussions of Russia’s security culture. Nor are there many clear, generally-accepted definitions of what such a culture is. In possibly the most rigorous discussion of the subject, Doyle and Mladineo offer a useful definition of “safeguards culture,” which captures some elements of nuclear security.²

To clarify matters, we define security culture as (a) the degree of awareness of and commitment to widely understood security norms (namely the tenets of nonproliferation and best practices), not only by supervisors but by junior and mid-level personnel; (b) the degree to which available security technology is put to use; and (c) how effectively security rules and procedures are implemented.

As this definition suggests, there are several key characteristics of a robust security culture: it is characterized by (a) clearly promulgated, enforceable, and rigorously enforced rules and procedures; (b) nuclear workers who possess the technical know-how to use their security equipment correctly; and (c) workers who know why these technologies, rules, and procedures are necessary and perform their duties accordingly.

Finally, several prerequisites must be met for maintaining an efficacious security culture, including decent, regularly paid wages and a stable working environment. The workforce at nuclear facilities must have the skills, knowledge and motivation to do their jobs in accordance with best practices. Russians often use the concept of the *human factor* to capture the importance of a skilled and motivated workforce in explaining outcomes – especially accidents and mishaps in the nuclear sector. We believe that insight into how Russians perceive the human factor and its effects on nuclear security to be critical for U.S. and Western efforts to support nuclear security in Russia.

¹ International Atomic Energy Agency, General Conference, “Measures to Improve the Security of Nuclear Materials and other Radioactive Materials,” 45th regular session, item 19 of agenda, GC(45)/RES/14, September 14, 2001; Anita Nilson, Head, Office of Physical Protection and Material Security, the International Atomic Energy Agency, “IAEA Material Security Programme Overview,” Symposium on International Safeguards—Special Session on Combating Nuclear Terrorism, http://www.iaea.or.at/worldatom/Press/Focus/Nuclear_Terrorism/nilson.pdf.

² They define a “safeguards culture” as a “pervasive, shared belief among political leaders, senior managers, and operating personnel that effective MPC&A is critically important, as manifested in decisions and actions, large and small.” James E. Doyle and Stephen V. Mladineo, “Assessing the Development of a Modern Safeguards Culture in the NIS,” *The Nonproliferation Review* 5, no. 2 (winter 1998): 91.

SECTION 1: U.S. APPROACHES TO NUCLEAR SECURITY AND THE U.S.-RUSSIA MPC&A PROGRAM

The United States has decades of experience with nuclear security, and over time has developed what are arguably the most rigorous nuclear controls in the world. This was not always the case, however. The U.S. safeguards system was mainly understood to be a matter of economics, and fissile materials were controlled primarily because of their intrinsic value as property, rather than concerns about proliferation or terrorism. As a result, there were often serious weaknesses in U.S. fissile-material controls. For example, early on, it was perfectly legal to ship kilograms of plutonium through commercial freight and to store separated plutonium in facilities without 24-hour guard forces. Attention was increasingly devoted to the risks of proliferation and sub-national terrorism in the 1960s and 1970s, however, with the introduction of the Atoms for Peace Program and the Nuclear Nonproliferation Treaty, and as incidents of non-nuclear terrorism increased worldwide. As a result, the United States redoubled its efforts to improve the physical security both of defense nuclear facilities and of private-sector power reactors.³

Nevertheless, numerous congressional assessments in the 1980s and 1990s continued to find problems with U.S. nuclear security systems. For example, in 1986, the House Subcommittee on Oversight and Investigation reported that “the DOE’s own internal inspection reports show that plutonium and highly enriched uranium are still highly vulnerable to theft and sabotage [at key nuclear weapons facilities]”.⁴ Even as recently as the mid- to late 1990s, governmental oversight agencies continued to identify difficulties with the U.S. nuclear security. The DOE’s Office of Independent Oversight and Performance Assurance performed reviews in 1995 and 1998 that found significant problems with the DOE’s fissile-material assurance programs.⁵ While speculation about potential vulnerabilities in the U.S. nuclear industry has increased after the September 11 terrorist attacks, most governmental oversight assessments have found that the majority of difficulties with nuclear security has been addressed.

The nuclear-security systems that the United States has developed rely heavily on advanced technology. In addition, U.S. MPC&A systems are designed to provide “defense in depth,” meaning that there is a degree of redundancy in the systems, so that the failure of one part of the

³ William Desmond, Neil Zack, and James Tape, “The First 50 Years: A Review of the Department of Energy Domestic Safeguards and Security Program,” presented at a workshop on *A Comparative Analysis of Approaches to the Protection of Fissile Materials*, Stanford University, July 28–30, 1997, 4; John McPhee, *The Curve of Binding Energy* (New York, NY: Farrar, Strauss, and Giroux, 1974), pp. 28, 48, 52–53; and Mason Willrich and Theodore B. Taylor, *Nuclear Theft: Risks and Safeguards* (Cambridge, MA: 1974).

⁴ John D. Dingell, Chairman of the Subcommittee on Oversight and Investigations, Congressional Testimony, in *Safeguards at DOE’s Nuclear Weapons Facilities*, Hearing before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, House of Representatives, 101st Congress, 1st session, 7.

⁵ The United States General Accounting Office (GAO) also conducted several investigations of the security at DOE facilities. In one report in 1990, the GAO found that at Los Alamos National Laboratory, 78% of the security personnel failed a test of required skills. It reported that of the 54-member guard force, “42 failed to demonstrate adequate skill in using weapons, using a baton, or apprehending a person threatening the facility’s security.” See *Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities*, GAO/RCED-91-12, October 11, 1990. These findings are summarized in *Department of Energy: Key Factors Underlying Security Problems at DOE Facilities*, GAO/T-RCED-99-159, 8.

system does not result in the failure of the entire system.⁶ The entire MPC&A system must be carefully integrated so that all of its components work in conjunction. This requires that the specific objectives of the MPC&A system be identified, the MPC&A system be carefully designed, and the system be extensively tested to ensure that it performs as an integrated whole.

U.S. MPC&A systems are generally divided into physical protection and Material Control and Accounting (MC&A) systems. Physical protection systems are intended to deter and defeat attacks on nuclear facilities, while MC&A systems are designed to detect thefts of fissile materials. The ultimate purpose of a physical protection system is to prevent the theft of nuclear materials and the sabotage of nuclear materials or facilities. These objectives are achieved in two ways: by deterring threats, or by defeating them should groups or individuals attempt to steal nuclear materials or sabotage nuclear facilities. This deterrence is achieved by implementing a physical protection system that is *perceived* to be too difficult to overcome. And, of course, if anyone *does* attempt to steal materials or sabotage a facility, the physical protection system must also be able to stop the attempt. An effective physical protection system uses barriers, surveillance systems, alarms, and guards to achieve these goals.⁷ Armed and effectively trained security forces are required at facilities possessing Category I and/or Category II quantities of fissile materials. The qualifications and authority for protective personnel at DOE and DOE-Contractor Personnel are clearly established in official U.S. government regulations.

Unlike physical protection systems, which are intended to stop theft or sabotage attempts before they occur, MC&A systems, on the other hand, are used to detect a theft or diversion of nuclear materials once it has occurred. Materials are controlled through technologies and procedures intended to verify the precise location and storage condition of nuclear materials. In addition, accounting systems are in place to provide “a regularly updated, measured inventory of nuclear weapons usable material, based on routine measurements of material arriving, leaving, lost to waste and remaining within the facility.”⁸

Nuclear-materials accountability programs must ensure that all nuclear materials are accounted for and that theft or diversion has not occurred.⁹ They must therefore meet three objectives: to assure that all materials are present in the correct amount, to provide timely detection of a material loss, and to estimate the amount of any loss and its location.¹⁰

Nuclear control programs must control nuclear materials sufficiently to prevent or deter loss or misuse.¹¹ The general requirements for MC&A systems are thoroughly outlined in official

⁶ C.A. Coulter, R. Shropshire, and K. E. Thomas, “The Structure of Nuclear Material Safeguards Systems,” presented at a workshop at Los Alamos National Laboratory, *Fundamentals of Nuclear Materials Safeguards Systems*, April 12–16, 1999, II-9–I-10.

⁷ Guidance and Considerations for Implementation of INFCIRC/225/Rev.3, par. 401–402.

⁸ Jason Ellis and Todd Perry, “Nunn-Lugar’s Unfinished Agenda,” *Arms Control Today* 27, no. 3 (October 1997), 16.

⁹ U.S. Department of Energy, DOE O 474.1, *Control and Accountability of Nuclear Materials*, (Washington, D.C.: Government Publishing Office, 1998), 2.

¹⁰ J. T. Markin, “Fundamentals of Materials Accounting,” presented at a workshop at Los Alamos National Laboratory, *Materials Accounting for Nuclear Safeguards*, April 12–16, 1999, I-1.

¹¹ *Ibid.*, 5.

U.S. government documents.¹² These documents divide material control into four functional performance areas: access controls, material surveillance, material containment, and detection and assessment. The requirements in each of these areas depend on the attractiveness level of materials contained in each facility.

Cultivating a U.S. Security Culture

Although the United States places a high priority on high technology, it also recognizes that MPC&A systems can only be effective if workers at the facilities take ownership of nuclear security – following the necessary security procedures, using the security systems properly, and so forth. Although the United States has long maintained security-training programs and personnel-reliability programs for all personnel coming into contact with Special Nuclear Materials, a series of espionage allegations and security breaches at Los Alamos National Laboratory drove home the importance of proper security-awareness training in the late 1990s. Among the breaches was a loss of computer hard drives containing critical information on U.S. nuclear weapons. These revelations led to a renewed emphasis on security-awareness training at U.S. nuclear facilities.

In October 2002, in order to gain a better understanding of U.S. security-training programs, researchers from the Center for International Trade and Security met with employees at the Westinghouse Savannah River Company who oversee security arrangements at the Department of Energy’s Savannah River Site (SRS) in South Carolina. Although the following discussion specifically outlines the security-awareness program at SRS, all critical facilities in the U.S. nuclear complex have similar awareness programs.

- *Training for Managers and Executives Responsible for Security.* Because site managers and high-level officials are critical for cultivating and maintaining the security culture at nuclear facilities, these supervisory employees are generally enrolled in courses that train them to develop and manage security-awareness programs. The Albuquerque National Nuclear Institute provides such training seminars in Albuquerque and at DOE facilities.
- *Establishing and Promulgating Security Procedures.* The specific requirements for security awareness at DOE facilities are outlined in the DOE 470 regulation series. These regulations are available on the DOE website at <http://www.oa.doe.gov/sase/directives/p4701.pdf>. All employees are expected to be familiar with these regulations.

In addition, employees are given thorough briefings on security procedures at DOE facilities. These briefings include General Employment Training (GET) for all personnel employed at the facility, Comprehensive Briefings for all personnel with access to classified information or Special Nuclear Materials, annual refresher courses for all personnel with access authorizations, and termination briefings when an employee

¹² See, for example, U.S. Department of Energy, Office of Safeguards and Security, “Guide for Implementation of DOE 5633.A,” (Washington, D.C.: Government Publishing Office, 1993); and DOE 5633.3B, *Control and Accountability of Nuclear Materials* (Washington, D.C.: Government Publishing Office).

terminates his or her security clearance. The topics of these briefings vary with each type of briefing. Security regulations, and the corresponding briefings that explain these regulations, would obviously be much more extensive for employees with access to fissile materials or sensitive classified information.

- *Promoting Personnel Reliability.* The United States has also implemented a personnel reliability program for personnel in sensitive positions, including positions that require access to nuclear weapons, fissile materials, or classified information. This program includes extensive background checks for personnel prior to their receiving a security clearance, as well as regular in-house reviews of these employees. These in-house reviews, conducted annually, consist of an interview, urinalysis, psychological testing, and a credit check.¹³
- *Providing Competitive Salaries and Employee Benefits.* Another obvious, but often overlooked aspect of nuclear security in the United States is the fact that employees are well paid and receive generous benefits packages as part of their employment.¹⁴
- *Continuing Awareness Programs.* The Security Awareness Program also provides education on security issues throughout the year. It does so in a number of ways. These approaches include day-to-day briefings on security issues, including any security violations at the site or new security procedures or technologies that have been introduced at the site. The program also identifies a “security topic of the month,” which is discussed in the monthly meetings of individual groups and projects within the facility. A Security Meeting Guide is also published every month with slides and talking points to provide employees with timely information on security issues occurring at the SRS. Moreover, if any specific security concerns are identified for a particular project at the site, then specific briefings are given to the members of the project.

Attendance at security meetings and briefings is considered in employees’ yearly performance appraisals. In order to reinforce the importance of maintaining security on a day-to-day basis, signs containing security-awareness slogans are posted along roadways as a visual reminder to employees of the security posture at a specific site. Finally, DOE facilities have instituted a “Challenge Rule,” whereby employees are required to question any unusual event or politely challenge any unknown person on the site or at specific facilities.

- *Creating Incentives for Whistle-blowing.* There are a number of measures that create incentives for whistle-blowing. These include anonymous employee hotlines and crime-

¹³ Daniel Patrick Moynihan, *Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2 better check format on Senate docs, this isn’t quite right, 103rd Congress (Washington, D.C.: Government Publishing Office, 1997), available from <http://www.fas.org/sgp/library/moynihan/chap4.html>.

¹⁴ For an example of the pay scales and benefits packages given to DOE employees, see the Los Alamos National Laboratory Benefits and Compensation website, including “Fiscal Year 2002 Rate Tables,” available from <http://www.hr.lanl.gov/Benefits/salarymanagement/rate.stm>, and “UC Benefits Plans,” available from <http://www.hr.lanl.gov/Benefits/BenPlans/>.

stoppers hotlines. After an investigation, a monetary award may be given to the employee who reported the incident.

All of these factors help to ensure that the United States has nuclear personnel who are skilled, knowledgeable about security threats and procedures, and motivated to take action. Readers should not entertain the illusion that the U.S. approach to nuclear security is faultless and should be blindly emulated in Russia. There is always some room for improvement, and, hopefully, even the American MPC&A system is continuously adjusted to meet new threats and challenges. As we turn to a discussion of the role of the human factor in Russia, we will find evidence that Russians and Americans approach these matters differently, and that the human factor plays a crucial role in efforts to safeguard fissile materials in Russia.

U.S.-Russian Collaborative Programs

Following the collapse of the Soviet Union, the United States and Russia instituted collaborative programs that sought to help Russia improve its nuclear controls. In 1991 Congress approved funding for the Cooperative Threat Reduction program, or the Nunn-Lugar program, nicknamed after its primary co-sponsors in the U.S. Senate. Since its inception, this program has grown to incorporate a number of projects, including those intended to help Russia improve its MPC&A.

The U.S.-Russian MPC&A program is now a separate program overseen by the U.S. Department of Energy. Over the years, it has made significant progress in providing and installing physical protection and MC&A systems to improve security at Russian nuclear facilities. These MPC&A upgrades include the following:

- Placing bars on windows, reinforcing doors, and installing high-security fences.
- Installing sophisticated video surveillance and alarm systems, including infrared, sound, and vibration detectors.
- Installing portal monitors at all exits. The portal monitors sound an alarm if anyone tries to remove radioactive materials from the facility.
- Providing precision measurement equipment for obtaining accurate inventories of fissile materials, and thus verifying that no nuclear material has disappeared.
- Placing bar codes and tamper-indicating seals on storage containers to verify that the containers have not been opened or tampered with.
- Providing computer systems to keep track of the amounts and locations of all the nuclear materials at the facility.

The MPC&A program has made notable progress in improving Russian nuclear security. According to recent assessments, the program has provided improved security for about 192 metric tons of fissile material and is working to improve security systems for an additional 410 tons of material.¹⁵ Because of the massive assistance provided by the United States, Russia's MPC&A system strongly resembles the American system. Nevertheless, there is much that still

¹⁵ Jack Caravelli and Chris Behan, "Accomplishments and Challenges in the MPC&A Program," *The Monitor: International Perspectives on Nonproliferation* (Spring 2001), 3.

needs to be done. It is currently estimated that only 40% of the 600 metric tons of nuclear materials at risk is now stored in buildings with improved physical protection; less than half of that is reportedly stored in buildings with comprehensive MPC&A systems.¹⁶

Both the United States and Russia, however, have renewed their joint commitment to bolster Russia's nuclear security systems, and the MPC&A program is poised to make swift progress. For example, in 2001, the United States and Russia concluded an agreement to open most of Russia's remaining sensitive facilities to American technicians in order to carry out security upgrades. Moreover, after their November 2001 summit meeting, Presidents Bush and Putin issued a joint statement calling for "improving the physical protection and accounting of nuclear materials for all possessor states." On November 29, 2001, in line with this presidential guidance, Energy Secretary Spencer Abraham and Minister of Atomic Energy Alexander Rumyantsev announced that the two countries had agreed to expand and accelerate efforts to improve MPC&A arrangements.¹⁷

That the human factor was an important ingredient in the overall MPC&A assistance effort became apparent to DOE officials in the late 1990s. Improving the training of Russian personnel and encouraging them to embrace security procedures, it seemed, was a vehicle for promoting the long-term sustainability of the U.S. assistance program, which itself relied on enhanced performance by the personnel staffing Russian nuclear facilities.¹⁸ The human factor, believed DOE officials, was taking on added importance as experienced personnel in Russia's nuclear sector reached retirement age and were replaced by new recruits.

DOE has launched a multi-pronged effort to ensure that knowledge and operational training were passed on to the next generation of workers charged with executing security procedures. The first prong created regional training and education centers to school trainers and managers in the concepts involved with physical protection, material control and accounting, and protective force.¹⁹ The second will institute site-level training programs to provide on-the-job training and mentoring. And the third will devise specific job qualifications and standard operating procedures that complement this improved training – and round out the U.S. strategy of buttressing the human factor within the Russian nuclear sector.

These pioneering efforts to contribute to and improve the human factor are an important tool, without which the loss of institutional history and knowledge will increase the chances for accidents, losses, and theft. However, as will become evident in the next two sections, fostering a robust nuclear security culture, made up of motivated personnel, may require additional inputs and training – in combination with the ongoing DOE efforts.

¹⁶ Matthew Bunn, John P. Holdren, and Anthony Wier, "Securing Nuclear Weapons and Materials: Seven Steps for Immediate Action," Nuclear Threat Initiative and the Managing the Atom Project, 2002, 10.

¹⁷ "Text: U.S., Russia to Step-up Efforts to Safeguard Nuclear Materials," *Washington File* (Washington, D.C.: U.S. Department of State, December 4, 2001).

¹⁸ Kenneth Sheely and Katherine McCann, "Long-Term Sustainability in Russia – Moving Beyond MPC&A Upgrades," in *Proceedings of the 42nd Annual Meeting of the Institute of Nuclear Material Management* 2001.

¹⁹ As of now, these fully functional centers include the Russian Methodological Training Center (RMTC) and Interdepartmental Special Training Center (ISTC), both located in Obninsk, as well as the Moscow State Engineering and Physics Institute

SECTION 2: THE HUMAN-FACTOR-CENTERED MENTALITY IN RUSSIA

In Russia, professional/work culture and attitudes bear the burden of the Soviet past. If we hope to enhance nuclear security in Russia, consequently, we must understand and come to terms with the Soviet legacy as it relates to worker performance and attitudes. Only then can we find solutions that can counter or offset this legacy. In particular, it is important to understand the greater emphasis Russians place on individual authority and responsibility, as opposed to formal rules and regulations.

Impact of the Soviet Political System

Unlike a Western liberal democracy, which operates predictably regardless of who is in office, Soviet governance depended heavily on the personal loyalties, beliefs and preferences held by individual political leaders. Top managers in Russia have much greater power and discretion than their Western counterparts while weak democratic institutions and a lack of accountability tend to strengthen their position. At the same time, a considerable portion of lower-level employees continue to disregard regulations in a manner consistent with the old Russian saying “I am just a small fish.” This attitude is still somewhat characteristic of Russia’s nuclear personnel today.

- *Double Work Standards.* Stark inconsistencies between the proclaimed goals of achieving Communism and the reality of shortages of basic consumer goods generated cynicism and political apathy. Under such circumstances, citizens felt little allegiance to the official ideology, especially in the later days of the Soviet Union. The system became something to be beaten rather than conformed with. This adversarial mindset contributed to the development of people’s extreme resourcefulness and ingenuity, making informal, semi-legal, “under-the-counter” interpersonal relationships for the purpose of obtaining goods and services the norm. At the same time, as some observers note, “Central control over all political and economic aspects of society created an unmotivated, and often careless, workforce.”²⁰ The more people became resourceful in obtaining consumer goods and services for personal use, the less they were committed to their official jobs and duties. Regular jobs were less a profession than a vehicle to survive, or to increase personal wealth. This trait partly explains numerous cases of stealing and diversion of a variety of nuclear materials in the early and mid-1990s.
- *“Scapegoat” Mindset.* During the Soviet era, glaring societal and economic inconsistencies could not on an official level be attributed to flaws of the political system. Consequently, these intrinsic shortcomings in the system were typically ignored, or explained as either sabotage by “enemies of the people,” the product of foreign conspiracies, or anomalous mistakes by specific individuals. The performance of the party or the political system was never called into question. Specific failures were officially investigated, those found guilty were punished, and the problem was considered resolved until the next incident. This practice instilled a *scapegoat mentality* that

²⁰ Ajay Goyal, “Russia’s Untapped Treasures,” *The Russian Journal*, available from http://www.norasco.com/ajay_goyal_6.html.

reflexively placed the blame on individual error or ineptitude, rather than more constructively looking for problems within the political and economic system – the problems that spawned problematic behavior. Both the tragic accident involving the *Kursk* submarine and a recent military helicopter crash in Chechnya, which caused the deaths of hundreds of people, have led many to complain about ineptitude, but will probably not lead to new regulations, norms, or procedures that might ward off such tragedies in the future. Instead, a host of high-ranking military officers and government officials were identified and subjected to various degrees of punishment and reprimand.²¹ It remains unclear how breaches of nuclear security were dealt with and evaluated in the Soviet period, but in all likelihood the blame for such infractions was affixed to individuals. Improving procedures was a secondary concern at best.

- *Poor Implementation Record.* It is often said that the severity of Russian laws is balanced out by the selectiveness of their application. But poor discipline and failure to follow procedures cannot be attributed to the lack of standard procedures alone. Rather, like any overly bureaucratic and centralized political system, Russia produced numerous laws, rules and regulations, which are often bulky, complicated, contradictory, frequently changed – and therefore hard to follow.²² It is not surprising that officials and ordinary citizens often skimp on following rules and regulations – both for reasons of personal negligence, and because the procedures carry little respect and value due to their vagueness and inconsistency.²³

Failure to follow procedures and regulations may have particularly serious consequences in the nuclear sector. For example, despite the existing regulations for handling radioactive materials and byproducts, evidence constantly surfaces indicating that such crucial rules are not universally followed – in the full knowledge of the resulting hazard to human health. In the month of October 2002 alone, Moscow Radiation Emergency Service “Radon” discovered almost 30 tons of radioactive waste throughout the city, and removed the waste for safe storage.²⁴ If such regulations have a poor implementation record in Moscow – where supposedly the city government has the nation’s best personnel and resources to implement and enforce them – conditions are likely even worse in the rest of the country.

²¹ Susan Glasser, “Navy Found Culpable in Russian Sub Disaster,” *Washington Post Foreign Service*, August 30, 2002, available from <http://www.washingtonpost.com>; Steven Lee Meyers, “Putin Dresses Down Military for Crash that Killed 116,” *The New York Times*, August 22, 2002, available from <http://www.nytimes.com>; www.strana.ru/print/157914/html.

²² The Soviet legal system was simpler because of the relative simplicity of economic and social relationships. As Russia began developing democratic political institutions and a market economy, the legal system had to be transformed to reflect the new realities, at the same time making it less comprehensible and therefore alien to citizens unused to such complexities.

²³ Some in Russia’s leadership are very concerned about the negligence and lack of discipline among government officials. A recent report by the Main Control Directorate under the Office of the President revealed a problem with timely and complete fulfillment of government orders and instructions within the government ministries and agencies themselves. As a result, over 600 memoranda had to be dispatched in the first six months of 2002 to these agencies demanding them to take appropriate measures and determine the responsibility of involved officials. ITAR-TASS News Agency, September 16, 2002, available from <http://www.integrum.ru/webpush/agents/defense/vpk/un007572.htm>.

²⁴ INTERFAX News Agency report, October 31, 2002; available from <http://www.interfax.ru>.

Technological Gap

A more tangible and utilitarian explanation of the greater reliance on human factor in Russia also comes to mind. The lopsidedness of the Soviet economy, which was geared towards non-productive sectors such as defense and space programs, coupled with the lack of incentives for individual achievement, overtaxed the nation's vast national resources. A widening gap with the West in cutting-edge technology, research, and production ensued, and persists even now.²⁵ Even the abundance of scientists and engineers produced by Russian institutes and universities generates little economic benefit. Thousands of highly educated Russians emigrated to Europe, the United States, and Israel owing to the economic crisis in the 1990s and the attendant lack of funding and employment. Western information-technology companies operating in Russia often complain that the local pool of professionals consists mostly of overqualified university graduates who possess vast theoretical – but obsolete – knowledge, and who lack either the culture or commitment to work in a rapidly Westernizing professional environment.²⁶

It is not surprising that, in industries hampered by decrepit and unreliable equipment, confidence in the ability and resourcefulness of individuals was depicted as the solution to the nation's economic woes. Painful failures, especially in electronics and computer manufacturing, considerably aggravated the situation. As a result, Russia's technological culture came to depend on simplistic solutions that left little room for rapid improvements in quality. In the nuclear sector this trend brought about a dramatic disparity that was illustrated, among other things, by the world-class nuclear fuel cycle found in Soviet plants, which existed side by side with obsolete – again, by world standards – MPC&A systems. Nuclear personnel lacked the skills needed to operate sophisticated security equipment; indeed, on occasion they even treated it with suspicion.

Corruption and the Disruptive Human Factor in the Military

In the military, the human factor negatively – even disruptively – influences the government's ongoing efforts to instill discipline and enforce regulations. A combination of obsolete and disintegrating equipment and hardware, improper use, low morale, and corruption within even the highest military ranks has had severe consequences. Accounts recounting the theft and resale of weaponry and military hardware, often to militant groups in Chechnya and criminal gangs throughout the country²⁷ do not even begin to convey the extent of the corruption. Desertion is commonplace, and the deserters usually take their weapons with them. Mass killings of military personnel by their comrades through misconduct such as hazing, drinking, and drug use are likewise widespread. Criminal negligence causes massive military accidents, such as the

²⁵ A recent study by Center for International Development, Harvard University, lists Russia as sixty-third out of seventy-five ranked countries in 2001, down from fifty-fourth in 2000, on the Growth Competitiveness Index. On the Index's technology component, Russia is ranked sixtieth while the United States ranks first <http://www.cid.harvard.edu/cr/index.html>.

²⁶ Ajay Goyal, "Education Hurdle for Russia's IT Sector," available from http://www.loot.ru/ajay_goyal_d.htm. Refer to Figure 1.

²⁷ Russia's Interior Minister, Boris Gryzlov, revealed recently that there are over 134,000 units of illegally owned weaponry throughout the country, most of which originated from military bases. Also, an investigation into of the deadly May 2002 terrorist attack on Kaspisk revealed that the bombs and explosives used by terrorists had been purchased at a nearby military base.

sinking of the submarine *Kursk*; cover-ups and blame-shifting inevitably follow.²⁸ A recent report reveals that within the last ten years, investigators uncovered thefts of military hardware and weaponry totaling some 350 billion rubles (almost \$12 billion).²⁹ This malaise will make the task of safeguarding Russia's fissile material and upgrading the security of its nuclear sites even more daunting.

The problem with the military is twofold:

- *Equipment and Technology.* First, because of economic difficulties, the Russian government has little funding to allocate to the armed forces, and no coherent plan to refurbish and replace their weaponry and hardware. The equipment and weaponry currently used by the armed forces are aging rapidly, are often stolen (either wholesale or for parts) and suffer tremendous wear and tear from the ongoing war in Chechnya.
- *Human Factor.* Problems with hardware are aggravated by the deepening social and psychological crisis in the military, which afflicts both the officer corps and rank-and-file conscripts. Morale among officers has plummeted amid low pay, unsuitable living conditions, the falling prestige of military service, and, most importantly, the lack of prospects for advancement. The military profession, which used to be highly regarded and generously rewarded in the Soviet Union, now compares very unfavorably with the lifestyles and incomes enjoyed by the new Russian business elite and the emerging metropolitan middle class. For conscripts, the two-year term of military service is tantamount to a prison sentence because very little distinguishes one from the other. On top of low-quality food, poor living quarters and uniforms, and confinement to barracks for long periods of time, the soldiers have to endure severe hazing from both their peers and commanding officers, who often use their units as cheap labor and find it therapeutic to vent their frustrations on them in the form of physical violence.³⁰ Personality cults in the military have reached dangerous and grotesque proportions.

Corruption in the Russian military is yet another sign of a human-factor-related problem, which is ubiquitous at all levels. According to the Interior Minister Boris Gryzlov, his troops continue to confiscate illegally acquired heavy weapons from legally established entities. Fully equipped battle tanks and multiple-rocket-launching systems (MRLS) are among the booty recovered by the government. On only two recent occasions, August 28 and September 4, 2002, two T-72 tanks with all standard weapons and two "Smertch" MRLSs were found in possession

²⁸ Investigation into the *Kursk* tragedy revealed that the sinking was caused by a misfiring of an experimental torpedo, itself the result of inadequate training of the submarine's crew. The damage to the vessel, and the loss of the entire crew, were caused by the absence of damage-control equipment and structures. Most troubling, however, is the fact that it took the military command nine hours to declare the boat missing, and 31 hours to find it despite the fact that 5 other submarines, as well as 18 surface ships carrying a total of 22 rescue aircraft and 11 helicopters were at the scene. For months after the disaster, certain high-ranking military and government officials insisted that the cause of the accident was a collision with a stray foreign submarine http://ntvru.com/russia/29Aug2002/kursk_rg.html.

²⁹ <http://www.ntvru.com>.

³⁰ Five thousand military personnel in Russia commit suicide annually – more than die in combat in Chechnya; almost 90 percent of draft-age youth are draft-dodgers. Michael Orr, "Chaos in the Barracks," *The Wall Street Journal*, October 4, 2002; available from <http://inopressa.ru/details.html?id=9401>.

of two private companies based near Moscow. Gryzlov announced in September 2002 that his agency alone had confiscated about 1.5 tons of explosive substances and 9,000 explosive devices in 2001.³¹ These widespread illicit trafficking in a range of weapons systems can potentially present a threat to nuclear security because they can be used by organized criminal or terrorist groups to orchestrate an attack on a nuclear facility. Russia has yet to introduce a nationwide accounting and control system for conventional weapons, ammunition, and explosives.

One of the most popular “businesses” is smuggling precious metals from electronic systems, particularly high technology and strategic weapons.³² Therefore, personnel disaffected with low morale and low salaries – particularly mid-level managers who know the system – can easily become an insider threat. What has been going on in the armed forces should serve as a warning to the nuclear sector. Despite the difference between the two sectors, some common trends do exist.

Changing Times

The experience with political and economic reform in Russia, which now spans over a decade, has demonstrated that culture and mentality are not inherent traits congenial to the Russian people – contrary to the view taken by some historians³³ – and that they can be changed given time and appropriate training and resources. Economic reforms are gradually bringing about modest changes within the traditional Russian industries, such as agriculture, defense, or aerospace; at the same time, reform has permitted an entirely new range of enterprises, previously unfamiliar to the Russian public, to develop. Among them, to name just a few, are modern telecommunications, private security, personal computers, mobile telephones, and e-trade. Their rapid infusion into the nuclear sector is also expected to accelerate. In addition, Western standards are moving slowly into traditional fields such as politics and education.

- *Cultural Transformation and New Industries.* In addition to the obvious conveniences that such rapid expansion of consumer-oriented goods and services brings to a heretofore unpretentious public, it also generates a considerable cultural transformation,³⁴ particularly with regard to Russians’ attitudes about new technologies and the role of the human factor in their application. Since most of the advanced technologies thus introduced are of Western origin and/or enter the Russian consumer market through Western suppliers, the process also carries with it a set of professional ethics, attitudes,

³¹ INTERFAX News Agency, “Interview with Interior Minister Boris Gryzlov,” September 13, 2002.

³² At Vidyaevo at Northern Fleet, a sailor stole parts of monitoring devices of nuclear reactor after finding keys for the control panel. Two naval officers were detained in Petropavlovsk-Kamchatsky for attempting to sell nuclear-submarine components in April 2001. According to a military prosecutor based in Petropavlovsk-Kamchatsky, Yuri Sazonov, it was the fifth attempt in Kamchatka by soldiers, sailors, and officers to bolster their personal wealth by trafficking in military property. On New Year’s Eve 2000, two sailors tried to smuggle uranium rods out of one vessel’s nuclear reactor. More often, valuable metals such as copper, palladium, beryllium, and lithium are being smuggled. The Northern Fleet reported fourteen cases of smuggling, all involving precious metals, in 2000, and there have been eight cases so far in 2001. *Inopressa.ru*, June 16, 2001; *ITAR-TASS*, April 23, 2001; *Chronicle of Criminal Events*, June 6, 2001.

³³ See, for example, Alexander Zinoviev, *The Demise of Russian Communism* (Moscow: Tsentrpoligraph, 2001).

³⁴ Many observers have noted the changing work ethic, accompanied by a culture geared towards better service and performance, among the younger generation of Western-trained Russian managers. *BISNIS Bulletin*, June 2002.

and practices associated with a Western-developed advanced technology or product. These new technologies are more easily and readily embraced by the younger contingent of Russian professionals, who are not burdened by the classic Soviet education and culture, with all the limitations that culture entailed. Despite the costs, the installation of more sophisticated MPC&A equipment, paired with young people with better skills and motivation, can yield overall improvements to Russian nuclear security.

- *Changing Attitudes towards the Human Factor.* An Internet search of the Russian-language websites³⁵ for the topics “human factor” and “security culture”³⁶ yielded an interesting pattern, which supports the proposition about the shifting cultural attitudes regarding the role of the human factor in technology. Whereas sites concerning modern technologies such as software development and automated security systems looked at the human factor as something that has an adverse effect on the performance of new products and technologies and should be eliminated, other sites from the same list of search results maintained that the human factor was especially important to the safety and security of an enterprise.
- *Cultural Transformation in Old Industries.* Such stark differences in attitudes, which seem puzzling on the surface, are understandable considering the above discussion. New high-tech industries are populated by a younger generation of professionals who have firsthand knowledge of the capabilities of new technologies. These individuals consequently regard the human component as more of an impediment than an asset to their firms. By contrast, professionals working in traditional industries, including the nuclear sector, that remain dominated by older, Soviet-built equipment and technologies, still harbor the mentality and the culture that emphasize the role of the human factor.

Although there has been a modest influx of young employees in the nuclear industry, it is still dominated by the technical elite born and educated under the Soviet system. As long as this is the case, the success of U.S. and Western efforts to introduce Western-style security equipment and procedures will rely on the ability and willingness of the personnel staffing Russian nuclear facilities to adjust to new equipment, rules, and regulations. The special attitude towards the human factor in Russia may be a remnant of the disappearing era – but international security over the short term, and cooperation between Russia and the West over the longer term, will depend on how well this stubborn cultural obstacle can be overcome.

³⁵ Russian language Internet search engines at <http://www.rambler.ru>, <http://www.yandex.ru>.

³⁶ Terms “safety” and “security” in the Russian language are represented by the same word – “bezopasnost,” which is often confusing in a bilateral dialogue.

SECTION 3: THE CRITICAL ROLE OF HUMAN FACTOR FOR SAFEGUARDING FISSILE MATERIALS IN RUSSIA

Technology is playing an increasing role in nuclear security. Yet, in Russia, the personnel charged with nuclear security are not yet able to use new technology effectively. The lack of nuclear security in Russia, then, has more to do with the practices of personnel than with the presence or absence of technology. The dismal conditions under which nuclear personnel toil, combined with pervasive lax attitudes towards nuclear security, mean that nuclear material in Russia is at much greater risk of diversion than in other nations. Thus, efforts to enhance nuclear security through new gadgetry alone will fall short. Improving nuclear security in Russia will require both technical upgrades and attention to the motivation, training, and work environment of employees assigned to nuclear facilities.

Personnel Shortcomings

Personnel at nuclear facilities in Russia have already proved that they frequently misuse and mismanage security equipment. A U.S. General Accounting Office (GAO) report of February 2001 unearthed several examples of poorly administered equipment.³⁷ Gates were left open and unattended. Guards failed to respond to alarms. Guards also failed to check the identification of personnel entering sensitive areas housing nuclear material. Others have noted that equipment is often left uninstalled or inoperable.³⁸ Mid-level managers sometimes bypass security equipment

³⁷ According to one report by the U.S. General Accounting Office, GAO-01-312, "Security of Russia' Nuclear Materials," (Washington, D.C.: Government Publishing Office, 2001), 12, at three out of nine sites GAO group visited, "some problems appeared to decrease the effectiveness of the new systems. For example, one site left a gate to its central facility opened and unattended during the day. According to a site official, the gate was left open to allow employees to enter and leave the facility without having to use the combination locks on the gate. When the gate is open, the only other controlled access point is on the perimeter of the site. At another site the guards did not respond to metal detectors that were set off when the GAO team entered the site, nuclear materials portal monitors were not working, and the alarm system had exposed cabling that could allow an adversary to cut the cable and disable the alarm easily. At the third site, the DOE had provided heavy metal containers that could be bolted to the floor to make it more difficult for an individual to gain access to the material, but some of the containers were empty, and the site stored material in old containers that did not offer as much protection. In addition this site did not have access controls, such as material detectors or nuclear material portal monitors at locations where nuclear material is stored, and the guards did not check the identification of the people entering the storage areas."

³⁸ In 1999, a well-known U.S. expert in Russian nuclear security, Matthew Bunn, said in an interview with PBS, subsequently broadcast on *Frontline* under the title *Russian Roulette* (available from <http://www.pbs.org/wgbh/pages/frontline/shows/russia/interviews/bunn.html>): "There are facilities where the electricity has been cut off, that runs the security systems, because the facility couldn't pay its bills. There are facilities where they literally don't have the money to have 24-hour manning even at the central guard station. So if you came and tried to steal the material when the guard was off duty, you'd be able to....But you have to work not only on technology; you have to work on people, on relieving the kinds of economic desperation to lead guards to go off and forage for food. I'm very concerned, frankly, that if we don't deal with the electricity at nuclear facilities keeping going, that runs the security systems, if we don't deal with guards who haven't been paid for months at a time and are literally hungry and heavily armed, that we could have a proliferation disaster on our hands, with nuclear material finally falling into the hands of a terrorist group or a rogue state....You have a situation at one of the largest Russian nuclear facilities – at Mayak in particular – where a guard goes berserk, kills a couple of his comrades, and runs off, heavily armed. No one's found him yet. You have a situation where a sailor goes berserk, takes over a nuclear submarine, and holds everybody at bay for 20 hours before finally committing suicide. You have a situation where five officers of the Twelve Main Directorate, the people in charge of guarding nuclear weapons, essentially rebel and take hostages, kill a couple of people, before they're finally subdued by Ministry of Defense and Federal Security Service forces."

or disable equipment. At several facilities security procedures are violated systematically: Either the personnel assigned there do not understand the procedures correctly, or necessary and adequate procedures simply are not in place.³⁹ The National Intelligence Council's report to the U.S. Congress mentioned that guards sometimes abandon their posts, and at one location an alarm system worked only half the time.⁴⁰

Inadequate Infrastructure

Russian facilities do not always have the infrastructure to support technical upgrades and equipment. Power outages at nuclear facilities are commonplace, shutting down equipment for hours at a time and rendering even state-of-the-art electronic security equipment useless. In these instances, maintaining security depends on the efforts of security personnel. Numerous media reports have described power outages at strategically important facilities – nuclear and biological. Sometimes the power is switched off by the staff itself on weekends to save money, or switched off by power providers when the facility is unable to pay its electric bill.⁴¹ Power outages are so common in Russia that the Russian government issued a resolution prohibiting any cuts in the supply of power to strategic facilities. However, local utilities often do not comply with this resolution, thus jeopardizing the safety and security of the strategic facilities when they fail to pay for their services on time. In some cases, nuclear facilities lack the funds to pay bills leading regional companies to cut their supply of electricity.

The equipment at these nuclear facilities is often inoperative because the facilities lack the funds and expertise to repair it. Moreover, a great deal of the security equipment at nuclear facilities has operated well beyond its service life.⁴² When asked about the condition of security systems at their facilities, 29 percent of nuclear managers reported that security equipment was “sometimes” broken, while only 43 percent said that they had on-site personnel capable of repairing inoperative or malfunctioning equipment. Some nuclear managers have resisted installing more advanced security systems for the simple reason that they feel ill-prepared to sustain imported technologies.⁴³

³⁹ Irina Koupriyanova, “Assessment of Effectiveness of US MPC&A Assistance to Russia,” *Yaderny Kontrol* 2 (March–April 2002), 57-65.

⁴⁰ U.S. National Intelligence Council, “Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces,” February 22, 2002, available from http://www.cia.gov/nic/pubs/other_products/icarussiansecurity.htm.

⁴¹ Matthew Bunn, Interview with *PBS Frontline*, 1999; and “Loose Nukes Fears: Anecdotes of the Current Crisis,” *Global Beat*, Issue Brief No. 45, December 5, 1998; For example, in the summer of 2002, the Scientific Research Institute for Applied Microbiology in Obolensk, whose inventory includes pathogens such as anthrax and the plague, was cut off from power supplies because of unpaid bills owed to local utilities (\$1.7 million). Earlier in 2002, under similar circumstances, the leadership of the Institute instructed the staff to get all the exits and entrances welded shut except for the main one, where additional guards were posted. “Custodians of Anthrax and Plague Were Cut Off from Power Supplies,” August 15, 2002, available from <http://www.strana.ru>

⁴² “People are Equipment are Tired. Economy on Security Hastens Technogenic Disaster,” *Novaya Gazeta* 56, August 5, 2002; *Hearings on Security at Russian Duma*, in *Yaderny Kontrol* 2, vol. 38 (March-April 1998), 34-36. According to Vladimir Kuznetsov, 50 to 90 percent of equipment is operated beyond its service life. Vladimir Kuznetsov, *Main Challenges to Security at Nuclear Fuel Cycle Facilities* (Bellona, 2002).

⁴³ Igor Khripunov, Masha Katsva, and Terrell Austin, “Working Towards a Security Culture in Russia: The Human Factor in MPC&A Preliminary Findings,” *The Monitor: International Perspectives on Nonproliferation*, Spring 2001, 10-14

Socio-Economic Collapse

The dire economic conditions at nuclear facilities also threaten to undermine effective nuclear security practices. Personnel are underpaid, as noted earlier. Many of the cases of nuclear diversion arose when personnel at these facilities saw an opportunity to make quick money. Fortunately, most cases of nuclear theft by staff personnel have not involved significant quantities of material. This of course assumes that most cases of smuggling have been detected.

Poor working conditions, low salaries, and the reduced prestige associated with the nuclear industry also threaten to undermine the conditions necessary to support a security culture. During the Soviet era, work in the nuclear sector brought with it pride and patriotism. Work in the weapons complex was especially prestigious, as weapons engineers were recruited from Russia's top universities and institutes. Many were motivated by a desire to serve the country and the cause. These motivators have been on the wane in the post-Soviet years. Senior employees at the facilities generally retain a sense of personal responsibility. However, the patriotism and pride that characterized workers in the past is hardly to be found in the new cadre of nuclear leaders.⁴⁴ The nuclear industry is no longer so prestigious, and rising managers are inferior to their Soviet-era predecessors. The best and brightest in Russia now aspire to high-paying jobs in the private sector.

This lack of motivation and decline of prestige in the industry has serious implications for security. Security is also threatened by problems of alcohol and drug abuse at nuclear facilities.⁴⁵ Increased and compulsive drinking is a reflection of general trends in Russia. In the first five months of 2002, 18,224 Russians died from excessive drinking (compared with 16,858 in the first five months of 2001).⁴⁶ The requirements for drug and alcohol tests among nuclear personnel are often ignored, so there is no way of knowing how many people working at nuclear sites are actually intoxicated on the job.⁴⁷

Failing to Grasp the Threat

Most nuclear security analysts believe that a scenario in which nuclear site personnel steal nuclear material is the most probable, and thus the one to be most concerned about. In fact, nearly all known cases in which nuclear material was diverted have involved insiders.

⁴⁴ When a computerized inventory was launched at the Kurchatov Institute, several facilities found "unaccounted excess nuclear materials." The Kurchatov Institute apparently lost records regarding a total of 18 kg of plutonium and 67 kg of uranium-238. The findings may have been suppressed had it not been for well-motivated old cadres with a sense of responsibility. However, an expert at the Kurchatov Institute complained that the morale in the nuclear industry had decreased dramatically. Interview with A. Rummyantsev, Kurchatov Institute, November 2000.

⁴⁵ Statistics about criminal activities reveal that more than half the soldiers apprehended with drugs in their possession began using them for the first time during their military service. The Russian military paper *Krasnaya Zvezda* reported that, "despite the tightening of measures to keep [drug users] out of the draft, their penetration into the army ranks continues." In May 2000 the head of the 12th Defense Ministry Directorate (12th GUMO) in charge of nuclear weapons, General Valynkin, stated that two students at the 12th GUMO's Security Assessment Training Center had been expelled as a result of the drug tests. Deborah Yarsike Ball, "The Security of Russia's Nuclear Arsenal: The Human Factor," *Policy Memo Series*, Memo no. 91, October 1999.

⁴⁶ Andrei Vaganov, "Russia's Regions Alcohol Rating," *Nezavisimaya Gazeta*, August 16, 2002.

⁴⁷ Kuznetsov, *Main Challenges to Security at Nuclear Fuel Cycle Facilities*.

For example, the Elektrostal machine building plant was the scene of the first smuggling cases in the early 1990s. It was the first facility to receive upgrades and became one of DOE's success stories. Yet there were two further smuggling attempts at the facility in 2000, both involving managers. When one of the culprits was caught, he claimed financial motivations. In May 2001, the Novosibirsk Federal Criminal Police and Ministry of Interior Affairs arrested a group of four individuals who had gained access to nuclear material by convincing three employees of the Novosibirsk Chemical Concentrates Plant to steal lithium from the plant. This diversion occurred despite technical upgrades at the facility.

In a recent test of security precautions by the Kurchatov Institute in Moscow, an "interloper" was able to gain access to nuclear material, even though he had only limited knowledge of the system.⁴⁸ At one of the facilities a mid-level manager made a bet with his director that he would be able to smuggle nuclear material out of the facility. He won the bet. At another facility a genuine case of smuggling took place while employees were changing shifts.⁴⁹

However, surveys and interviews with nuclear personnel in Russia suggest that the insider threat is not fully appreciated. Instead, nuclear leaders are just as likely to identify external threats as a source of concern. According to a preliminary survey conducted by Center for International Trade and Security in 2001, neither top-level managers nor mid-level managers see the inside threat as any greater than the threat posed by outsiders such as terrorist groups. In part this may reflect mass media coverage of the nuclear threat.⁵⁰ The Western mass media has drawn much greater attention to the threat posed by disgruntled Russian workers who are tempted to sell radiological material to make money. Russia's mass media has focused on nuclear threats, to be sure, but the concerns voiced there have centered more on the ability of external groups to sabotage or divert nuclear materials.

In the aftermath of the October 2002 hostage-taking situation and subsequent threats by a Chechen rebel leader to strike Russia's nuclear facilities, Russia's Ministry of Atomic Energy (MINATOM) set up an anti-terrorist coordinating group and improved security arrangements. While that was certainly a justified and timely precaution, these arrangements will inadvertently divert attention and funding away from insider threats.

Underdeveloped Normative and Legal Basis

The lack of security guidelines and regulations, coupled with a culture that emphasizes compliance with superiors –rather than compliance with rules – threatens the security of the Russian stockpile of nuclear material. The legal basis underpinning nuclear-material security is underdeveloped. There are few national standards that set practices for nuclear materials accountability and management. Site-level procedures for nuclear security are also wanting. Some Russian experts characterize the volumes of U.S. Nuclear Regulatory Commission (NRC)

⁴⁸ Interview with Kurchatov Institute's nuclear expert, November 2000.

⁴⁹ Interview with Konstantin Dushutin, Moscow Institute for Professional Training MIPK 'Atomenergo' March 19, 2001.

⁵⁰ Khripunov, Katsva, and Austin, "Working Towards a Security Culture in Russia," 10-14. Immediately before this survey, the Russian cabinet had two meetings on MPC&A and nuclear security. The meetings garnered broad media coverage.

and DOE security regulations as excessive, but admit that the dearth of adequate normative and regulatory guidelines that is the norm in Russia is a real problem.

Those documents that do exist sometimes lack clarity and abound in generalizations. Interagency coordination is not adequate, since each different agency defines the same terms and procedures in its own way. One survey shows that only 10 percent of nuclear facility employees working with nuclear materials consider the “procedures” clearly defined at their facility; only 15 percent could identify specific security “procedures” and “instructions,” and 68 percent suggest that many of the existing procedures are obsolete.⁵¹ The problem is that a lack of clear instructions and procedures gives individual operators and technicians more room to interpret situations and to choose courses of action. The lack of standards also suggests that security does not receive the high priority it deserves.

Corruption and Crime

Corruption and crime are widespread in Russia, giving the nation a reputation as one of the most corrupt countries in the world. In one survey, for example, Russia is ranked eighty-second for its level of corruption (after Nicaragua and Zimbabwe).⁵² The low-paid employees at nuclear sites are no exception to the rule. The number of crimes in Russia increases every year. In the first quarter of 2002 more than 750,000 crimes were registered in Russia – mostly serious crimes.⁵³ During the Soviet time, Russia’s nuclear cities were isolated from the rest of the society and enjoyed a low incidence of crime. However, the situation changed for the worse after 1991. New information about these cities and a rather relaxed procedure for visitors who were Russian nationals attracted criminal elements to these territories. When these “closed cities” were given some significant tax privileges to raise money for their municipal budgets, criminal organizations managed to register front companies there. Security personnel at the nuclear facilities in these cities were unprepared to cope with increasing crime levels, either technically or psychologically, and consequently could be bribed.

Corruption is widespread among MINATOM employees. Not only have there been numerous scandals involving former Minister of Atomic Energy Yevgeny Adamov and his staff, but mid-level managers and operators have also been implicated. Russia’s Chamber of Audits reported in January 2002 that \$270 million in U.S. and European aid earmarked for improving storage sites for radioactive waste had been misappropriated. The media has also reported numerous cases in which employees have smuggled metals and scrap material. One of the most popular “smuggling businesses” is removing the precious metals from electronic systems, particularly high-tech hardware and nuclear-powered submarine propulsion systems, and selling them illicitly.

Nuclear security in Russia will depend on addressing the human factor – the conditions and environment in which personnel work, along with their motivation, training and attitudes. Unfortunately, there is no panacea, and there are no quick fixes. Strengthening nuclear security will require a long-term commitment to correcting the problems identified above. Addressing the

⁵¹ Koupriyanova, “Assessment of Effectiveness of US MPC&A Assistance to Russia,” 57-64.

⁵² Leonid Barinov, “Corruption in Russia Threatens National Interests,” *Nezavisimaya Gazeta*, September 7, 2001

⁵³ Dmitry Nikolaev, “Crimes Threaten State’s Security,” *Nezavisimaya Gazeta*, June 3, 2002.

human factors affecting nuclear security will be critical to sustain the progress already achieved with the help of the United States and other nations.

SECTION 4: HOW THE WEST CAN HELP RUSSIA DEVELOP A NUCLEAR SECURITY CULTURE

The United States and other nations have invested significant resources in a bid to enhance the security of nuclear facilities in Russia. Most of this funding has gone towards providing equipment and other hardware to improve material protection and security at Russian sites. As extensive evidence suggests, however, not nearly enough has been invested in cultivating among the personnel the accompanying security culture as an essential ingredient for effectively reducing nuclear danger. The reality is that nuclear-site personnel do not yet recognize the importance of strict security measures; do not fully comply with existing regulations; and either use their equipment improperly, neglect to maintain it, or fail to use it at all. Many key personnel are completely unfamiliar with, or greatly underestimate, the notion of proliferation threat. Therefore, reducing nuclear dangers in Russia will require not only technological innovation, but also the cultivation of knowledgeable, skilled, and motivated personnel trained to use modern equipment and adhere to the best practices.

A strategy to promote the nuclear security culture in Russia cannot and must not be the sole responsibility of Western donors. Unless the Russian government demonstrates its understanding and commitment to this endeavor, any efforts to this effect by the West will bring at best only limited results. No matter what joint strategy is developed, however, it must be clearly understood that Western experience and standards cannot be transplanted wholesale to Russia, which is undergoing rapid political and socioeconomic change. To be successful, this strategy must adequately reflect differences in work culture, traditions, and the unique role of the human factor in safeguarding nuclear materials in Russia.

There are at least five basic prerequisites for nurturing the nuclear security culture and appropriately shaping the human factor to which the West can contribute:

I. Promote a sincere commitment to fostering a robust security culture. The nation's political leadership and top executives in the nuclear industry must embrace the principles articulated here if Russia is to produce a workforce dedicated to safeguarding fissile materials. Senior government officials, up to and including the president and prime minister, must follow events relevant to fissile-material security and use their bully pulpit to gain public support for efforts aimed at enhancing security arrangements. For example, in the fall of 2000, Russia's Council of Ministers (cabinet) discussed MPC&A issues twice, in September and November. The underlying rationale for such high-level attention was the continued U.S. concern with the security of Russian nuclear facilities, and U.S. pressure on Russia to pay more attention to the issue. The grounds for U.S. concern were repeated cases of smuggling involving nuclear materials, the inability of Russian agencies to solve the problem of nuclear security and MPC&A given the lack of funding,⁵⁴ and inadequate interagency coordination. The cabinet discussed ways to improve the effectiveness of MPC&A systems, not only by addressing funding shortfalls but also by weighing structural and strategic changes in the program, interagency

⁵⁴ According to some Russian experts, the responsible agencies would need thirty times their current funding to do their work efficiently. Interview with Russian MPC&A experts, November 2000.

coordination, a redistribution of functions, changes in the legal foundation for nuclear regulations, and methods for implementing nuclear-security measures.

As a result of the high-level attention to the issues, both the public and the media became more aware of the dangers posed by inadequate security at the nation's nuclear sites and were encouraged to provide input in the ensuing debate. Moreover, in the report it presented at the cabinet meetings, MINATOM had to provide – for the first time in recent years – official information about actual cases or attempts of diversion and breaches of security.⁵⁵

Top leaders must demonstrate a continuing interest in resource allocation. The leadership can effectively promote the nuclear security culture by prioritizing relevant projects, promoting quality control, encouraging the dissemination of information and training, tapping additional funding sources, and in a host of other ways. Given the importance of safeguarding nuclear materials, Western leaders must engage their Russian counterparts in productive discussions and exchanges of information at the cabinet level or higher – circumventing bureaucratic politics. Oftentimes MINATOM's parochial interests and competition for scarce funding push the issues of nuclear-material security to the back burner. Personal attention to these issues by Russia's prime minister, to whom MINATOM reports by law, could be decisive.

The time has also come for MINATOM to phase out the Cold War policy of placing generals and other officers from the KGB (now FSB, the Federal Security Service) at key MPC&A-associated posts. Most of these people barely understand the technical side of the nuclear sector, especially its technologies and production processes.⁵⁶ The goals of fostering civic society in Russia, privatizing some components of the nuclear sector, and attracting investment will certainly require more transparency and less emphasis on the role of the secret services in routine supervision of nuclear materials. What the industry needs is Western assistance in establishing, training, and equipping its own departmental guards, as specified by the Federal Law on Departmental Guards and relevant government resolutions. The guards subordinate to MINATOM are likely to be more effectively integrated in facilities' overall teams, and thus to avoid dual loyalties, than is the case now.

⁵⁵ Briefing journalists about nuclear thefts at a press conference in September 2000, then-Deputy Minister of Atomic Energy Viacheslav Ivanov claimed that there had been twenty-three incidents of nuclear theft in Russia since 1991 (twenty-one in 1991-1995, and two from 1996-2000). However, the official statistics on the number of diversions vary: In 1998, Nikolai Redin, then the deputy head of MINATOM's Department for Security of Information, Facilities and Materials, stated that there had been about 30 cases of nuclear theft at MINATOM facilities between 1992 and 1995 (*ITAR-TASS*, October 28, 1998). In 1999, Victor Yerastov, head of the MC&A office at MINATOM's Department on Information, Materials and Facilities Security, noted that approximately 52 cases of radioactive and nuclear theft were known to have occurred by that date. *Yaderny Kontrol* 6, (November-December 1999).

⁵⁶ General Anatoliy Kotelnikov, who was appointed in July 2001 to the post of deputy minister in charge of security at MINATOM, admitted in an interview that his understanding of nuclear technology and the workings of the industry was very limited, *Zolotoye Koltzo*, July 2001.

II. Develop individual commitments through training and information exchange. The objective would be to work with top- and mid-level managers to instill personal responsibility, the determination to comply with safety regulations, and the ability to employ unorthodox solutions. Although possibly the best way to improve the motivation and performance of the workforce would be to significantly increase their salaries, this is an area where the West can provide little assistance, since they cannot simply underwrite sites' budgets. Rather, the West can help to improve the motivation of Russian workers using intangible incentives and stimuli. If the top managers at Russian facilities are more aware of the importance of MPC&A, they will be more flexible in allocating money for relevant projects and will elevate the priority of training their subordinates. Personnel with MPC&A responsibilities must be encouraged to develop a professional pride in what they are doing, because what they are doing is of national importance and global significance. Although the DOE is now paying more attention to security culture and has launched a program for improving it, the West can offer an additional interdisciplinary training package designed to change the mentality in a much wider context. Nongovernmental organizations can play a crucial role in training and information exchange.

First, the syllabus for these training programs must include the U.S. experience in and vision of security culture. If Russian personnel do not understand the U.S. mentality and approaches to nuclear security, it will be difficult to bolster the security culture in Russia and stimulate bilateral dialogue.

Second, training should not be limited to MPC&A only. It must include a broader variety of disciplines, ranging from nonproliferation to personnel management, professional psychology, defense conversion, and so forth. Security culture cannot be cultivated overnight, but can be nurtured using a carefully tailored training package. Such a package should include an overview of U.S.-Russian cooperation on matters of nonproliferation; threat assessment; vulnerability analysis; and case studies of smuggling and diversion.⁵⁷

III. Make instructions and regulations more user-friendly and understandable. The Soviet approach to developing instructions and regulations had numerous and serious flaws, which led to massive noncompliance, and even to a rejection of official directives. Russia has yet to remedy the problem of popular resistance to instructions and regulations. The West, however, is in a position to step in and help Russia adapt the U.S. and international experience to its own needs. The key problems related to instructions are:

- They are obsolete and poorly structured, as well as too general, formalized, and lengthy.

⁵⁷ Center for International Trade and Security has a limited experience in conducting training courses for high- and mid-level MINATOM officials through MINATOM's Atomenergo Institute of Professional Training, aimed at raising their awareness of the importance of nonproliferation and nuclear security.

- They contain a lot of unnecessary technical jargon, making them difficult to understand and blurring the guidance they provide.
- They were designed to describe technical minutiae, and not to provide solutions to the problems likely to be encountered by the workforce.
- They lack specific and detailed algorithms for handling fissile-material security and carrying out other critical tasks.

Instructions should be brief and should be solution- rather than process-oriented. They should lay out step-by-step solutions to problems in readily understandable, not overly technical language. Instructions should preferably be computer-based, with special software that can be used to identify and solve problems. Manuals and instructions can be tailored for personnel with different levels of experience, and can also be adapted to specific facilities. To enable these instructions to address specific problems, and to instill pride of ownership, the personnel who will carry out the instructions should be involved in preparing them. This would allow them to understand the rationale behind procedures that might otherwise seem unnecessary and redundant. Instruction-related briefings and training are also crucial. However, once the personnel have been briefed and agree with the instructions, strict adherence and implementation become the key element in assuring security. This should be more easily achieved, however, because the personnel have been co-opted into developing and understanding instructions and procedures.

Although there have been attempts in Russia to change and streamline the instructions, there are very few success stories. The United States can help by applying international and U.S. practices to the Russian realities, by helping train Russian personnel and managers in writing instructions and developing manuals and procedures, and by establishing “security culture islands” – model facilities that boast an improved security culture, and whose personnel would be rewarded in tangible and intangible ways.

IV. Change how nuclear-site personnel perceive the threat. A major difference between the U.S. and Russian approaches to nuclear security is the U.S. emphasis on insider theft or diversion, and the Russian reluctance to accept this view of the threat. For decades, the Russian nuclear security system has sought to deflect a potential outside act of sabotage, while relying heavily on the KGB to provide internal personnel screening and security. The dissolution of the Soviet Union and drastically different political and economic conditions created entirely new challenges. The current managerial and administrative personnel in the Russia’s nuclear sector have been reluctant to accept this view.

One of the key tasks that will help raise workers’ awareness of proliferation risks will be to explain, using concrete examples, that an insider diversion is far more plausible than an outside attack on a facility. Once the trainees embrace this view, following the letter of established procedures will become the critical element in minimizing this threat. But given Russia’s recent experiences with terrorism and the widely publicized cases of military personnel essentially supplying potential terrorists with weaponry and special equipment in exchange for money – an egregious example of an insider job – getting the point across to nuclear managers may not be such a daunting task after all.

Another tool worth trying is to help introduce whistle-blowing practices at nuclear sites, with appropriate transparency and awards. It would be a traumatic experience for the Russian personnel given the painful historical memories from the wide-spread pattern during the Soviet period of sending anonymous letters to the KGB reporting “subversive” activities of the fellow citizens. However, a carefully designed and well-thought out campaign to introduce the whistle-blowing system can reinforce procedural compliance at nuclear sites.

V. Improve the testing and recruitment procedure. One serious obstacle to the implementation of an effective security culture is inadequate personnel testing and recruitment. Training does not guarantee the implementation of procedures if personnel do not fit the position from a psychological standpoint. Tests of personnel reliability should be conducted at different stages in the worker’s education and career and be differentiated for a variety of groups. Tests should be initially conducted before students enter specialized institutes to acquire the specialized knowledge and skills required for work in the nuclear industry. The aim of these tests should be to find out whether students would be reliable and whether their psychological characteristics fit the requirements of the job. There should be recruitment tests for different kinds of employees (operators, low-level managers, mid-level managers, top managers, guards) in accordance with their functions. Selective tests (psychological, drug-use, etc.) should also be conducted regularly.

The United States must share both the hardware and the software required for such testing. Requirements for testing exist in Russia’s nuclear sector, but the tests are not conducted on a regular basis, and their methodology leaves much to be desired. The U.S. Department of Defense provided polygraphs to Russia’s Strategic Rocket Forces – making for a clear success story. Russia’s top military officials bestowed high praise on this program, which dramatically enhances the reliability of nuclear-weapons personnel. This positive experience can be applied to MPC&A operators and other personnel in the nuclear sector.

The G-8 Global Partnership meeting of June 2002 recognized an urgent need to devote greater resources to safeguarding nuclear materials in Russia. There are grounds to believe that Western contributors will follow through on this insight as part of their broader effort to enhance security standards. The participation of major industrial nations with developed nuclear industries would provide different examples of how to cope with the human factor, promoting innovative and effective solutions. International efforts to generate a nuclear security culture in Russia will provide a fund of valuable lessons to be learned by other countries with emerging nuclear sectors. With so many risks involved, there is hardly a reasonable limit of security beyond which further strengthening and promoting cannot be justified.