Nuclear Security Culture as a Tool to Address Insider Threat

I.Khripunov[1], C. Speicher[2]

[1]University of Georgia, Athens, Georgia, USA

[2] Ministry of the Environment, Climate Protection and the Energy Sector, Baden-Württemberg, Germany

Email of main author: igokhrip@uga.edu

Abstract. Nuclear facilities, organizations, and regulatory agencies have a compelling interest in developing effective methodologies to help mitigate potential insider threat. The IAEA defines an “insider” as one or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so. The IAEA Implementing Guide on Preventive and Protective Measures Against Insider Threat (NSS No.8) has multiple references to the role of nuclear security culture (NSC) in addressing insider threat but does not provide any specifics in this regard. This paper attempts to fill in this gap and develop step-by-step guidance for using the evolving NSC methodology to perform this vital function. The IAEA NSC model has 30 characteristics of culture while the Draft Technical Guidance for NSC Self-Assessment lists over 300 culture indicators to illustrate the meaning of each characteristic. At least several of them are directly linked to widely used practices designed to prevent insiders from committing malicious acts and mitigating their possible consequences. For example, Human Reliability Program is covered by NSC characteristic “Continual determination of staff trustworthiness; Mitigation of Occupational Strain by “Work environment”; Compliance with IAEA Proposed Preventive and Protective Measures by “Adherence to procedures”; and Improved Observation Skills by “Vigilance,” which includes observation and reporting. Culture indicators associated with these characteristics would enable management to self-reflect to determine existing weaknesses and strengths or launch, if deemed necessary, a full-scope self-assessment focusing on insider threat as the main theme. A follow-up NSC enhancement plan will prioritize, among other tasks, improving relevant management systems, targeted training curricula, awareness raising and reliable communication systems in a comprehensive effort to promote a robust culture with special emphasis on dealing with insider threat. NSC self-assessments held at regular intervals will enable management to determine whether its follow-up plans yield desired results and what adjustments need to be made under the next plan. This cycle of IAEA recommended assessment and enhancement of security culture will keep insider risks under continuous scrutiny in a NSC general context rather than implementing separate and often disconnected initiatives in this regard. In addition, involving a considerable portion of the workforce in surveys, interviews and focus groups as methods of self-assessment can be a valuable and sustainable learning experience in addition to conventional classroom training format. Continuous focus on NSC as well as organization-wide dissemination and discussion of self-assessment reports can deter potential insiders from implementing their plans. The proposed approach is just one possible way to cope with the insider risk but it has several important advantages which is discussed in this paper.

Key words: Nuclear Security Culture, Self-assessment, Insider Threat

1. Introduction

Nuclear security culture (NSC) refers to human performance when interacting with security risks, systems, products, and the environment. In practice, the flexibility and intelligence of people are considered the key ingredients in protecting nuclear sites and material from internal and external threats.

What is nuclear security culture and its scope? The International Atomic Energy Agency (IAEA) defines it as "the assembly of characteristics, attitudes and behavior of individuals and organizations and institutions which serve as a means to support and enhance nuclear security." [1] As a supporting and enhancing tool, the role of culture can be deducted from the definition of nuclear security, which is "the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, or other radioactive substances or their associated facilities." [2] This concept of nuclear security is noteworthy in that it goes beyond traditional physical protection, material accountancy and control, and other measures. This cross-cutting concept—explicitly or implicitly—covers a much wider playing field, including border security, customs, export control, illicit trafficking, personnel reliability screening, and *malicious acts by insiders*.

The IAEA defines an "insider" as one or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt an unauthorized removal or act of sabotage, or who could aid an external adversary to do so. The IAEA Implementing Guide on Preventative and Protective Measures Against Insider Threat (NSS No. 8) contains multiple references to the role of nuclear security culture (NSC) in addressing insider threat, but does not provide any specifics on how to apply this methodology. Many different methods exist to evaluate the overall effectiveness of a nuclear security system against insider threat, including table top exercises, performance testing, inspections and assessments, scenario analysis method and others. This paper attempts to develop step-by-step guidance for using the evolving NSC methodology for addressing insider threat, by applying major tools of self-assessment to prevent malicious acts, protect assets, and mitigate their effects. In this sense, the NSC approach is designed to complement existing methods by identifying root causes of their behavior and enhancing vigilance of entire personnel by self-reflecting their own roles and responsibilities.

2. What is Insider Threat?

The term "insider" is used to describe an adversary with authorized access to a nuclear facility, a transport operation, or sensitive information. A physical protection system is designed and evaluated against threats posed by both outsiders and insiders; but insider threats are different, as they present a unique problem. Insiders could take advantage of their access (i.e. right or opportunity to gain admittance), complemented by their authority (i.e. power or right to enforce obedience), and knowledge of the facility (i.e. awareness or familiarity gained by training or experience), to bypass dedicated physical protective elements or other provisions such as safety, nuclear material control and accountancy (MC&A), and operating measures and procedures.

Moreover, inside individuals with authorized access and positions of trust are more capable of defeating security obstacles not available to outsiders. Insiders have more opportunity (i.e. more favorable conditions) to select the most vulnerable target, and the knowledge of when the best time to perform the malicious act would be. They can extend the malicious act over a long period of time to maximize the likelihood of success. This could include, for example, tampering with safety equipment to prepare for an attempt or act of sabotage, or falsifying accounting records in order to repeatedly steal small amounts of nuclear material.

Potential insiders may hold different positions including physical protection system designers, system administration staff, experimenters, IT specialists, security guards, material handlers, clerks, nuclear material custodians, safeguards officers, operational maintenance workers, or senior managers. Others not directly employed may include vendors, emergency personnel (firefighters and first responders), contractors, subcontractors, and outsource services. It would however be a dangerous fallacy to underestimate possible impacts caused by ordinary workers and employees, e.g. decommissioning, construction or decontamination workers) .

Insider motivation may include ideological, personal, financial, and psychological factors. Management should never assume that their personnel are so loyal that they will never be subject to ideology change, a shift in allegiance, or vulnerable to personal incentives that could lead them to become insider threats. Following a negative work-related event such as termination, dispute with an employer, demotion, or unwanted transfer, disgruntled employees are much more likely to become insiders—and much less likely to proactively help improve organizational security. As many first generation nuclear power plants (NPPs) are being decommissioned, the personnel whose jobs are at risk are more likely to develop a grudge against their employers and become a threat.

Also, an individual could be forced to become an insider by coercion or by coercing others, including family members. In a case in Northern Ireland in 2004, for example, thieves robbed a bank and made off with £26 million. They kidnapped the families of two bank managers and blackmailed the managers into helping them carryout their crime. [3] Similarly, terrorists also can make use of such coercion tactics for enlisting help in stealing nuclear materials.

Security guards and personnel can also present insider threat. In non-nuclear guarded facilities, guards are responsible for about half of the security incidents involving insiders. Conspiracies of multiple insiders, familiar with the weaknesses of security operations are among the most difficult of threats for security systems to defeat. Hence, whenever possible, nuclear security systems should be designed to offer substantial protection against even a small group of insiders working together.

A database with information from the 1960s to 2013 contains a total of 119 nuclear and radiological incidents, of which at least 20 were committed by insiders or with insider support. Thomas Megghammer’s database codes for motivation (“political” or “apolitical”), attack type (“facility attack,” “radiological dispersion,” or “other”), and insider involvement (“yes” or “no”). Table I. summarizes the findings and illustrates the proportion of insider attacks.

In 40 of the 58 incidents caused by politically motivated individual, the overall objective was identified as the damage or destruction of vital equipment at nuclear facilities, or the capture of facilities. Ten plots were disrupted by law enforcement agencies, while the 11th was aborted by terrorists. In 17 incidents explosives were planted and detonated. Additionally, terrorists launched 12 armed assaults—including four suicide bomb attacks—against eight military sites reportedly holding nuclear arms and against four civil nuclear plants. The eight remaining incidents at nuclear facilities have been acts of sabotage, conducted with unknown or non-weaponry equipment.

Table I. Distribution of Serious Nuclear and Radiological Incidents Worldwide 1960-2013 by Motivation, Attack Type, and Insider Involvement [4]

Motivation		Attack Type		Insider	
Political	58	Facility attack	40	Yes No/unknown	3 37
		Radiological dispersion	12	Yes No/unknown	1 11
		Other	6	Yes No/ unknown	0 6
Unknown	22	Facility attack	22	Yes No/ unknown	9 13
Apolitical	39	Facility attack	14	Yes No/Unknown	4 10
		Radiological dispersion	25	Yes No/ unknown	3 22
Total	119			Yes No/ unknown	20 99

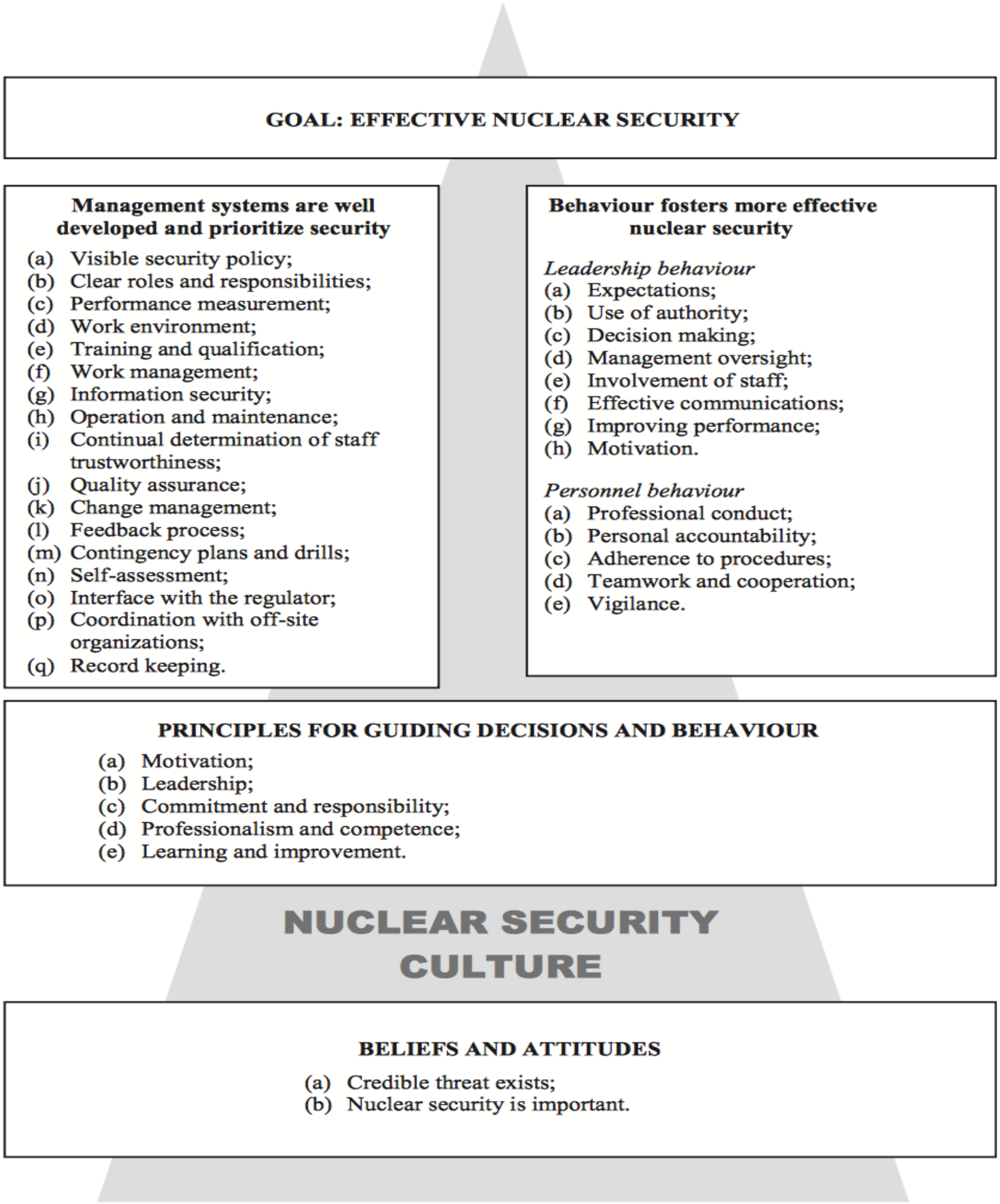
It is important to avoid the “myth of absolute security”—the belief that a facility is already completely secure—which is never correct and will lead to complacency. This is the enemy of preparedness and limits the effectiveness of prevention, detection, protection, and mitigation. More importantly, while prevention of insider threat is a high priority, managers should never succumb to the temptation of minimizing emergency response and mitigation efforts in an attempt to maintain the illusion that there is nothing to be afraid of.

One of the reasons why nuclear security culture is proposed in this paper as a tool to deal with insider threat and its consequences is because the IAEA Implementing Guide on Insider Threat explicitly recognizes that “an absence of security culture, security awareness and trustworthiness programs may be favorable or conducive to insider attempts to perform malicious acts.” [5] The human factor focused approach described in the IAEA Implementing Guide on Nuclear Security Culture (NSS No.8) provides a unique opportunity to use security culture as an instrument to deal with insider threat. Also notably important is that previously applied methods were largely based on the qualifications, motivations and attitudes of the people directly or indirectly involved in their implementation, which makes security culture an attractive choice as a mechanism for prevention and protection.

3. Security Culture Applicability

The 2008 IAEA model of nuclear security culture (see Figure 1) has 30 characteristics and lists 120 culture indicators that are assigned to each characteristic in order to illustrate their meaning.

Figure 1. IAEA Nuclear Security Culture Mode l [7]



GOAL: EFFECTIVE NUCLEAR SECURITY

Management systems are well developed and prioritize security

(a) Visible security policy;
(b) Clear roles and responsibilities;
(c) Performance measurement;
(d) Work environment;
(e) Training and qualification;
(f) Work management;
(g) Information security;
(h) Operation and maintenance;
(i) Continual determination of staff trustworthiness;
(j) Quality assurance;
(k) Change management;
(l) Feedback process;
(m) Contingency plans and drills;
(n) Self-assessment;
(o) Interface with the regulator;
(p) Coordination with off-site organizations;
(q) Record keeping.

Behaviour fosters more effective nuclear security

Leadership behaviour
(a) Expectations;
(b) Use of authority;
(c) Decision making;
(d) Management oversight;
(e) Involvement of staff;
(f) Effective communications;
(g) Improving performance;
(h) Motivation.

Personnel behaviour
(a) Professional conduct;
(b) Personal accountability;
(c) Adherence to procedures;
(d) Teamwork and cooperation;
(e) Vigilance.

PRINCIPLES FOR GUIDING DECISIONS AND BEHAVIOUR

(a) Motivation;
(b) Leadership;
(c) Commitment and responsibility;
(d) Professionalism and competence;
(e) Learning and improvement.

BELIEFS AND ATTITUDES

(a) Credible threat exists;
(b) Nuclear security is important.

The culture indicators constitute a framework under which management can reflect upon the status of security culture and facilitate change and development by promoting desirable and discouraging undesirable behavior.

The IAEA Draft Technical Guidance for Self-Assessment of Nuclear Security Culture in Nuclear Facilities and Activities is under review and is due for release by the Agency in 2018. In the meantime, this assessment methodology has been successfully applied in Indonesia, Bulgaria, and Malaysia. The draft technical guidance is based on the IAEA model and expands the list of culture indicators to over 300.[8] The self-assessment is a multi-stage process comprising both non-interactive and interactive assessment tools (surveys, interviews, document review, observation) focusing on management and behavior characteristics. Due to the heavy focus on perceptions, views, and behavior, regularly held comprehensive assessments help us better understand personnel behavior in certain circumstances and their root causes.

Surveys are important to self-assessment because they establish a baseline for tracking changes over time. Survey statements are derived from culture indicators, and respondents are asked to grade each statement based on a 7-point scoring system. The 7-point scale ranges from 1 (Strongly Disagree) to 7 (Strongly Agree). *Interviews* play a significant role in cultural assessment because they allow for flexible questioning and follow-up clarifications from interviewees. This eases the task of getting at the deeper tenets of an organization's culture. *Observations* allow organizations to record actual performance and behavior in real time and under different circumstances.

The cycle of regular assessments focusing on culture characteristics relevant to insider threat will keep these risks under continuous scrutiny in a NSC framework, rather than implementing separate and often disconnected initiatives. Involving a considerable portion of the workforce in surveys, interviews, and focus groups will not only enable organizations to identify culture weaknesses conducive to insider threat, but also serve as a sustainable learning experience to complement classroom training formats. Continuous focus on NSC as well as organization-wide dissemination of self-assessment reports may deter potential insiders.

4. Selection of Cultural Characteristics

At least six of the total 30 security culture characteristics in the IAEA model are directly linked to the widely used practices designed to deal with insider threat. They are to be selected together with their associated indicators for use in a security culture self-assessment. Depending on the profile of the organization and the capacity of its personnel to perform self-assessment, such characteristics will identify culture weaknesses and strengths, that generate beliefs, assumptions, and attitudes that may lead to malicious attitudes or encourage security awareness. Culture indicators associated with these characteristics should be used as statements for surveys (quantitative data), further explored during interviews (qualitative data), and carefully evaluated in the process of observation (qualitative data). Below are the six characteristics recommended for the insider threat focused self-assessment process.

1. Continuous determination of trustworthiness –MS(i)

   Trustworthiness determination is an initial and ongoing assessment of an individual’s integrity, honesty, and reliability in pre-employment checks and checks during employment that are intended to identify the motivations or behavior of persons who could become insiders. The checks attempt to identify factors such as greed, financial status, ideological intents, psychological considerations, desire for revenge due to perceived injustice, physical dependency on drugs, alcohol or sex, and factors due to which an individual could be coerced by outsiders with malicious intentions.

2. Work environment –MS(d)

   This characteristic is known as employee satisfaction. It implies that a professional work ethic/attitude of staff members and management should be given due consideration and should be a part of the security culture. As adopted from the General Strain Theory[1] (GST) in criminology, organizational strains (mismatching expectations, sanction pressures, jobs dissatisfaction, low prestige, and others) can lead to perceived organizational injustice eventually leading to noncompliance and deliberate or even unintended malicious acts. [9]

3. Adherence to procedures –PB(c)

   This characteristic implies compliance with the entire range of preventive and protective measures recommended in the IAEA Implementing Guide on Insider Threat. They include administrative measures (procedures, instructions, rules) and technical measures (protection layers, accounting hardware) designed to prevent malicious acts from being carried out. Their objective is to detect, delay, and respond to them, as well mitigate their possible consequences. An effective nuclear security culture will motivate personnel to prioritize and comply with their implementation or lack thereof will lead to shoddy performance.

4. Training and qualifications –MS(e)

   This characteristic’s focus is to determine and raise security awareness among personnel about insider threat and the possible consequences of malicious acts for everybody (the stakeholders, the company and its staff). The purpose is to establish an environment in which all employees are mindful of security policies and procedures, so that they can aid in detecting and reporting inappropriate behavior or acts. Security awareness raising should also provide measures to reduce the possible consequences of blackmail, coercion, extortion or other threats to employees and their families. Security awareness raising programs should be developed in a coordinated manner with safety programs in order to establish effective and complementary safety and security cultures. It is important for management to ensure that security awareness concerning insider threat is

[1] More information on the General Strain Theory can be found in “AGNEW, R., “Building on the Foundation of General Strain Theory: Specifying the Types of Strain Most Likely to Lead to Crime and Delinquency,” Journal of Research in Crime in Delinquency, Vol. 38, November 2001, pp.319-361

fully integrated into the overall facility's nuclear operational culture and its self-assessment cycle.

5. Vigilance –PB(e)

   The success of any measures to deal with insider threat depends on both vigilance and observational skills of personnel. An appropriate questioning and reporting (feedback) attitude should be encouraged throughout the organization. To this end, personnel should be motivated and trained to observe behavior, recognize suspicious behavior, and properly handle those who exhibit such threatening behavior. Reporting unusual activities or behavior should be everyone's responsibility. Personnel should understand that the security and safety of their coworkers and themselves are at stake. Multiple layers of security working toward the same goal will provide a larger probability of stopping insider threat before a malicious act occurs.

6. Personnel accountability –PB(b)

   Accountability for actions and a clear understanding of consequences are a strong deterrent for potential insider threat. Violators are averse to being caught and are more likely to act when they believe they will not be discovered. Successful insider threat programs have shown that establishing and promoting clear accountability for actions and setting expectations and boundaries for staff conduct have significant potential for dealing with insider threat.

   Table II provides samples of culture indicators for the six characteristics recommended for an insider threat focused self-assessment process.

Table II. Samples of Culture Indicators for Characteristics Relevant to Insider Threat Prevention and Protection [8]

Continuous Determination of Trustworthiness	Work Environment	Adherence to Procedures
• The process of background checks is periodically reviewed • Screening processes are matched to the risks and threats associated with specific roles and responsibilities • Real or apparent failures of the screening process are appropriately investigated and adjudicated • Leaders provide support and resources for effective implementation of trustworthiness programs. • Staff is aware of and understand the importance of trustworthiness determination	• Management show that professional capabilities and experience are the most valuable assets • Managers make themselves approachable and call for effective two-way communication • Dissenting views, diverse perspectives and robust discussion are appreciated • Security is considered a respectable career-enhancing profession • Performance-improvement processes encourage staff to offer innovate ideas	• Personnel understand potential consequences of noncompliance • Instructions on security are easy to follow because they are clear, up to date, easily available and user friendly • Leaders lead by example and—as is expected from all staff—adhere to policies and procedures in their personal conduct • The organization actively and systematically monitors security performance through multiple means
Training and Qualifications	Vigilance	Personal Accountability
• Training materials include good practices and lessons learned from security breaches • Training programs at the organization address security-conscious behavior as a key element of professionalism • Systems are in place to ensure procedures and practices learned in training are applied in practice • Security awareness training instructs all staff on proper workplace security as well as requirements for reporting security violations	• Personnel notice and question unusual behavior and incidents and report them to management as soon as possible using the established procedures • Personnel seek guidance when they are unsure of the security significance stemming from unusual events, observations or incidents • Personnel are aware of a potential insider threat and its consequences • A policy prohibiting harassment and retaliation for raising nuclear security concerns is enforced	• Personal accountability is clearly defined in appropriate policies and procedures • Personnel consider themselves responsible for security at the organization • Personnel understand how their specific tasks support the nuclear security system • Behavior that enhances security culture is reinforced by peers

With the six characteristics and their associated indicators as the primary focus, the self-assessment process can identify numerous culture weaknesses in the organization as a precursor to security breaches and/or factors leading to insider risks. Such risks may be attributed to gaps in trustworthiness determination; inconsistent practices for dealing with organizational strains; inadequate adherence to prescribed preventive and protective measures; poorly managed personnel training; lack of a systemic approach to vigilance enforcement; and deficient personnel accountability. There may be others but it is up to the management to determine the choice of characteristics and indicators as well as the assessment scale. These culture assessment findings will help the management to calibrate its insider threat program and designate specific tasks to deal with insider threat.

5. Conclusion

The value of security culture self-assessment as a tool to address insider threat is in its systemic and comprehensive nature. The issue of insider threat is carefully examined through the prism of overall organizational culture, of which security is a major subset. Periodically held self-assessments focus on a wide range of topics falling under the general heading of nuclear security. Self-assessment teams are free to incorporate any culture characteristics and indicators of their choice, which would continuously keep under scrutiny potential root causes of malicious acts, as well as diagnose the identified weaknesses to prevent such actions from ever occurring. Like other evaluation methods, this approach is far from being perfect, but it is multifunctional and can effectively support other currently applied methods and compensate for their possible limitations.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008), p.3.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Plan 2010-2013, Report by IAEA Director General, GOV 54-GC (53)(18), IAEA, Vienna (2009).

[3] MOORE, C., “Anatomy of a £26.5 million Heist,” Sunday Life, 21 May 2006.

[4] BUNN, M., SAGAN, S., “Insider Threat”, Ithaca and London: Cornell University Press (2016), p.24.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, Implementing Guide, IAEA Nuclear Security Series No.8, IAEA, Vienna, 2008, p.6.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series No.7, IAEA, Vienna, 2008.

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Self-Assessment of Nuclear Security Culture in Nuclear Facilities and Activities, IAEA Draft Technical Guidance, NST026, 2 July 2014, IAEA, Vienna.

[9] AGNEW, R., “Building on the Foundation of General Strain Theory: Specifying the Types of Strain Most Likely to Lead to Crime and Delinquency,” Journal of Research in Crime in Delinquency, Vol. 38, November 2001, pp.319-361.