INMM 2015

Corrupting Nuclear Security: Potential Gaps and New Approaches to Insider Risk Mitigation

D. Donnelly, D. Kovchegin, S. Mladineo, L. Ratz, N. Roth

A. Abstract

Much of the literature on nuclear security focuses on identifying approaches that strengthen physical protection (PP) systems ("guards, gates, guns") and improve material control and accounting (MC&A) methods and technologies. Despite the growing body of evidence indicating that a well-placed insider could overcome some of the most sophisticated PP and MC&A systems, less attention has been focused on studying the "human factor" -- that is, analyzing the potential motivations, capabilities, and pathways an insider might take to perpetrate an act of nuclear theft or sabotage.

Corruption of an insider within an organization represents one of the likely pathways by which a security system might be deliberately compromised at a nuclear facility to facilitate nuclear theft or sabotage. Recent history demonstrates that the risk of insider corruption to a security regime is all too real. Yet, paradoxically, "anti-corruption" and "human reliability" in the nuclear security realm are typically treated separately, using different means, for different ends – potentially missing corruption risks that could feasibly be mitigated.

This paper offers an overview of the conceptual linkages between nuclear security and corruption and presents a brief review of experience from the realms of nuclear non-proliferation, breaches of highly sensitive national security information, and high-value thefts and heists. It then offers a preliminary assessment of the degree to which current approaches to anti-corruption and human reliability successfully address corruption risks, particularly in the nuclear security context. This paper's findings establish a need for additional research on how anti-corruption and nuclear security human reliability programs could more clearly, consistently, and proactively scrutinize and dis-incentivize behaviors that present increased risks of corruption.

B. How Corruption Can Impact Nuclear Security

While many definitions exist, this paper defines corruption as willingly seeking personal gain in exchange for the misuse of entrusted access, authority, or knowledge. Corruption can take many forms. An employee could steal sensitive materials or equipment outright, either to sell or keep. An employee of a nuclear facility can be bribed into assisting in theft or sabotage. Systemic organizational corruption can weaken a nuclear security system, making it difficult to detect insider threats or corruption. Even security systems within organizations that are not corrupt can be compromised if they exist within a larger corrupt system.[1]

[1] http://www1.worldbank.org/publicsector/anticorrupt/corruptn/cor02.htm

Corruption poses a particularly significant challenge to nuclear security. Every country in the world is vulnerable to corruption, including those with nuclear material. Alarmingly, four of the countries with the most nuclear material—Russia, China, Pakistan, and India— appear in the bottom half of Transparency International's ranking of countries according to perceived levels of corruption.[2] Even in countries where there is less corruption, organizations that handle nuclear material or technology are vulnerable because they are often shrouded in secrecy and often insulated against public accountability mechanisms like the press.

Like all insider threats, corrupted insiders could potentially use their access, authority, or knowledge to bypass security measures without being detected. Insiders can fly below the radar biding their time to reduce the likelihood of being noticed. Gathering evidence to determine whether there is an insider threat may also be difficult, as their connection to a crime could be tenuous or because they may be able to subvert an investigation.

What distinguishes a corrupt insider from other insiders is motivation. Insiders can be motivated by a range of factors (ideology, politics, coercion, etc.). A corrupt insider is motivated by personal gain in some form or another (monetary, political, etc.). The possibility that an insider could be involved in illicit transactions increases the likelihood they could be detected.

The threat of corruption within a nuclear facility is not merely an abstract concept. Recent history is filled with instances where corruption has assisted in the theft of state secrets, high-value items, and even nuclear material or technology.

Examples of individuals who have sold national security information for cash include Aldrich Ames, Robert Hanssen, and John Walker. Ames is reported to have collected as much as $4.6 million from the KGB for his espionage.[3] Despite various indicators and reliable tips about Ames' lavish spending, it took several years for the government to undertake a thorough inquiry and initiate appropriate response measures that would lead to his eventual arrest.[4]

Corrupt insiders have also played important roles in both simple and complex heists of high-value items. In one study of 23 heists involving millions of dollars, recruited, planted, or opportunistic insiders willingly played roles in almost half of the cases. For example, in 1983, six men stole $86 million worth of gold bullion from a Brinks-Mat depot in London, aided by one of the depot employees. In another case, hundreds of millions of dollars' worth of valuables were stolen from the Diamond Center in Antwerp by an individual with insider knowledge of security practices. The thief pretended to be a diamond merchant for two years in order to gain access and identify vulnerabilities within the facility.[5]

---

[2] Corruption Perceptions Index 2014, http://www.transparency.org/cpi2014/results.
[3] Rupert Cornwell, The Independent, January 16, 2013.
[4] Famous cases and criminals, Federal Bureau of Investigations, http://www.fbi.gov/about-us/history/famous-cases/aldrich-hazen-ames.
[5] Jarret M. Lafleur, Liston K. Purvis, Alex W. Roesler, *The Perfect Heist Recipes from Around the World* (Livermore, CA: Sandia National Laboratories, 2014) http://prod.sandia.gov/techlib/access-control.cgi/2014/141790.pdf.

Nuclear facilities have similarly been compromised by corruption. Corruption has been a key contributing factor to the proliferation of sensitive nuclear technology over the past two decades and has played a role in numerous cases of nuclear theft or attempted nuclear theft. The first known instance of nuclear material theft from a Russian facility was perpetrated by a corrupt insider. In 1992, Leonid Smirnov—an engineer at the Luch Scientific Production Association—stole small quantities of highly enriched uranium over the course of several months that he intended to sell.[6]
In another case, Boris Markin, a wealthy Russian businessman, offered two residents of a town near a Russian nuclear weapons laboratory $750,000 in exchange for stealing weapons-grade plutonium that he planned to provide to a third party. Although they never carried out the act, he went as far as providing $50,000 as a down payment.[7] In 2012, the director and two of the deputy directors of one of the largest nuclear material producing facilities in Russia were arrested for embezzlement and corruption. More than $2 million in cash and gold was found in the director's home.[8]

States have only recently begun recognizing corruption as a serious threat to nuclear security systems. Insider threats — corrupt or otherwise — were not incorporated into International Atomic Energy Agency's Recommendations for the Physical Protection of Nuclear Material until its fourth revision in 1999. Even today, nuclear security regimes in many countries still do not require that systems specifically protect against multiple insiders, despite strong evidence that multiple-insider scenarios are a credible threat.[9]

C. Approaches to Addressing Corruption

C.1. Anti-corruption

"Anti-corruption" as a concept encompasses a broad and diverse sweep of measures and initiatives. When viewed as a whole, these efforts have tended to focus on limiting opportunities for self-dealing by officials (through increased transparency and elimination of conflicts of interest)[10], imposing criminal

---

[6] For more on Smirnov, see Frontline, "Loose Nukes: Interviews" (Public Broadcasting System, original air date November 19, 1996), http://www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/smirnov.html.
[7] For a more complete taxonomy of how corruption contributes to nuclear proliferation, see Matthew Bunn, "Corruption and Nuclear Proliferation," in Robert I. Rotberg, ed., Corruption, Global Security, and World Order (Washington, D.C.: Brookings, 2009), pp. 124-126.
[8] For more on this case and others like it, see Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey. "Advancing Nuclear Security: Evaluating Progress and Setting New Goals" (Cambridge, Mass.: The Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard University, March 2014), http://belfercenter.ksg.harvard.edu/files/advancingnuclearsecurity.pdf.
[9] See Matthew Bunn and Eben Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey*, (Cambridge, Mass.: The Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard University, March 2014), http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf.
[10] See, e.g., United Nations Convention Against Corruption (UNCAC), Art. 7(4), 8(5), 9, 10, 13, 9 December 2003, in Report of the Ad Hoc Committee for the Negotiation of a Convention Against Corruption on the work of its first to

liability on individuals and corporations for conduct such as bribery and money laundering[11], and on requiring due diligence and reporting of suspicious activity by financial institutions.[12] International recommendations and state practices for preventing and detecting money laundering have become quite extensive, typically following a risk-based approach under which cases that involve indicators of increased risk of money laundering are subjected to enhanced scrutiny.[13]

Although anti-corruption measures are now fairly detailed, they nonetheless appear largely to fail to address the specific corruption concerns described above. Standing international recommendations do not offer measures that state institutions can take to actively and continuously protect the integrity of their functions against the risk that an outsider might supply some benefit to an insider in exchange for assistance in compromising security.

Logical protections against corruption of state officials in sensitive positions might include clear policies providing for auditing and regular monitoring of officials' assets and large or high-risk transactions, similar to long-accepted and widespread policies to monitor for drug and alcohol abuse. Auditing of institutional accounts and assets is recommended to ensure the integrity of public funds.[14] There are, however, no comparable recommendations for monitoring or auditing individual officials' finances to ensure that they are not being paid to abuse their authority.

International recommendations emphasize that financial institutions need to scrutinize finances and assets for so-called "politically exposed persons" (PEPs) entrusted with "prominent public functions," who are recognized as presenting a potential increased risk for corruption and money laundering.[15] The PEP concept, however, is not consistently implemented by states, and in any case the concept as currently articulated would not extend to nuclear facility personnel. The United States and Canada, for instance, actively scrutinize only foreign officials, not domestic officials, as PEPs for anti-money laundering purposes.[16] In addition, the current generally accepted definition of PEPs applies only to

---

seventh sessions, G.A. Res. 58/4, U.N. GAOR, 58th Sess., 50th & 51st plen. mtgs., Annex, Agenda Item 108, U.N. Doc. A/58/422 (2003).

[11] See, e.g., UNCAC, *supra* note 10, Chapter III; Foreign Corrupt Practices Act of 1977 (15 U.S.C. §78dd-1, *et seq.*); Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Dec. 17, 1997, 337 I.L.M. 8 (OECD Anti Bribery Convention).

[12] See, e.g., UNCAC *supra* note 10, Art. 14, 23, 58; Financial Action Task Force Recommendations (FATF Recommendations), D.10., 20., pp 14-15, 19, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[13] See, e.g., Federal Financial Institutions Examination Council, VSA/AML Risk Assessment, "Customers and Entities" http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_005.htm.

[14] See, e.g., UNCAC, *supra* note 10, Art. 9.

[15] See UNCAC, *supra* note 10, Art. 52(1),(2); FATF Recommendations, *supra* note 11, A.1., D.12., pp 11, 16.

[16] See Bank Secrecy Act Anti-Money Laundering Examination Manual, Federal Financial Institutions Examinations Council, "Politically Exposed Persons - Overview," http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_087.htm; Declaration of Canada upon acceptance of UNCAC, *available at* http://www.unodc.org/documents/treaties/UNCAC/ReservationsDeclarations/DeclarationsAndReservations14Aug2008.pdf. The U.S. regards its ethics and financial disclosure laws (5 U.S.C. Appendix §101-111) as satisfying the

senior government officials, and would thus presumably not apply to working level nuclear personnel.[17] This presents a potentially significant gap in the current risk-based approach to anti-money laundering, as low- and mid-level national security officials, especially those in a nuclear weapons complex, often have responsibilities that, if compromised, could result in tremendous harm to society.

C.2. Human Reliability

In nuclear security, applicable international conventions and standards require that states put in place measures to establish the trustworthiness of personnel who are to be granted access privileges to protected areas with nuclear materials.[18] These conventions and standards do not define "trustworthiness", nor do they provide any guidance for states on how to reliably establish the trustworthiness of personnel. There is also currently no accepted international guidance on whether and how corruption risks should be considered as a derogatory factor in assessments of trustworthiness for nuclear security.

State approaches to the establishment of trustworthiness typically involve background investigations to assess derogatory information that might preclude an affirmative determination on trustworthiness and serve as a basis for denial of a security clearance. Nuclear facility personnel are often subject to even more stringent monitoring and standards than other national security personnel. These programs can be quite extensive. Of note, however, is that there are no standing international recommendations for continuous assessment of trustworthiness once it is "established" initially, and state practice varies. Among certain states of key significance for nuclear security, such as the United States, derogatory information is assessed only in connection with initial investigations and periodic re-investigations – and not on a continuous basis – and significant time can elapse between periods of scrutiny. Further, where several derogatory factors are often treated in detail, such as foreign contacts, narcotics and alcohol abuse, mental health, and financial distress, states do not consistently or continuously scrutinize their

---

purpose of PEP scrutiny (see Articles of the UN Convention Against Corruption on Asset Recovery: analysis of reported compliance and policy recommendations, Conference of the States Parties to the UN Convention Against Corruption, p 50, http://www.unodc.org/documents/treaties/UNCAC/COSP/session3/V0987578e.pdf). However, these laws extend only to U.S. federal employees at or above GS-15 or equivalent (they do not apply to national laboratory contractor employees, who comprise the bulk of workers in the U.S. nuclear weapons complex), and they impose no requirements for heightened scrutiny of officials by financial institutions. Further undermining international consistency on this issue, a UN Office of Drugs and Crime review of U.S. compliance with Art. 52 acknowledged the incomplete U.S. application of the PEP concept, but did not identify it as a serious concern against the backdrop of U.S. implementation of certain other risk-based factors ("United States of America: Review of the Implementation of Articles 5, 15, 16, 17, 25, 46 Paragraphs 9 and 13, 52 and 53 of the United Nations Convention against Corruption," Sec. 3.7.b., Paragraph 2, 2009, http://www.state.gov/j/inl/rls/rpt/131235.htm).

[17] See Open-ended Intergovernmental Working Group on Asset Recovery, Discussion Guide for the Thematic Discussion of Article 52, Article 53, paras. 15,17, Sept. 2014, http://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup2/2014-September-11-12/V1404104e.pdf.

[18] Convention on the Physical Protection of Nuclear Material, Annex I,1.c., 18 ILM 1419 (1979); IAEA Information Circular 225, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, Revision 5, 4.26 (2011).

personnel for unexplained financial interests or other benefits. These issues will be treated in greater detail in the discussion of the U.S. Department of Energy's Human Reliability Program (HRP) below.

D. Illustrative Case Studies

D.1. Anti-corruption in Rosatom and the Russian Federation

Corruption is commonly acknowledged as a major problem in Russia, and it is one from which the Russian nuclear industry and Rosatom—Russia's state corporation for atomic energy—are not immune. In recent years, several top Rosatom managers, including the Deputy Head of Rosatom and the director of the Siberian Chemical Combine, a major nuclear site, have been prosecuted for corruption-related offences.

While troubling, these cases have also demonstrated at least some willingness by Russian authorities to curb corruption in the nuclear industry. Rosatom's anti-corruption efforts strongly reflect the paradigm characterized earlier of being targeted to reduce the risk of self-dealing and significant theft from the state budget or Rosatom nuclear sites' funding, but not explicitly to reduce risks to security. Specific Rosatom anti-corruption efforts include:

- Rosatom's corporate procurement standard. This standard has been adopted by most Rosatom organizations, including all major nuclear sites. The standard is revised regularly based on feedback from stakeholders. Since it was first issued in 2009, the standard has been revised nearly 50 times.[19]
- Extensive federal and Rosatom agency level regulations on preventing corruption.[20]
- Publication of the income and assets of top Rosatom managers and their families.[21] The list of officers who must report their income and assets is set by Rosatom. Currently this list only includes top-level managers at Rosatom headquarters, not personnel at Rosatom nuclear sites.[22]
- A training program on preventing corruption established in Rosatom's Institute for Continuing Education and Training.[23]
- The creation of a "Transparency Enhancement Council" with continuous participation by Transparency International.[24]

---

[19] http://zakupki.rosatom.ru/?mode=CMSArticle&action=siteview&oid=68&returnurl=&node=af23
[20] http://www.rosatom.ru/aboutcorporation/anti_corruption/normative_akts/
[21] http://www.rosatom.ru/aboutcorporation/anti_corruption/income/
[22] Rosatom Order #1/666-P of June 25, 2013. http://www.rosatom.ru/wps/wcm/connect/rosatom/rosatomsite/resources/8a9acb8043ce02d7a1cce558732d9c8b/prikaz_1_666.doc
[23] http://www.vz.ru/news/2015/2/12/729271.html
[24] http://www.rosatom.ru/aboutcorporation/prozrachnost/ http://www.rosatom.ru/wps/wcm/connect/rosatom/rosatomsite/resources/4691a78045da51aaab41ffd203d7ee18/GO+ROSATOM+2013.pdf (see statement by Elena Panfilova, Transparency International Russia, pp 8-9)

- Initial implementation of a policy on conflict of interest, with a separate adjudicative body (which is still in the initial stages of being stood up, and has not yet publicly reported on its activities).[25]

Rosatom's procurement system became the subject of a study on corruption risks performed by Transparency International. The study consisted of an initial report in November 2010[26] and a follow-up report that incorporated and responded to feedback from Rosatom in October 2011[27]. On the one hand, these reports concluded that Rosatom's procurement system still contains multiple gaps and provides opportunities for abuses. On the other hand, subsequent analysis by Transparency International noted a positive dynamic and continued improvement by Rosatom, even going so far as to rate Rosatom as the best of the six Russian state corporations that were rated in terms of their anti-corruption efforts.[28]

At the same time, Rosatom's anti-corruption program has been narrowly focused, addressing only potential abuses in managing the state budget or Rosatom nuclear site funds. These efforts do not cover such risks as bribery of nuclear site employees for the purpose of gaining access to nuclear materials or inflicting other damage to nuclear security. This problem could potentially be mitigated by explicitly addressing corruption risks in the process for administering the clearances of personnel allowed to work with nuclear materials and at nuclear sites, as well as through developing proper components of a nuclear security culture program.

Current security clearance procedures for Russian nuclear sites[29] fail to clearly address corruption. The full scope of background checks implemented by security services is not publicly available. However, based on the list of information applicants are required to provide to obtain a clearance, this background check does not include any financial audits and does not require declaration and monitoring of substantial assets, major transactions and financial interests. The clearance procedure establishes certain criteria that may lead to denial of clearance, including a past history of convictions for so-called "grave" crimes (roughly equivalent to a felony in the United States). Under the current Russian Criminal Code, however, a significant share of corruption-related offences are not categorized as being sufficiently grave to justify a denial of clearance. For example, the conviction of the director of the Siberian Chemical Combine mentioned above did not meet the threshold of gravity that would bar him from obtaining a clearance in the future.

Rosatom's guide on nuclear security culture activities recommends analysis of "the impact of the human factor on the effectiveness of MPC&A system operation" and establishes requirements for certain personnel behaviors. However, this does not explicitly include anything aimed at prevention of corruption risks and associated threats to nuclear security.

---

[25] http://www.rosatom.ru/aboutcorporation/anti_corruption/comission/
[26] http://transparency.org.ru/goszakupki/predvaritelnaia-ekspertiza-zakupok-rosatoma
[27] http://transparency.org.ru/goszakupki/itogovyi-doklad-po-zakupkam-rosatoma
[28] http://transparency.org.ru/component/docman/doc_download/537---1113
[29] Government Decree #63 of February 6, 2010.
http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=137414

D.2. Human Reliability Regulations for the U.S. Department of Energy

A Human Reliability Program (HRP) is in force at US Department of Energy (DOE) and National Nuclear Security Administration (NNSA) sites and facilities where the security of nuclear materials is of concern. A similar program for nuclear weapons security at Department of Defense facilities is called a Personnel Reliability Program (PRP). The HRP is governed by regulations published in the Code of Federal Regulations. These regulations are quite extensive, focusing on assessing indications of trustworthiness. Initial and periodic reinvestigations assess such areas as foreign contacts, psychological health, signs of economic irresponsibility or distress, and monitoring for alcohol or narcotics abuse.[30]

The full extent of procedures under the HRP are not available to the public, but those regulations that are public provide guidance on the kinds of concerns that a supervisor must report on an individual in the program. For example, these include: psychological or physical disorders that impair performance of assigned duties; arrests for criminal behavior; suicidal tendencies; use of illegal drugs or the abuse of legal drugs or other substances; alcohol use disorders; significant behavioral changes, moodiness, depression, or other evidence of loss of emotional control; or indications of deceitful or delinquent behavior. Alcohol testing, periodic drug testing, and medical reviews are prominent components of the program.

A more difficult area to assess is the accumulation of unexpected or unexplained wealth. For adjudicating security clearances generally, outside activities and financial assets for which legitimacy cannot be established would be derogatory considerations.[31] Areas for self-reporting and review in the form used for HRP annual reviews, however, only address outside activities with foreign nationals, foreign financial interests and indicators of financial distress (bankruptcy, hardship, etc.). Such reporting would not capture instances where a potentially conflicting financial interest has no apparent foreign nexus, where outside activity does not involve foreign nationals, or where a person is not financially distressed but nonetheless accepts some form of payment.

There are extensive provisions on regular random drug testing, but no comparable provisions detailing financial reviews or audits. As such, on their surface, the publicly available portions of the regulations suggest potential gaps for financial and other outside activity that does not need to be reported, may be less likely to be detected or scrutinized, and is relatively less likely to adversely affect a clearance. This raises a potential vulnerability; clearance applicants and holders may conclude that their full assets and income stream are unlikely to be subject to scrutiny, thus lowering barriers to entering into conflicts of interest. Thus, a person in an HRP position may not be subject to clear, consistent or systematic evaluation of his or her financial situation, at least not anything like to the same degree as areas such as foreign contacts, mental illness, narcotics abuse, and financial distress.

[30] 10 C.F.R. §§709,710,712

[31] 10 C.F.R. §710, Appendix B, Guidelines F,L

E. Conclusion, Next Steps

This paper's findings suggest that current scrutiny of the finances, assets, and conflicts of interest of personnel in sensitive nuclear security positions is potentially lax, and that anti-corruption and human reliability efforts could be better integrated and focused. This state of affairs may present a weak deterrent against corrupt conduct and result in substantial security risks. With no system for independent verification of declared assets, a nuclear facility insider may find it easy to arrange to receive payment without detection. This could allow such an insider to avoid both criminal prosecution and adverse consequences for his or her clearance, which could, in turn, allow a scheme to carry on for some time (as occurred with Aldrich Ames). Further, it is concerning that a conviction on corruption charges may not result in denial of subsequent applications for security clearance in Russia.

Our findings additionally suggest that current national-level, risk-based approaches to anti-corruption and anti-money laundering could better conceptualize and account for risks such as those inherent in the nuclear security field. Assessment of "risk" need not look in a binary way for the presence or absence of money laundering alone, for instance - it could also account for the magnitude of social harm that could flow from the likely illegal activity in question. Corruption of domestic officials that could undermine the functioning of government, or of personnel at security institutions involving high levels of danger to the public, such as nuclear facilities, likely merit significant weight in a hierarchy of potential risks for enhanced scrutiny.

Additional research is necessary to identify effective policy interventions that could integrate anti-corruption measures into human/personnel reliability programs. In principle, an "integrated" approach to HRP for institutions responsible for nuclear materials could consist of:

- Integration into clearance and HRP/PRP-type processes of clear requirements for declaration and monitoring of substantial assets, major transactions and financial interests
- Strong, clear policies on declaring and reconciling conflicts of interests and outside activities as an integral component of security clearances
- Maintaining robust pathways for anonymous and protected reporting of suspicious activity (conspicuous consumption, use of cash, etc.)
- Standards for assessing risks and conflicts of interests
- Reasonably independent/impartial tools for performing assessment and issuing a determination

Furthermore, countries may consider developing special, heightened reporting requirements for financial institutions servicing persons holding HRP-required positions, requiring these institutions to enhance monitoring of financial assets to detect unusual patterns of transactions.

As policymakers consider policy interventions that integrate nuclear security and anti-corruption, they should consider involving stakeholders with competency and jurisdiction that could enhance the overall effectiveness of efforts to prevent corruption at nuclear facilities. Central government authorities responsible for investigating anti-money laundering schemes are likely to have more experience and

expertise in dealing with addressing money laundering schemes than nuclear operators/regulators/oversight authorities. For example, a more effective and integrated approach to addressing money laundering risks in the nuclear security context could be to have existing anti-money-laundering monitoring programs prioritize HRP personnel, and to integrate any derogatory information that such monitoring reveals into HRP-type clearance assessments on a continuous, real-time basis.

Importantly, implementation of policy interventions should balance reasonable privacy and civil liberty considerations, consistent with national laws, customs and regulations. Auditing and continuous financial monitoring also have the potential to be onerous, intrusive, labor intensive and even demoralizing tools. Public officials and national security personnel should feel pride for doing important work, and overly draconian measures could alienate personnel and increase insider risks. These concerns should be weighed carefully to achieve a reasonable balance of scrutiny and privacy.

The feasibility, potential costs and reliability with which such approaches might deter and detect attempts at corrupt recruitment of insiders should also be carefully assessed through further research. There is a growing debate, for example, concerning the cost effectiveness of asset monitoring efforts related to anti-money laundering and "counter proliferation financing" programs, with some experts arguing that these interventions come at very high costs and yield few results because perpetrators are more likely than not to evade monitoring programs or participate in informal financial transactions outside of the financial services industry.[32]

Future research into policy interventions that seek to integrate anti-corruption and nuclear security efforts will thus need to lay the groundwork for a careful cost-benefit analysis that will include analysis of likelihood of detection of corruption, deterrence effects, privacy concerns, and implementation costs.

Considering the potential consequences of nuclear theft, measures to address corruption should elevate the sense of scrutiny facing persons holding public trust positions in the nuclear field, increase the likelihood of detection of corruption, increase the costs of engaging in corruption, and enhance deterrence of corruption among potential bribe-givers and takers. More generally, policymakers should invest resources in interventions that meaningfully address the "human factor" in light of two basic propositions: that some of the most sophisticated security equipment in the world can be undermined by a knowledgeable and well-placed insider, and that a large share of the world's nuclear materials remains situated in corruption-prone environments.

[32] http://www.economist.com/node/5056338?story_id=E1_VDVGPPR