

# Policy Analysis

No. 571

June 14, 2006

Routing

## *Reappraising Nuclear Security Strategy*

by Rensselaer Lee

### Executive Summary

The danger posed by Russia's inadequately secured stocks of nuclear weapons and fissile material is a major national security concern for the United States. Various cooperative U.S.-Russian programs aimed at securing nuclear material, weapons, and design intelligence have been mounted since the 1990s, but clever and determined adversaries may be able to circumvent or defeat the defenses that the United States and its partners are attempting to put in place. U.S. programs are by their nature reactive: they have long time horizons; they focus preeminently on the supply side of the problem; and they face serious technological limitations. Russia's imperfect commitment to nonproliferation also undermines the effectiveness of U.S. nonproliferation efforts.

There are no easy ways to close the nuclear proliferation window. A proactive and intelligence-based nuclear security policy, one that

complements existing programs while enabling authorities to do a better job of targeting and preventing proliferation damage, is needed to counter this threat. Various measures to strengthen nuclear security policy could include the use of "vulnerability profiles" of each Russian facility that handles weapons-usable nuclear materials and better collaboration with Russian and other former Soviet security organizations. A comprehensive nuclear security strategy must also focus more attention and resources on the demand side of the proliferation equation. The United States cannot conduct nonproliferation work effectively without reference to adversaries' programs for weapons of mass destruction and procurement aims. Ideally, U.S. policy should embrace the concept of demand reduction—influencing the motivations of adversary states and subnational groups so as to prevent the spread of nuclear weapons capability.

---

*Rensselaer Lee is a senior fellow at the Foreign Policy Research Institute in Philadelphia and president of Global Advisory Services in McLean, Virginia. He is the author of Smuggling Armageddon: The Nuclear Black Market in the Former Soviet Union and Europe (St. Martin's, 1998).*

**Various cooperative U.S.-Russian programs aimed at securing nuclear material, weapons, and design intelligence have been mounted since the 1990s, but such efforts fall short of an effective strategy for proliferation prevention.**

## **Introduction**

In the years after the collapse of the Soviet Union, the apparent proliferation danger posed by Russia's poorly secured stocks of nuclear weapons and fissile material (colloquially "loose nukes") emerged as a major national security concern for the United States. The evident nuclear ambitions of hostile states such as Iran and North Korea and the terrifying prospect that al-Qaeda could acquire nuclear weapons have accentuated U.S. proliferation fears. Various cooperative U.S.-Russian programs aimed at securing nuclear material, weapons, and design intelligence have been mounted since the 1990s, but such efforts fall short of an effective strategy for proliferation prevention. Clever and determined adversaries may be able to circumvent or defeat the defenses that the United States and its partners are attempting to put in place. Inadequate funding may be part of the problem, but there are other, more fundamental problems, including the essentially reactive nature of U.S. programs, their long time horizon, their preeminently supply-side focus, and their technological limitations. An additional constraint is what some observers view as Russia's imperfect commitment to nonproliferation, reflected in its cozy nuclear relations with Iran as well as a tendency of some Russian officials to downplay the threat of nuclear theft.

There are no easy ways to close the proliferation window in Russia and the other states that were once part of the Soviet Union. This paper recommends a more proactive and intelligence-based nuclear security policy, one complementing existing programs but enabling authorities better to target potential adversaries and prevent proliferation damage.

## **Evolution of U.S. Programs**

The conceptual architecture of U.S. nonproliferation policy originated in the Soviet Nuclear Threat Reduction Act of 1991, also known as the Nunn-Lugar act after its main

sponsors, Sens. Sam Nunn (D-GA) and Richard Lugar (R-IN). Nunn-Lugar, drafted as the USSR was disintegrating, noted that the "profound changes" under way there posed several types of threats: the dispersal of nuclear arms among Soviet successor states; the seizure, theft, sale, or use of nuclear weapons and their components; and the transfer of weapons and related components and expertise outside the territory of the Soviet Union. The legislation's main programmatic focus was to secure and destroy nuclear and chemical weapons and to establish "verifiable safeguards" against their proliferation; it appropriated \$400 million for that purpose and designated the Department of Defense as the "executive agent" to spend those funds.<sup>1</sup>

Over the years, the original Nunn-Lugar concept expanded to include protection of fissile materials, border and cargo monitoring to interdict nuclear smuggling, reduction of highly enriched uranium (HEU) and plutonium stockpiles, and various programs to rebuild or redirect the economic potential of the former Soviet nuclear complex. New bureaucratic players—the Department of Energy and the Department of State—came to share responsibility for the enlarged nonproliferation effort. DOE funds and U.S. national weapons laboratories implement security upgrades for fissile materials, an effort now under way at more than 50 former Soviet civilian and military sites. Programs sponsored by DOE and DOD are introducing new protective regimes at some Russian nuclear warhead sites. DOE, DOD, and State all maintain different programs to counter nuclear smuggling. DOE and State provide funding to stabilize employment for displaced nuclear workers and to prevent "brain drain." As of the middle of this decade, the United States was spending almost \$1 billion a year on overseas nuclear security and related disarmament projects.<sup>2</sup> Most of those funds were directed toward Russia and other newly independent states, but some recent DOE initiatives—such as installation of radiation detectors at major shipping hubs ("megaports") and removal of HEU from

research reactor sites deemed vulnerable to theft—reach much farther afield.

### Measuring Effectiveness

Considerable dedication, ingenuity, and scientific expertise have gone into crafting this welter of programs. Investment in them has been substantial. DOE calculates that it spent \$1.5 billion from 1993 to early 2005 on its Material Protection, Control and Accounting program to secure fissile materials at the (mostly Russian) sites where they are stored. A financial review concluded that the average cost of securing a single kilogram of such material amounted to \$5,300 in fiscal year 2005.<sup>3</sup> Likewise, outlays for nuclear interdiction, export control, and anti-brain-drain initiatives by DOE and other agencies have exceeded \$1 billion since 1993.<sup>4</sup>

Whether these efforts can successfully prevent the migration of nuclear material and expertise from Russia and the former Soviet republics (or have prevented them) is an open question. U.S. agencies tend to rely on metrics of performance such as tons of fissile materials or numbers of warheads protected by advanced safeguards, border posts equipped with advanced radiation monitors, or weapons scientists relocated to civilian jobs. Measures of effectiveness, such as major diversion threats defeated by the new security features, are harder to devise in the Russian context and are infrequently used by U.S. nuclear managers or by nongovernmental organizations (NGOs) that track these programs.

To be sure, the consensus view holds that nuclear security conditions in Russia have improved in recent years and infusions of U.S. technology and equipment have played some role in that change. There are some encouraging signs that validate this consensus. Quantities of HEU and plutonium being offered for sale internationally, never voluminous, have diminished dramatically; in fact, no such material has been reported seized since the early to mid-1990s. Similarly, Russian atomic energy officials claim that cases of attempted thefts of weapons-usable material have been declining in Russia. A National

Academy of Sciences report from 2005 cautiously concludes that “upgraded physical protection and accounting systems . . . may have contributed to the reduced number of attempts to steal material.”<sup>5</sup>

Nevertheless, other significant factors, unrelated to Nunn-Lugar, also may account for these trends. For example, the obvious improving performance of the Russian economy—which has grown at a pace of 6.5 percent per year since 1998 and generated a federal budget surplus of \$8.1 billion—has had a positive effect on the livelihood of nuclear workers. That is significant because desperate economic conditions at Russia’s nuclear enterprises were a prime proliferation risk factor in the 1990s. By 2002 the average monthly salary at nuclear research and development facilities was \$209, well in excess of the Russian average of about \$146. At one premier nuclear weapons design laboratory in Snezhinsk (Chelyabinsk-70) salaries reached a relatively princely \$262 in early 2003.<sup>6</sup> By contrast, salaries at nuclear facilities (excluding the power industry) had hovered well below the national average for much of the 1990s.<sup>7</sup> Also, workers are now usually paid on time. In 1996 the director of the Snezhinsk center, Vladimir Nechai, committed suicide, allegedly because of emotional stress relating to Snezhinsk’s inability to pay its workforce for more than five months.<sup>8</sup> The rebounding economy may have reduced economic incentives for insiders to steal and sell dangerous materials, although other motivations such as ideology might inspire would-be nuclear thieves.

A second factor relates to the tightening of central government control over the nuclear complex via Russian security organs, most notably the Federal Security Service (FSB). Sources agree that the FSB has become “omnipresent” in the nuclear sector, restricting access to Russia’s formerly secret cities and to nuclear sites within them as well as increasing its formal presence within the enterprises themselves. (According to one article, FSB representatives often preside as “deputy directors of security” within the enterprises.)<sup>9</sup> U.S. nuclear lab personnel tend

**The rebounding Russian economy may have reduced economic incentives for insiders to steal and sell dangerous materials.**

**Although Russia's nuclear security posture has changed for the better, it remains less than fully mature, at least by U.S. standards.**

to view the heavy hand of the FSB as an impediment to the progress of the MPC&A program. "They tell us who can visit, how many, where, when, and for how long," said one lab official.<sup>10</sup>

Yet it is possible to view the FSB controls in a more positive light. Russian authorities told a visiting National Academy of Sciences delegation in 2003 that three unsuccessful attempts to steal fissile material had occurred since 1996, and each had been foiled by the FSB.<sup>11</sup> One episode is widely believed to have occurred in 1998 at Snezhinsk (Chelyabinsk-70) where work to introduce MPC&A systems had been under way since 1995.<sup>12</sup> Russia obviously has an interest in extolling the virtues of its security forces, and cases in which thefts have been defeated or aborted at the source may owe just as much to the vigilance of human agents as to U.S.-installed technological safeguards. By the same token, MPC&A can serve as a check on possible corruption or incompetence within the security services, so human and technical components of a protective regime ideally should function in tandem.

Finally, although Russia's nuclear security posture has changed for the better, it remains less than fully mature, at least by U.S. standards. The NAS study from 2005 observed that, although reported incidents of attempted theft had been declining in Russia, "there is no basis for judging the actual number of unreported attempts or successful thefts."<sup>13</sup> U.S. MPC&A experts with access to Russian sites generally have not attempted to collect intelligence about current or past diversion episodes in Russia's nuclear complex. An apparent lack of activity may simply mean that prospective thieves and smugglers have become more proficient at neutralizing the new technological controls and circumventing the security forces. Furthermore, as Russia seeks expanded markets for legitimate nuclear sales abroad (in Iran, for instance), nuclear insiders are more likely today than in the past to have developed international contacts and relationships enabling them to connect with potential customers for illicit nuclear goods. We cannot conclude, there-

fore, that the threat of criminal nuclear proliferation has diminished, even while the visible signs seem encouraging.

### **Assessing the Threat**

Although fears of catastrophic terrorism have grown in recent years, the shape of the nuclear proliferation threat posed by leaky Russian stockpiles remains ill-defined and somewhat hypothetical. Illicit sellers and buyers of nuclear wares are assumed to exist, but hard evidence of a true black market for such items is sparse. Judging from seizure data, little nuclear material of significance and no nuclear warheads circulate in international smuggling channels. Only about 20 of the hundreds of trafficking incidents recorded since the early 1990s have featured HEU or plutonium, the explosive ingredients of nuclear weapons.<sup>14</sup> Moreover, the total amount seized did not add up to enough to make a single atomic bomb. More to the point, a General Accounting Office study found that none of the cases in which such material was proffered appeared to be "part of an organized criminal or terrorist activity or organization." Indeed, evidence of connection to any bona fide buyer—whether a state seeking nuclear weapons, a terrorist agent, or a criminal entity—was lacking. Most of the episodes in question were sting operations initiated by law enforcement or intelligence agencies, effectively creating an artificial market; in others perpetrators were trapped by security forces while looking for a buyer.<sup>15</sup>

Nonetheless, observed data from seizures and associated arrests may be unrepresentative of the wider universe of illegal nuclear deals, including sophisticated schemes that escape detection. As with other illicit commodities—drugs, for example—what is captured is just a fraction of what is available for sale in the international marketplace. Underscoring this point, then-CIA director Porter Goss informed Congress in December 2004 that "we [the intelligence community] assess that undetected smuggling has occurred and we are concerned about the total amount of material that could have been diverted or stolen in the past 13 years."<sup>16</sup> Significant proliferation episodes may

go unreported. Observers such as William Potter, director of the Center for Nonproliferation Studies at the Monterey Institute of International Studies, have commented on the failure of the former Soviet republics to report nuclear smuggling incidents for inclusion in the International Atomic Energy Agency's trafficking data base. He concludes that "we cannot exclude the possibility—I would say probability—that additional diversion incidents have occurred but have been concealed by [authorities in these states]."<sup>17</sup>

Moreover, diversion events that authorities admit to typically involve opportunistic thefts of small amounts of material by solitary nuclear workers. The perpetrators then search for a buyer, often with the help of local petty criminals, who in turn are apprehended by police. Yet hints that this may inaccurately reflect smuggling realities have surfaced in Russian media. For example, in 1998 Russia's FSB reportedly foiled an attempt by "staff members" of a Chelyabinsk nuclear facility (by all indications Chelyabinsk-70) to steal 18.5 kilograms of HEU, almost enough for an atomic bomb. The episode was later confirmed by a spokesman for Russia's atomic energy ministry.<sup>18</sup> The reports did not divulge where the material was headed, or who the prospective customers were. Also unclear is whether the theft was an isolated case or a single failure in a string of successful diversions by facility insiders.

Likewise, on the demand side, the elusiveness of buyers in known nuclear smuggling cases should not be cause for complacency. We can be fairly certain from intelligence reporting, media accounts, and other sources that a handful of nation-states and subnational groups are "in the market" for stolen nuclear materials. States are likely to place a premium on self-reliance in nuclear development—witness Iran's high-profile enrichment program—but that does not preclude a state from shopping for fissile materials to shorten the time frame for building a bomb. Over the years, Iran, Iraq, and North Korea reportedly have tried to purchase materials for a nuclear bomb, though details are murky. For example,

a 2001 DOE report states that "Iran, among others, has tried to exploit Russia's nuclear security problems by attempting to acquire fissile material."<sup>19</sup> Iran's wide-ranging cooperation agreements with Russia in the nuclear sphere may have been a vehicle for those forays, though there is no direct evidence that such is the case.

Among nonstate actors, al-Qaeda is believed to have sought HEU (apparently unsuccessfully) in various venues—Africa, Western Europe, and the former Soviet Union—since the early 1990s. Most experts agree that a reasonably well funded terrorist group probably could muster the expertise and facilities needed to fashion a rudimentary nuclear device but that the main sticking point is getting the requisite quantities of nuclear material.<sup>20</sup> Unlike nation-states, terrorists cannot leverage official contacts and exchanges in the nuclear realm to advance their military procurement objectives. Their best option probably would be to form a liaison with a local criminal or ideological group that has connections to nuclear facilities and cross-border smuggling capabilities. Reports that al-Qaeda has sought assistance from Chechen criminals and the Islamic Movement of Uzbekistan in its pursuit of a nuclear capability would seem to corroborate this pattern. For example, a November 1998 report in the Paris-based Arabic newspaper *Al-Watan Al-Arabi* asserts that al-Qaeda concluded a deal with the "Chechen mafia" to buy 20 tactical nuclear weapons for \$30 million and two tons of Afghan opium. Most observers doubt that the transaction actually took place or that the Chechens have any such weapons to sell. Yet contacts between al-Qaeda and the Chechen resistance are extensive, and discussions about acquiring nuclear weapons or materials could well have occurred. According to terrorism expert Michael Scheuer, former head of the Osama bin Laden unit at the CIA, the account has "the ring of plausibility, perhaps even echoes of truth."<sup>21</sup>

The prospect that terrorist groups could obtain finished nuclear weapons from sources in Russia or elsewhere is indeed frightening.

**Former Soviet republics have failed to report nuclear smuggling incidents for inclusion in the International Atomic Energy Agency's trafficking data base.**

**The notorious marketing network established by Pakistani scientist A. Q. Khan demonstrates that a functioning nuclear black market can persist for years without being detected by international watchdogs.**

To be sure, a general consensus exists among U.S. nuclear scientists and intelligence experts that Russian nuclear weapons are substantially more secure than are their fissile material counterparts. There is no evidence that intact nuclear weapons have been stolen, or have gone missing. Alexander Lebed's well-publicized assertions of missing "suitcase weapons" have been denied by officials in Russia, the IAEA, and the United States.<sup>22</sup> Even if Lebed's claims were true, such weapons would not have been armed. In the case of an intact weapon, a terrorist's main challenge would be to bypass the multiple arming and fail-safe codes (permissive action links or PALs) designed to prevent detonation by unauthorized persons. Nevertheless, theft of a nuclear weapon remains a theoretical possibility, and some specialists believe that terrorists, rather than try to circumvent the PALs, would simply cut open the weapon casing and fashion their own bomb from the component parts.<sup>23</sup>

Furthermore, purveyors of strategic nuclear goods may converge with end users or their representatives in ways not readily apparent to Western intelligence or security services. The prime modern example of a clandestine supply chain or shadow market in the nuclear realm is the notorious marketing network established by Pakistani scientist A. Q. Khan, the father of Pakistan's nuclear bomb. For several years beginning in the late 1980s, Khan sold key components of a nuclear weapons program—mainly uranium enrichment technology and hardware—to Iran, North Korea, and Libya. Libya, which later renounced nuclear weapons, also received from Khan blueprints for building a Chinese-type implosion nuclear device (similar in design to Pakistan's). Khan's operation finally unraveled in early 2004 but not before significant transfers of centrifuge designs and equipment had already occurred.<sup>24</sup> The lesson here is that a functioning nuclear black market can persist for years without being detected by international watchdogs. Indeed, a Khan-type network dedicated to covert sales of fissile materials and weapons know-how conceivably could take shape on the territory of the former

Soviet Union, managed by corrupt elements within the nuclear establishments of Russia and other newly independent states.

## Washington's Response

Washington's efforts to counter these threats have focused largely on strengthening security at nuclear facilities, deploying technological monitoring equipment at key border crossings, and checking the dissemination of militarily significant nuclear know-how. Those efforts are comprehensive in scope, yet their programmatic components add up to just a partial defense against the spread of nuclear weapons capability. U.S. programs suffer from technical and physical limitations that clever adversaries can easily exploit. Finally, cases of deliberate "state-sponsored" proliferation would appear to be beyond the capability of the new systems to prevent, since the programs and systems are based on the presumption that states wish to keep their nuclear assets under control. A very different set of tools is needed to deal with deliberate weapons or materials transfers. Diplomacy, deterrence, and economic sanctions are appropriate tools for modifying a country's behavior in such circumstances.

Limitations are apparent in DOE's MPC&A program, which many people consider the nation's first line of defense against the proliferation threat posed by insecure Russian stockpiles. Sources of strategic nuclear items "are relatively few in number compared with the many potential points of transit across national borders and are protected by state-run security infrastructures," a 2002 report by the National Academy of Sciences concluded.<sup>25</sup> Nonproliferation specialists such as Harvard's Graham Allison believe it possible to lock down all weapons and fissile material to a Fort Knox-type gold standard of infallibility to the point where leakage or disappearances of significance are impossible.<sup>26</sup>

Yet such a gold standard may be impractical, given the large number of facilities that house nuclear material.<sup>27</sup> Another major

impediment is the complexity and unpredictability of the human element. Nonproliferation advocates increasingly emphasize the cultural determinants of technology transfer in the nuclear realm. As Laura Holgate, vice-president of the Nuclear Threat Initiative, notes, “The perceptions, judgments and actions of human beings, individually and in groups, are what make the difference in nuclear security.” Reports from Russian facilities of vault doors propped open and insouciant guards who “shut down alarm systems to avoid the annoyance of frequent false alarms” seem to exemplify the weak points of Russia’s nuclear security culture.<sup>28</sup>

Even when used properly, the new hardware and software being deployed are not fail-safe. The systems probably are effective against opportunistic theft attempts, which were fairly common in Russia in the early to mid-1990s. But today’s main threat at the facility level comes, not from disgruntled solo players, but from conspiracies of well-placed insiders able to shut down alarms, bribe guards, and alter relevant paperwork. Russian and U.S. experts agree that at most Russian nuclear enterprises the cooperation of just four to five individuals is required to pull off a successful diversion scheme.<sup>29</sup> Thefts organized by senior managers are probably the most serious threat. Managers know precisely the sequence of steps required to remove the desired material while minimizing the risk of detection. In a well-publicized case at the Mayak Production Association in Chelyabinsk, the manager of Mayak’s isotope separation plant was convicted on several counts of exporting a valuable nonnuclear substance (iridium-192), using false customs documentation.<sup>30</sup> Managers could just as easily create appropriate paperwork to conceal a more serious diversion—substituting HEU in containers marked as cesium-137, for example.

To be fair, the MPC&A program does include consideration of the human factor in the nuclear workplace. Recent U.S. legislation, the Bob Stump National Defense Authorization Act of 2003, has established a five-year time frame for transferring all

MPC&A responsibilities to Russia by the year 2013. Accordingly, DOE has asked for almost \$50 million in FY07, nearly twice the FY06 level, to support a National Program and Sustainability Initiative under MPC&A that incorporates aspects of the security culture concept including management plans, operating procedures, and human resource programs.<sup>31</sup> But training nuclear workers to obey norms and follow established procedures is not quite the same as deterring corrupt acts by criminally inclined insiders, although admittedly some overlap exists.

The various U.S. programs for technological monitoring of people and cargo at key border and transit points face even more daunting challenges. Russia’s 12,500-mile border with its neighbors is simply too long to monitor effectively. Smugglers won’t necessarily opt to move their wares through customs posts equipped with radiation detectors, and detectors themselves are subject to all the vulnerabilities associated with corruption: they can be turned off, bypassed, or simply ignored. A further significant problem is that most of the equipment being installed at borders is not sufficiently sensitive to detect well-shielded fissile material. This is especially the case with HEU, which has a weak neutron signature and is not very radioactive.<sup>32</sup> HEU is the material most likely to be sought by terrorists, because a gun-type device using substantial quantities of that material is easier to make than an implosion device using either uranium or plutonium. In short, complete border integrity probably is not an achievable goal. As Harvard’s Matthew Bunn argues, “Once stolen material is removed from authorized control, much of the battle is already lost—finding stolen material within a country, or detecting and interdicting its passage across borders, are herculean tasks, in most cases only practicable if good intelligence and police work tells officials where to look.”<sup>33</sup>

U.S. nonproliferation work in Russia also aims to prevent the dissemination of nuclear intelligence by creating economic lifeline projects for underemployed or displaced nuclear

**Today’s main threat at the facility level comes from conspiracies of well-placed insiders able to shut down alarms, bribe guards, and alter relevant paperwork.**

**Our non-proliferation toolbox simply is not designed to prevent situations in which states as a matter of policy, or high-ranking government officials, deliberately transfer strategic nuclear goods to third parties.**

personnel. Types of projects range from short-term grants and subsidies for weapons personnel to collaborative research projects with U.S. weapons labs to partnerships with private industry to develop commercially viable technologies. Many scientists in nuclear and other WMD fields have benefited from programs such as DOE's Global Initiatives for Proliferation Prevention and the State Department's International Science and Technology Center; some have obtained long-term civilian employment as a result. In addition, the business of installing MPC&A safeguards and developing related technologies has itself created jobs for some indeterminate number of nuclear experts and workers.

Yet the overall impact of such efforts remains to be seen. Military-scientific knowledge is difficult to contain under the best of circumstances. Recall that America could not keep its own closely guarded nuclear secrets from gravitating to the Soviet Union in the 1940s and (probably) to China in the 1990s. These days scientists in their home bases in Russia could transmit nuclear or ballistic missile designs by fax or e-mail. Also, supply-side leakage of nuclear intelligence or material may reflect complex motivations. Economic uncertainty and the need to make ends meet are factors, but so are greed, resentment, and ideological conviction. Recall the case of British nuclear physicist and Soviet master spy Klaus Fuchs, who worked at the Manhattan Project and later at Los Alamos. Fuchs hardly fit the profile of an unemployed or economically desperate scientist.

Finally, it should also be emphasized that our nonproliferation toolbox simply is not designed to prevent situations in which states as a matter of policy, or high-ranking government officials, deliberately transfer strategic nuclear goods to third parties. The above-mentioned underground network organized by Pakistani scientist A. Q. Khan is the prime example of a senior government official willfully circumventing state policy. Most observers believe that Khan's businesses emphasized sales of technology, although an Iranian exile group—the National Council of

Resistance of Iran—claims that the network delivered an undetermined quantity of HEU to Iran in 2001.<sup>34</sup> In a related development, the Pakistani Atomic Energy Commission took out a full-page advertisement in a Pakistani newspaper in July 2000 (under the rubric of the Ministry of Commerce) offering plutonium, enriched uranium, and other nuclear materials for export. (The offer was rescinded under U.S. pressure.)<sup>35</sup> In yet another case, Russia's cozy nuclear relationship with Iran epitomized by, but not limited to, the construction of a 1,000-MW nuclear power plant at Bushehr, is a continuing source of proliferation concern. Some U.S. officials believe that Iran leverages the relationship to expand contacts with Russia's nuclear entities and to acquire information and materials directly applicable to nuclear weapons programs.<sup>36</sup> The extent of such covert transfers is not known. Yet the temporary assignment of thousands of Russian specialists to Iran in connection with the Bushehr facility constitutes a brain drain of sorts and therefore contradicts at least the spirit of U.S. nonproliferation programs with Russia.

## **Reviewing Progress**

U.S. nonproliferation projects in Russia and elsewhere have uncomfortably long time frames. For example, goals projected in DOE's 2007 budget include securing 195 Russian buildings that contain nuclear material by 2008, equipping 350 border crossings and 64 megaports (major international shipping hubs) by 2013, and creating 11,000 "long-term" private-sector jobs for displaced weapons scientists by 2019. As of the end of FY05, 86 percent of the targeted buildings were secured by some form of MPC&A, 37 percent of the needed jobs were created, and about a quarter of the strategic crossings and only four megaports had been outfitted with radiation monitors.<sup>37</sup> The sluggish progress of MPC&A and other threat reduction efforts can be explained by such factors as funding constraints, bureaucratic inertia,



disputes over access to sensitive facilities, and inadequate Russian commitment to technological modernization of nuclear protective regimes.

Yet as those programs drag on, efforts by terrorists to acquire a nuclear capability represent a consequential and near-term threat, creating an opportunity for prospective nuclear thieves and smugglers. There is no reason to believe that our adversaries will stand idly by until all Russian facilities are MPC&A-ready or until complete border integrity is achieved before orchestrating a major diversion event. U.S. programs have an intrinsic threat-reduction value, but their strategic justification and the payoff for U.S. security interests recede with the passage of time.

Indeed, at this point—already 15 years after the collapse of the USSR—there is a danger that our programs amount to locking the proverbial barn door after some of the horses have escaped. Consider the circumstances in Russia during much of the 1990s—a period of deep malaise in the Russian nuclear complex. The loss of orders for nuclear goods, a deteriorating security climate, unpaid wages, a fraying social safety net, and a spreading ethos of corruption put much of the nuclear stockpile at risk. As Sen. Sam Nunn told a Senate hearing in 1995, the collapse of the USSR “let loose a vast potential supermarket for nuclear weapons, weapons-grade uranium and plutonium, and equally deadly chemical or biological weapons.”<sup>38</sup> Even allowing for some hyping of the threat, it would be a miracle indeed if no leakage of significance took place during this period.

Admittedly, the visible machinations of the nuclear black market provide little clue as to what might have happened. Nuclear smugglers captured in western Europe in the mid-1990s indicated to authorities that significant quantities of HEU and plutonium—enough for several bombs—had already escaped government control and were available for sale.<sup>39</sup> Where such vagabond material, if it exists, is now is anybody’s guess; it could be buried somewhere in a birch forest, stashed in someone’s refrigerator, circling the globe looking for

potential buyers, or hidden in a cave in remote eastern Afghanistan. Troubling reports have surfaced of corrupt practices by certain nuclear facilities during the Yeltsin administration, including “off the books” processing of uranium for private commercial clients and altered paperwork to conceal substitution of dangerous substances in legal radioactive shipments.<sup>40</sup> Hence, the possibility that America’s adversaries already have obtained some of what they need to make a nuclear weapon should not be ruled out. At the same time, accelerating the timetable for key U.S. projects in Russia and elsewhere can reduce the threat of further proliferation damage.

## The Road Ahead

Securing fissile material at the source should be the most immediate priority, since it offers greater promise of success than preventing cross-border trafficking of such material or clandestine transfers of nuclear weapons expertise. As far as MPC&A is concerned, the endgame appears to be in sight. DOE plans to get out of the business of securing fissile material and warhead storage sites by the end of FY08 and FY09, respectively. In 2013, under current U.S. legislation, full responsibility for sustaining the new systems is supposed to be transferred to Russia. The prospect of transition to Russian control is fraught with uncertainties, however. For example, the NAS study from 2005 claims that Russia has failed to take “adequate steps” to provide financial support for MPC&A activities; it also concludes that Russian officials and experts “do not share the high level of concern regarding the vulnerability to theft of nuclear material from facilities that is held by U.S. experts.”<sup>41</sup> The investments that Russia has made in MPC&A tend to focus on perimeter defenses—to prevent terrorist break-ins and sabotage of nuclear facilities—rather than on accounting and inventory controls, which are designed largely to prevent insider theft. Moscow’s main threat reduction priorities may lie elsewhere, such as in dismantling nuclear sub-

**There is a danger that our programs amount to locking the proverbial barn door after some of the horses have escaped. At the same time, accelerating the timetable for key U.S. projects in Russia and elsewhere can reduce the threat of further proliferation damage.**

**Washington’s approach to nonproliferation is too narrowly defined, emphasizing introduction of modern technology. What is also needed is a proactive and intelligence-based nuclear security policy that would complement these systems.**

marines and preventing radiological terrorism.<sup>42</sup> Furthermore, competing social and developmental needs—according to the CIA, an estimated 17.8 percent of the population in Russia live below the poverty line<sup>43</sup>—will place major demands on the state budget. In sum, despite the influx of substantial revenues from the sale of oil, Russia’s willingness to take on full financial responsibility for maintaining and enhancing MPC&A is viewed by some observers as problematic, at least in the near term. To address this potential shortfall the NAS study recommends creating a \$500 million MPC&A “indigenization” fund, supported by the United States, Russia, and other G-8 countries. The United States would contribute \$200 million, the other G-8 countries would contribute another \$200 million, and Russia would contribute the remaining \$100 million. The fund would be doled out to Russia over a 10-year period.<sup>44</sup>

Some new funding is doubtless desirable and could enhance Russia’s interest in supporting MPC&A over the longer term. However, the United States and Russia need to address the more basic shortcomings of MPC&A and related cooperative programs. Washington’s approach to nonproliferation is too narrowly defined, emphasizing introduction of modern technology (albeit with some attention now paid to “nuclear security culture” in deploying new technological safeguards). Moreover, some Russians are skeptical of the utility of modern security systems, as noted above. What is also needed is a proactive and intelligence-based nuclear security policy that would complement these systems. The general aim would be to provide early warning of illegal nuclear “deals in the making” and to reduce the risk of consequential proliferation episodes. Several recommendations for implementing such a policy are outlined below.

First, it might be useful to construct a “vulnerability profile” of each Russian facility that stores, produces, or works with weapons-usable nuclear materials. Such a profile could be based on such factors as economic conditions and wage scales, presence of organized crime or Islamic extremist

groups in the neighborhood, past histories of thefts or theft attempts, accessibility to foreign visitors, and frequency of travel abroad by enterprise scientists. It should also be possible, on the basis of a cooperative U.S.-Russian effort, to gauge the susceptibility of the nuclear workforce to bribes or blackmail and employees’ propensity to engage in corrupt or disloyal conduct. Illicit drug use, gambling habits, major medical expenses, and conspicuous consumption unrelated to income are obvious warning signs—weaknesses that could be exploited by an adversary seeking access to strategic nuclear wares

In the same vein, human reliability systems, if intelligently deployed, can capture evidence of corrupt or high-risk behavior. Certain pre- or postemployment screening techniques—polygraphs, psychological testing, and investigation of bank records—can be powerful predictive tools. They also can yield information on prior thefts, possibly leading to recovery of stolen material that perpetrators have not yet had the chance to export from Russia. Another technique might be the introduction of motion-detection cameras for remote surveillance of nuclear storage areas and guard posts. The data feed from the cameras could be transmitted to review stations inside and outside the facility, providing an additional measure of security against insider thefts. Some of these personnel reliability concepts are now being implemented (the Russian military reportedly has introduced polygraph examinations at weapons storage sites) but not yet on the scale contemplated here.<sup>45</sup> A comprehensive human reliability system for nuclear custodians might also be extended to persons charged with interdiction responsibilities, such as customs officials and police. Judging from U.S. experience in screening people for high-security jobs, such a system would be expensive to implement, doubtless requiring additional infusions of U.S. funds for nonproliferation work in Russia.

Second, a comprehensive nuclear security strategy must go beyond containment, or at least broaden the definition of it. Specifically,

it should focus more attention and resources on the demand side of the proliferation equation. Better intelligence is a vital component of such a strategy, complementing the essentially reactive and stationary risk management system that the United States is implementing in Russia and elsewhere. Much more needs to be known about adversaries' procurement chains inside and outside the former Soviet republics: how those chains are organized and financed, what front companies and other intermediaries are used, who their inside collaborators are, and what smuggling pipelines have been established. Law enforcement sting operations in which operatives pose as purveyors of HEU or plutonium could play a big role in fleshing out buyer and end-user networks and in shutting some of them down. The United States cannot conduct nonproliferation work effectively in a vacuum, without reference to adversaries' WMD programs and procurement aims.

Third, and related to this, collaboration with Russian and other former Soviet security organizations needs to be strengthened, since those organizations—by Russian accounts at least—do much of the heavy lifting in containing nuclear theft and smuggling. Mechanisms for formal and informal information exchange on smuggling incidents, actors, and trends would be of great value in configuring U.S. nonproliferation programs in the newly independent states. As the Center for Nonproliferation Studies' William Potter explains, "Meaningful intelligence-sharing on trafficking incidents . . . is crucial in filling in gaps in past trafficking cases" and "is particularly vital in the context of the ongoing war against international terrorism."<sup>46</sup>

Ideally, a nuclear security policy should also embrace the concept of demand reduction—influencing the motivations of adversary states and subnational groups to prevent the spread of nuclear weapons capability. Unfortunately, the desire for asymmetric advantage, whether of states striving to join the nuclear club or of terrorists intent on imposing their demands on civilized nations, is deeply imbedded in the fabric of the inter-

national system. In contemplating demand reduction, different strategies will need to be applied to different adversaries—diplomacy and negotiations between states and military action to deny terrorists safe havens and keep them off balance. Certain high-profile actions, such as the controversial U.S. invasion of Iraq, might actually increase the craving of small states and other actors for a nuclear deterrent of their own. Thus, contrary to our nonproliferation hopes, a more rather than a less nuclearized world may be in the offing, even as the United States and Russia work to reduce the threat of a global nuclear catastrophe.

The requirements of our nuclear security policy are ultimately inseparable from the requirements of our global campaign against terrorism, especially against groups with nuclear ambitions such as al-Qaeda and its affiliates. Al-Qaeda's attempts to obtain nuclear materials, weapons, and expertise reportedly have gone on for well over a decade. At the same time, there is great uncertainty as to the extent of undocumented leakage—including smuggling that has occurred since the disintegration of the USSR. We do not know how far the global jihadist network might have proceeded toward building a bomb. Hence, our very real progress toward closing the proliferation window in Russia and elsewhere must be combined with unremitting vigilance against threats that may already be out there, waiting to strike us at a time and place that we least expect.

## Notes

1. Excerpts from "Soviet Nuclear Threat Reduction Act of 1991." Cited in National Academy of Sciences, *Strengthening Long-Term Nuclear Security: Protecting Weapon-Usable Material in Russia* (Washington: National Academies Press, 2005), pp. 65, 66.
2. Matthew Bunn and Anthony Wier, *Securing the Bomb 2005: The New Global Imperative* (Cambridge, MA: Harvard University, Belfer Center for Science and Technology, May 2005), p. 76.
3. FY07 Budget Request for National Nuclear Security Administration Office of the Chief Financial Officer, in Department of Energy, *FY*

**A more rather than a less nuclearized world may be in the offing, even as the United States and Russia work to reduce the threat of a global nuclear catastrophe.**

- 2007 Budget Request, vol. 1, p. 514; and personal communication with DOE financial official on March 15, 2005.
4. Bunn and Wier, p. 76.
  5. National Academy of Sciences. *Strengthening Long-Term Nuclear Security*, p. 12.
  6. Yuriy Romyantsev and Aleksei Kholodov, "Conversion Challenges in Russia's Secret Cities," *Nonproliferation Review* (Fall-Winter 2003): 168.
  7. See discussion in Rensselaer Lee, *Smuggling Armageddon: The Nuclear Black Market in the Former Soviet Union and Europe* (New York: St. Martin's, 1998), pp. 35-38.
  8. Steve Sandoval, "Director of the All-Russian Scientific Research Institute of Technical Physics Commits Suicide," *Daily News Bulletin*, November 1, 1996, <http://www.lanl.gov/orgs/pa/News/110196text.html>.
  9. Caitlin Talmadge, "Striking a Balance: The Lessons of U.S.-Russian Material Security Cooperation," *Nonproliferation Review* (Spring 2005): 32.
  10. Author interview with officials of Los Alamos National Laboratory, February 22, 2006.
  11. National Academy of Sciences, *Strengthening Long-Term Nuclear Security*, p. 12.
  12. Author interview with representative of PIR Center for Policy Studies in Russia, September 17, 2004.
  13. National Academy of Sciences, *Strengthening Long-Term Nuclear Security*, p. 12.
  14. The rest was mostly radioactive junk, useless in making weapons. U.S. General Accounting Office, "Nuclear Nonproliferation: U.S. Efforts to Help Other Countries Combat Nuclear Smuggling Need Strengthened Coordination and Planning," GAO-02-426, May 2002, pp. 31-33.
  15. *Ibid.*, pp. 32-34.
  16. "U.S. Intelligence Concludes Theft of Nuclear Material Has Occurred," Agence France Presse, February 23, 1995.
  17. William Potter, "Challenges in U.S.-Russian Cooperation," Paper presented at the Conference on Cooperative Threat Reduction in the 21st Century, Oslo, Norway, June 1, 2002, p. 5.
  18. Yevgeniy Tkachenko, "FSB Agents Prevent Theft of Nuclear Materials," *ITAR-TASS*, December 18, 1998; and "MINATOM Official Says 1998 Theft Attempt in Chelyabinsk Involved HEU," Center for Nonproliferation Studies NIS Nuclear Trafficking Data Base, October 30, 2000.
  19. FY07 Budget Request for National Nuclear Security Administration Office of the Chief Financial Officer, MPC&A Program: Strategic Plan, in Department of Energy, *FY 2007 Budget Request*, July 2001, p. 2.
  20. See, for example, J. Carson Mark et al., "Can Terrorists Build Nuclear Weapons?" Nuclear Control Institute, Washington, <http://www.nci.org/k-m/makeab.htm>.
  21. On the nuclear deal, see Riyad Alam-al-Din et al., "Report Links Bin Laden, Nuclear Weapons," *Al-Watan Al-Arabi*, November 13, 1998. On the Islamic Movement of Uzbekistan (IMU), see Graham Allison, *Nuclear Terrorism: the Ultimate Preventable Catastrophe* (New York: Henry Holt, 2004), p. 23. Allison cites Pakistani sources to the effect that al-Qaeda members had obtained what they claimed was fissile material from the IMU, but actually was radiological material only suitable for a dirty bomb. Scheuer quoted in *Through Our Enemies' Eyes* (Washington: Brassey's, 2001), pp.191-92.
  22. Lee, pp. 125-27.
  23. Charles D. Ferguson and William C. Potter, *The Four Faces of Nuclear Terrorism* (Monterey, CA: Center for Nonproliferation Studies, 2004), p. 63. The authors add the caveat that the terrorists would need the help of insiders familiar with weapons design or else risk being killed or injured by the conventional explosives that are used in all nuclear devices.
  24. William Langewiesche, "The Point of No Return," *Atlantic Monthly*, January-February 2006, pp. 96-118.
  25. National Academy of Sciences, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington: National Academies Press, 2002), p. 52.
  26. Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Henry Holt, 2004), pp. 149-51
  27. Critics of the gold standard idea also point out that far more people, vehicles, and materials go in and out of nuclear facilities than go in and out of Fort Knox. Author interview with officials of Los Alamos National Laboratory, February 22, 2006.
  28. Laura Holgate, "Nuclear Security Culture: The Key to Sustainability," Paper presented at the IAEA Conference on Nuclear Security, London, March 18, 2005, pp. 2-3. See also Igor Khripunov et al.,

- Nuclear Security Culture: The Case of Russia* (Athens: University of Georgia, Center for International Trade and Security, December 2004), pp. 1–13.
29. Author interview with official of Moscow area nuclear facility, September 15, 2004; and Bunn and Wier, p. 14.
30. Lee, p. 131.
31. National Academy of Sciences, *Strengthening Long-Term Nuclear Security*, p. 68; and FY07 Budget Request for National Nuclear Security Administration, Office of the Chief Financial Officer, pp. 517–18.
32. Author interview with officials of Lawrence Livermore National Laboratory, December 8, 2005.
33. Matthew Bunn, *The Next Wave: Urgently Needed New Steps to Control Warheads and Fissile Material*, Joint Publication of Harvard University's Project on Managing the Atom and the Nonproliferation Project at the Carnegie Endowment for International Peace (Cambridge, MA, and Washington, April 2000), p. 39.
34. Louis Charbonneau, "Pakistan's Khan Gave Iran Bomb-Grade Uranium—Exiles," Reuters, November 17, 2004.
35. Stephen Fidler and Victoria Burnett, "Pakistan's 'Rogue' Nuclear Scientist: What Did Pakistan's Government Know about His Deals?" *Financial Times*, April 6, 2004, p. 17.
36. See, for example, Brenda Shaffer, *Partners in Need: The Strategic Relationship of Russia and Iran* (Washington: Washington Institute of Near East Policy, 2001), p. 70.
37. In 2006 DOE changed the metric of MPC&A performance from tons of material to number of buildings—a more favorable indicator of progress. As of the end of FY04 only an estimated 46 percent of material had been secured, compared to 62 percent of buildings. FY07 Budget Request for the National Nuclear Security Administration Office of the Chief Financial Officer, pp. 497, 514.
38. Cited in James L. Ford and C. Richard Schuller, *Controlling Threats to Nuclear Security* (Washington: National Defense University Center for Nonproliferation Research, 1997), p. 3.
39. Justiniano Torres and Alexander Scherbinin, cited in Lee, pp. 94, 101–102.
40. Author interview with former Russian Academy of Sciences official, September 15, 2004. See also Lee, pp. 132–35.
41. National Academy of Sciences, *Strengthening Long-Term Nuclear Security*, p. 3.
42. Russians tend to see terrorists' acquisition of radiation sources that could be used in a dirty bomb as a bigger threat than insider theft of nuclear materials. Since 9/11 DOE has provided funding to secure such sources in Russia and other former Soviet republics, but the major thrust of the cooperative programs has always been on preventing terrorists from obtaining nuclear weapons capability, which has much more destructive implications. See FY07 Budget Request for the National Nuclear Security Administration Office of the Chief Financial Officer, p. 565; and National Academy of Sciences, *Strengthening Long-Term Nuclear Security*, p. 14.
43. *CIA World Factbook 2006*, [www.cia.gov/cia/publications/geos/rs.tyml](http://www.cia.gov/cia/publications/geos/rs.tyml). The CIA compiles estimates of the percentage of people falling below the poverty line in different countries based on surveys of subgroups, with the results weighted by the number of persons in each group. See [ww.cia.gov/cia/publications.factbook/docs/notesand defs.html](http://www.cia.gov/cia/publications.factbook/docs/notesanddefs.html).
44. National Academy of Sciences, *Strengthening Long-Term Nuclear Security*, pp. 29–33.
45. Author interview with officials of Los Alamos National Laboratory, February 22, 2006; and author interview with officials of Lawrence Livermore National Laboratory, December 8, 2005. Drug and alcohol testing already are under way at many nuclear facilities, a positive sign from a security perspective.
46. William Potter and Elena Sokova, "Illicit Nuclear Trafficking in the NIS: What's New? What's True?" *Nonproliferation Review*, Summer 2002, p. 119.

## OTHER STUDIES IN THE POLICY ANALYSIS SERIES

570. **The Federal Marriage Amendment: Unnecessary, Anti-Federalist, and Anti-Democratic** by Dale Carpenter (June 1, 2006)
569. **Health Savings Accounts: Do the Critics Have a Point?** by Michael F. Cannon (May 30, 2006)
568. **A Seismic Shift: How Canada's Supreme Court Sparked a Patients' Rights Revolution** by Jacques Chaoulli (May 8, 2006)
567. **Amateur-to-Amateur: The Rise of a New Creative Culture** by F. Gregory Lastowka and Dan Hunter (April 26, 2006)
566. **Two Normal Countries: Rethinking the U.S.-Japan Strategic Relationship** by Christopher Preble (April 18, 2006)
565. **Individual Mandates for Health Insurance: Slippery Slope to National Health Care** by Michael Tanner (April 5, 2006)
564. **Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act** by Timothy B. Lee (March 21, 2006)
563. **Against the New Paternalism: Internalities and the Economics of Self-Control** by Glen Whitman (February 22, 2006)
562. **KidSave: Real Problem, Wrong Solution** by Jagadeesh Gokhale and Michael Tanner (January 24, 2006)
561. **Economic Amnesia: The Case against Oil Price Controls and Windfall Profit Taxes** by Jerry Taylor and Peter Van Doren (January 12, 2006)
560. **Failed States and Flawed Logic: The Case against a Standing Nation-Building Office** by Justin Logan and Christopher Preble (January 11, 2006)
559. **A Desire Named Streetcar: How Federal Subsidies Encourage Wasteful Local Transit Systems** by Randal O'Toole (January 5, 2006)
558. **The Birth of the Property Rights Movement** by Steven J. Eagle (December 15, 2005)
557. **Trade Liberalization and Poverty Reduction in Sub-Saharan Africa** by Marian L. Tupy (December 6, 2005)
556. **Avoiding Medicare's Pharmaceutical Trap** by Doug Bandow (November 30, 2005)
555. **The Case against the Strategic Petroleum Reserve** by Jerry Taylor and Peter Van Doren (November 21, 2005)
554. **The Triumph of India's Market Reforms: The Record of the 1980s and 1990s** by Arvind Panagariya (November 7, 2005)

553. **U.S.-China Relations in the Wake of CNOOC** by James A. Dorn (November 2, 2005)
552. **Don't Resurrect the Law of the Sea Treaty** by Doug Bandow (October 13, 2005)
551. **Saving Money and Improving Education: How School Choice Can Help States Reduce Education Costs** by David Salisbury (October 4, 2005)
550. **The Personal Lockbox: A First Step on the Road to Social Security Reform** by Michael Tanner (September 13, 2005)
549. **Aging America's Achilles' Heel: Medicaid Long-Term Care** by Stephen A. Moses (September 1, 2005)
548. **Medicaid's Unseen Costs** by Michael F. Cannon (August 18, 2005)
547. **Uncompetitive Elections and the American Political System** by Patrick Basham and Dennis Polhill (June 30, 2005)
546. **Controlling Unconstitutional Class Actions: A Blueprint for Future Lawsuit Reform** by Mark Moller (June 30, 2005)
545. **Treating Doctors as Drug Dealers: The DEA's War on Prescription Painkillers** by Ronald T. Libby (June 6, 2005)
544. **No Child Left Behind: The Dangers of Centralized Education Policy** by Lawrence A. Uzzell (May 31, 2005)
543. **The Grand Old Spending Party: How Republicans Became Big Spenders** by Stephen Slivinski (May 3, 2005)
542. **Corruption in the Public Schools: The Market Is the Answer** by Neal McCluskey (April 14, 2005)
541. **Flying the Unfriendly Skies: Defending against the Threat of Shoulder-Fired Missiles** by Chalres V. Peña (April 19, 2005)
540. **The Affirmative Action Myth** by Marie Gryphon (April 6, 2005)
539. **\$400 Billion Defense Budget Unnecessary to Fight War on Terrorism** by Charles V. Peña (March 28, 2005)
538. **Liberating the Roads: Reforming U.S. Highway Policy** by Gabriel Roth (March 17, 2005)
537. **Fiscal Policy Report Card on America's Governors: 2004** by Stephen Moore and Stephen Slivinski (March 1, 2005)
536. **Options for Tax Reform** by Chris Edwards (February 24, 2005)
535. **Robin Hood in Reverse: The Case against Economic Development Takings** by Ilya Somin (February 22, 2005)

534. **Peer-to-Peer Networking and Digital Rights Management: How Market Tools Can Solve Copyright Problems** by Michael A. Einhorn and Bill Rosenblatt (February 17, 2005)
533. **Who Killed Telecom? Why the Official Story Is Wrong** by Lawrence Gasman (February 7, 2005)
532. **Health Care in a Free Society: Rebutting the Myths of National Health Insurance** by John C. Goodman (January 27, 2005)
531. **Making College More Expensive: The Unintended Consequences of Federal Tuition Aid** by Gary Wolfram (January 25, 2005)
530. **Rethinking Electricity Restructuring** by Peter Van Doren and Jerry Taylor (November 30, 2004)
529. **Implementing Welfare Reform: A State Report Card** by Jenifer Zeigler (October 19, 2004)
528. **Fannie Mae, Freddie Mac, and Housing Finance: Why True Privatization Is Good Public Policy** by Lawrence J. White (October 7, 2004)
527. **Health Care Regulation: A \$169 Billion Hidden Tax** by Christopher J. Conover (October 4, 2004)
526. **Iraq's Odious Debts** by Patricia Adams (September 28, 2004)



1000 Massachusetts Ave., N.W.  
Washington, D.C. 20001

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission.

Additional copies of Policy Analysis are \$6.00 each (\$3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001 or call toll free 1-800-767-1241 (noon-9 p.m. eastern time). Fax (202) 842-3490 • [www.cato.org](http://www.cato.org)

