BEST PRACTICES FOR ADDRESSING RISK FROM EMPLOYEES AT LOW POWER RESEARCH REACTOR FACILITY IN NIGERIA

Y. V. Ibrahim
Centre for Energy Research and Training,
Ahmadu Bello University, Zaria, Nigeria

J. Simon
Department of Physics,
Ahmadu Bello University, Zaria, Nigeria

A. Asuku
Centre for Energy Research and Training,
Ahmadu Bello University, Zaria, Nigeria

P. D. Lynch
Oak Ridge National Laboratory,
Oak Ridge, Tennessee, USA

ABSTRACT

Since the declaration of atoms for peace at the United Nations General Assembly in New York City on 8 December, 1953 by US President Eisenhower, peaceful applications of nuclear technology and research programs offered many benefits including the formation of the International Atomic Energy Agency (IAEA) in 1957 that will promote such applications. Upon realizing the benefits that could be derived from atoms, Nigeria joined the IAEA in 1964. Currently, Nigeria operates a low power research reactor at the Centre for Energy Research and Training (CERT) used mainly for research and teaching and host of Category 1, 2 and 3 sources for various applications such as in food irradiation, radiotherapy and industrial applications in Oil and Gas sector. These benefits are not without associated risks such as natural disasters, accidents and deliberate acts. Of particular concern is the risk from use of material in a radiological dispersal device or improvised nuclear device, the sabotage of the facility, theft or diversion of materials and/or technology, as well as information. Nigeria is steadfast in its commitment to mitigate rising national and global terrorism. Nigeria faces domestic issues that may lead to potential economic motives to steal and sell nuclear material, criminal activities such as kidnapping and unforeseen economic downturns and Terrorism, all of which could lead to a perception of the CERT site as an attractive target. One of the biggest threats facing the nuclear industry today is the insider, who likely has approved access to nuclear materials or radioactive sources, the ability to introduce malicious code, leak information to outside groups with malicious intent, sabotage a facility, as well as other detrimental acts. Nearly all known nuclear thefts or sabotage incidents appear to have been perpetrated by or with help from insiders. In order to continue to benefit from peaceful nuclear programs and research, we discuss Nigeria's risk-based, multi-layered security to address the insider threat at its low power research reactor.

INTRODUCTION

The purpose of this paper is to describe best practices at low power research reactor to mitigate against insider threat who might steal material or sabotage facility. Nigeria employs the use of nuclear technology for several applications in research, medicine, agriculture and \oil and gas exploration. The Nigeria Research Reactor-1 (NIRR-1) is situated at the Centre for Energy Research and Training (CERT), Ahmadu Bello University (ABU), Zaria. It is one of the Miniature Neutron Source Reactor (MNSR) designed and manufactured by the China Institute of Atomic (CIAE) having a rated power of 31 kW mainly for neutron activation analysis, research and education [1]. There are nine of such research reactors in the world, four in China and 5 outside China. Initially, the MNRS is fuelled with High Enriched Uranium (HEU), however, the NIRR-1 have since been converted to Low Enrichment fuel [2] in support of Nigeria's commitment to reduce proliferation risk.

Nigeria derives benefits from peaceful application of nuclear technology not only through the use of the research reactor but also in medicine, agriculture and the Oil and Gas industry. The continuous use of nuclear technology for socio-economic development of any country is not without some risks like natural disasters, accidents and deliberate acts.

Of particular concern is the risk from use of material in a radiological dispersal device or improvised nuclear device, the sabotage of the facility, theft or diversion of materials as well as information. Their malicious use especially in a radiological-dispersion device (RDD), can have severe environmental and economic impacts, social, and potentially large clean-up costs, as well as other effects on the operators and the public. These issues are important to Nigerian state, regulators and the public.

In the face rising national domestic issues and global terrorism, the potential economic motives to steal and sell nuclear material due to criminal activities such as kidnapping and unforeseen economic downturns and terrorism could lead to a perception of the CERT site as an attractive target. Nearly all known nuclear thefts or sabotage incidents appear to have been perpetrated by or with help from insiders [3]. The insider, who likely has approved access to nuclear materials or radioactive sources has the ability to introduce malicious code, leak information to outside groups with malicious intent, sabotage a facility, as well as other detrimental acts. In order to preserve the nuclear industry and continue to benefit from peaceful application of nuclear technology, we discuss Nigeria's risk-based, multi-layered security to address the insider threat at its low power research reactor.

Multi-layered security to address insider threat within CERT include information security, personnel security, administrative security, and physical security to eliminate single points of failure.

NUCLEAR SECURITY THREATS

Peaceful application of nuclear technology offers many benefits but also certain risks, that includes: Accidents involving release of radioactive material – Sabotage of facilities – Theft or diversion of materials, technology, or information – Use of material in a radiological dispersal device or improvised nuclear device. Five threat scenarios have been identified in literature if nuclear and or radioactive materials are not well protected [4]. These threat scenarios are:

a) acquisition and use of nuclear weapons,
b) use of improvised nuclear devices (INDs) fabricated from stolen nuclear material,
c) use of radiological dispersal devices (RDDs) fabricated from stolen radioactive material,
d) use of radiological exposure devices (REDs) fabricated from stolen radioactive material, and
e) sabotage against a nuclear facility or a transport with nuclear or radioactive material.

THREAT LANDSCAPE FOR NUCLEAR INSIDER INCIDENTS

Insider threat remains the biggest nuclear security challenge faced by the nuclear industry [3] while organisations are still in doubt of the existence of insiders in their organizations [5], at the CERT facility top management staff believe insider threats are real which is reinforced by lessons from past incidents in literature [6, 7, 8, 9, 10, 11]. Additionally, several issues have been considered by the management to believe insider threat is real. such issues include:

a) Rising Global terrorism
b) Domestic issues that could lead to nuclear terrorism
c) Financial needs to steal and sell nuclear material and information
d) Criminal activities
e) Unforeseen economic downturns or socio-political changes

Therefore, implementing multi-layered strategy to mitigate the insider threat is necessary to avert potential consequences of malicious use of nuclear and radioactive material and to continue to derive benefits from peaceful applications of nuclear technology as well as preserve the nuclear industry.

Insider has a lot of capabilities in a nuclear and or radiological facilities hence theft of nuclear and or radioactive material will require the insider. Such capabilities may include knowledge, access and authority. The insider can select optimum time to implement plan, utilize tools at work, test systems with normal “mistakes”, collude with others (insiders or outsiders) and extend acts over long periods of time. The possible insider threats at nuclear and or radiological facilities may include theft of nuclear materials or radioactive sources, Introduction malicious code, leaking information to an outside group with malicious intent, sabotaging a facility, collusion with outsiders, substance abuse, personal irresponsibility, fatigue, espionage and lack of training.

COUNTERING INSIDER THREAT AT CERT FACILITY

Security Policy/Procedures

The effectiveness of security at any facility begins with a policy on security. CERT facility has a security policy that have overarching priority over operations and profit. these policies include:

a) Employee hiring policy, including background check and random drug-testing
b) Access control policy, including authorized exclusion list for personnel access
c) Incident reporting policy
d) Memorandum of Understanding with local law-enforcement agencies
e) Control of sensitive information

f) Security Procedures to prevent an incident, as well as those taken to respond to it comprising of:
    - Response force's security post orders and procedures
    - Security training procedures
    - Alarm assessment (manual and remote)
    - Alarm-response procedures (covering remote- and manual-assessments)
    - Incident-reporting procedures
    - Local law-enforcement contact and reporting procedures
    - Incident-containment procedures
    - Key control- and access-procedures
    - Procedures for facility access after normal working-hours
    - Procedures for sign-out logbook
    - Preventative maintenance of the installed equipment
    - Arming and disarming sensors
    - System-configuration changes
    - Placing malfunctioning equipment out-of-service while awaiting repairs
    - Testing system's performance Physical security hardware Upgrades which include
    - Hardened doors (no glass in them) and high-strength mechanical locks
        i. Access control systems
        ii. Intrusion-detection and assessment systems
        iii. Balanced magnetic sensors
        iv. Recessed door and window sensors
        v. Duress switches in device rooms and proximal locations
        vi. Volumetric sensors (motion detectors) in the device room, approach corridors, and exclusion zones
        vii. Tamper-proof connectors (case-hardened, requiring non-standard tools for removal)
        viii. Sirens, alarms and strobe lights
        ix. Alarm enunciation at the Central Alarm Station (CAS)
g) Employee Training

Human Reliability Programme

Human Reliability Programme (HRP) is a "security and safety reliability program designed to ensure that individuals who occupy positions with access to certain nuclear materials (including information), facilities, and programs meet the highest standards of: "reliability (an individual's ability to adhere to security and safety rules and regulations), Trustworthiness (confidence in an individual based on his/her character), and Physical and mental suitability…" (o).

The first step towards developing an HRP is consultation with experts. CERT in collaboration with subject matter experts at the University of Tennessee and Oak Ridge National Laboratory in the United States of America trained its staff on trustworthiness programme for development of its HRP. In the development of its facility specific HRP, facility characterization, Vulnerability assessment and Job task analysis were conducted to identify HRP positions (critical positions). Individuals occupying critical positions were then trained on the HRP requirements and their responsibilities. The CERT HRP requirements include: Initial Evaluation, Annual and continuous

evaluations. Elements of Initial evaluation are: Background check, arrest check, credit check, education verification, work history verification and security evaluation. Annual and continuous evaluations requirements are: Drug test, Alcohol test, arrest check, financial review, unusual behaviour observation and training others are supervisory review, medical appraisal, management decision and Certifying Official Review. Random test is also carried out on HRP individuals.

Contractors and regulators who visit the facility on temporary basis are always escorted by facility security personnel and operators to ensure they are at the right place and performing the right duties. In this situation, the escort personnel are informed about their specific activities and are required to detect and deter malicious activities.

In addition, all employees at the facility are trained on security threats and potential consequences of malicious acts and of their own role in reducing.

Establishing an HRP provide CERT the opportunity of having reliable and trustworthy employees, strengthens facility safety and security culture and maintaining strong technical work force.

Material Control and Accounting

The Material Control and Accounting (MC&A) is a program that ensures that nuclear material is properly protected and that it is not removed from its authorized location without approval or timely detection. CERT MC&A is used to "to enhance nuclear security through timely detection of any unauthorized removal of nuclear material and providing deterrence against such possible actions. Through MC&A programme, CERT is able to maintain and annually reports to the regulatory authority accurate, timely, complete and reliable information on all activities and operations involving nuclear material, including the locations, quantities and characteristics of nuclear material at its facility.

The material surveillance is primarily concerned with detection of insider adversary activities through personnel observation to detect unauthorized activities such as: movements of nuclear material, tampering with containment of nuclear material, falsification of information related to location and quantities of nuclear material, tampering with safeguards devises. Locations of nuclear materials are clearly identified and if material is not in assigned location, material may be considered missing. Two things may happen: CERT will commence immediate investigations and report to the regulatory authority.

For effective material surveillance, two-man-rule is instituted with the individuals maintaining direct control of items, unobstructed view of each other and/or the item(s), ability to positively detect unauthorized or incorrect procedures and having appropriate training. Reactor fuels and other safeguard materials at the facility are monitored weekly to ensure nuclear material is in its authorized location for timely detection of loss of material. Additionally, Tamper Indicating Device (TID) is utilized such that a malevolent act cannot be accomplished without permanently altering the item or TID in a manner that would be obvious during visual inspection.

Administrative Controls

CERT has written policies, procedures, standards and guidelines for all levels of employees from top to bottom staff including contract staff for its day-to-day operations. Procedure for accessing critical areas is strictly adhered to and is implemented though access control. accessing vital areas requires two-man rule.

Compartmentalize Facility/Work Area

Through its access control system, no one person can access the reactor facility and material balance area. Access to the reactor facility is compartmentalized comprising of security personnel and operators in the control area and two operators to the control room. Access to the material balance area will require the material custodian, security and operator (three-man rule).

Prosecution of Individuals

The Nigerian Nuclear Regulatory Authority issued two regulations namely: the Nigerian Safety and Security of Radioactive Sources Regulations and the Nigerian Regulations on Physical Protection of Nuclear Material and Nuclear Facilities. The objective of the former is to reduce the likelihood of accidental harmful exposure or the malicious use of radioactive sources by preventing: unauthorized access, damage, loss, theft and unauthorized transfer while the latter is to protect against unauthorized removal of nuclear material, protect against sabotage and mitigate or minimize the radiological consequence of sabotage. any violation to these regulations by either the operating organization or employee would have firm consequences.

Physical Security

Most recently, CERT in collaboration with US Department of State upgraded its Physical Security System immediately after conversion of the reactor from the use of HEU to LEU. These include: Access control systems, Intrusion-detection and assessment systems, Balanced magnetic sensors, Volumetric sensors, Sirens, alarms and strobe lights, Cameras Alarm enunciation at the Central Alarm Station in addition to existing visible security patrol that helps to deter malicious insider from attempting to remove nuclear and or radioactive material from the facility.

Training

CERT facility requires that all staff have the qualifications, knowledge and skills required to perform their duties. Personal occupying critical positions receive initial and annual training on the need for an HRP, insider risks, nuclear security awareness and their security responsibilities. The management of CERT ensures continuous improvement in staff skills and work to prevent complacency from achieving the security objectives. This is done through weekly seminars on topical issues including security.

Additionally, the management create a mechanism for analysing security events in other industries, including those from other nuclear facilities and corrective actions are taken based on

the outcome of the analysis. The management engage in other activities that enhance security at the facility. such activities include: Internal audit of the security management systems for which it is responsible to identify and correct weaknesses, drills and exercises to test the performance of security systems, as well as the human factor, analysis of patterns and trends arising from known deficiencies and implement corrections, observation operational performance to confirm that expectations are being met, periodic review of training programs, benchmark performance to compare operations with national and international best practices, maintaining an awareness of the state of the art in security procedures, processes, and equipment so that security personnel have appropriate tools with which to implement security costs effectively implementing a comprehensive program regarding the required periodic maintenance, repairs, and occasional modification of the nuclear security equipment to match evolving threat.

CONCLUSIONS

Insider threat is a unique problem to the nuclear industry and no "one size fits all" solution. Using the "Defense in Depth" approach will apply multiple layers of security controls to help mitigate the actions of a malicious insider.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the Centre for Energy Research and Training, Ahmadu Bello University, Zaria, The US Department of State, University of Tennessee, Knoxville and the Oak Ridge National Laboratory for the valuable contributions that made this paper possible.

REFERENCES

[1] Iliyasu, U, Ibrahim, Y. V., Umar, S., Agbo, S. A., Jibrin, Y., 2017. An investigation of reactivity effect due to inadvertent filling of the irradiation channels with water in Nigeria Research Reactor-1. Applied Radiation and Isotopes, 123 11-16.

[2] SAR, 2019. Safety Analysis Report for the Nigeria Research Reactor-1

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, 2013. Insider Threats in Comparative Perspective. Proceedings of the International Nuclear Security: Enhancing Global Efforts, Vienna, July 1-5, 2013.

[4] International Nuclear Security Education Network, 2009: Introduction to Nuclear Security, INSEN Textbook Series, 2009.

[5] Bunn, M. and Sagan, S., 2014. A Worst Practice Guide to Insider Threats: Lessons from Past Mistakes. Cambridge mass., American Academy of Arts and Sciences, 2014.

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, 2016. IAEA Incident and Trafficking Database (ITDB): Incidents of Nuclear and Other Radioactive Material out of Regulatory Control, 2016 Fact Sheet, http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf.

[7] CBS NEWS, Nuke Facility Raid an Inside Job? CBS Interactive, 20 November 2008, www.cbsnews.com/8301-18560_162-4621623.html.

[8] Mackey, R., Have Pakistani Nuclear Facilities Already Been Attacked? The Lede, The New York

Times News Blog, 11 August 2009, thelede.blogs.nytimes.com/2009/08/11/have-pakistaninuclear-facilities-already-been-attacked/.
[9] Grossman, E., European Nuclear Base Security Tightened over Years, U.S. Brass Says, Global Security Newswire, National Journal, 20 September 2012, www.nationaljournal.com/nationalsecurity/european-nuclear-base-security-tightened-over-years-u-sbrass-says-20120920.
[10] Basrur, R., and Steinhausler, F., 2014. Nuclear and Radiological Terrorism Threats for India: Risk Potential and Countermeasures, The Journal of Physical Security 1 (1), 2004.
[11] Potter, W., 1997. Nuclear Terrorism and Nuclear Diversion in Russia, NTI: Nuclear Threat Initiative, 20 August 1997, www.nti.org/analysis/articles/less-well-known-casesnuclear-terrorism-and-nuclear-diversion-russia/.