October 24, 2014

MEMORANDUM TO: Catherine Haney, Director
Office of Nuclear Material Safety
and Safeguards

FROM: Marissa G. Bailey, Director **/RA/**
Division of Fuel Cycle Safety, Safeguards
and Environmental Review
Office of Nuclear Material Safety
and Safeguards

SUBJECT: CONSIDERATIONS TO DEFEND AGAINST UNAUTHORIZED DISCLOSURE OF ENRICHMENT OR REPROCESSING TECHNOLOGY AND THE DIVERSION OF ASSOCIATED NUCLEAR MATERIALS

In response to your e-mail request regarding the original draft of the enclosure, dated September 9. 2014, we have contacted Region II, the Office of the General Counsel, and the Office of Nuclear Security and Incident Response for review of the draft enclosure. Several minor changes have been made to address their comments, and we now have their approval.

The staff plans to have this transmittal memorandum and the final enclosure noted on the external website http://www.nrc.gov/about-nrc/ip/intl-safeguards.html with a brief description of the document and origin, as well as its U.S. Nuclear Regulatory Commission Agencywide Documents Access and Management System accession number. To further bring notice to it, the Office of Public Affairs will announce the existence of this memo and enclosure through the agency's Twitter account.

If you have any questions, please contact James A. Smith at 301-287-9138, or via e-mail to James.Smith@nrc.gov.

Enclosure:
Non-Proliferation Considerations

CONTACT: James Smith, NMSS/FCSE
301-287-9138

MEMORANDUM TO: Catherine Haney, Director
Office of Nuclear Material Safety
and Safeguards

FROM: Marissa G. Bailey, Director **/RA/**
Division of Fuel Cycle Safety, Safeguards
and Environmental Review
Office of Nuclear Material Safety
and Safeguards

SUBJECT: CONSIDERATIONS TO DEFEND AGAINST UNAUTHORIZED DISCLOSURE OF ENRICHMENT OR REPROCESSING TECHNOLOGY AND THE DIVERSION OF ASSOCIATED NUCLEAR MATERIALS

In response to your e-mail request regarding the original draft of the enclosure, dated September 9. 2014, we have contacted Region II, the Office of the General Counsel, and the Office of Nuclear Security and Incident Response for review of the draft enclosure. Several minor changes have been made to address their comments, and we now have their approval.

The staff plans to have this transmittal memorandum and the final enclosure noted on the external website http://www.nrc.gov/about-nrc/ip/intl-safeguards.html with a brief description of the document and origin, as well as its U.S. Nuclear Regulatory Commission Agencywide Documents Access and Management System accession number. To further bring notice to it, the Office of Public Affairs will announce the existence of this memo and enclosure through the agency's Twitter account.

If you have any questions, please contact James A. Smith at 301-287-9138, or via e-mail to James.Smith@nrc.gov.

Enclosure:
Non-Proliferation Considerations

CONTACT: James Smith, NMSS/FCSE
301-287-9138

DISTRIBUTION:

FCSS, r/f	OSiurano, FCSS	RidsNmss,FCSS	PHolahan, NSIR
JKEverly, NSIR	DHase, NSIR	BStapleton/NSIR	DSeymour, Reg II
OSmith, Reg II	LPitts, Reg II	MLessar, RII	JHickey, RII
LCuadrado, FCSS	TGrice, FCSS	TPham, FCSS	

ADAMS Accession No. : ML14294A700

OFFICE	FCSE/ECB	FCSE/ECB	FCSE/ECB	FCSE
NAME	JSmith	DMiller	BSmith	MBailey
DATE	10/22/14	10/22/14	10/22/14	10/24/14

OFFICIAL RECORD COPY

CONSIDERATIONS TO DEFEND AGAINST UNAUTHORIZED DISCLOSURE OF ENRICHMENT OR REPROCESSING TECHNOLOGY AND THE DIVERSION OF ASSOCIATED NUCLEAR MATERIALS

PURPOSE

The U.S. Nuclear Regulatory Commission (NRC) has prepared this document to provide a non-inclusive set of considerations that applicable fuel cycle facilities could implement to enhance their facilities and/or processes in their ability to prevent, detect, and defend against unauthorized disclosure of enrichment or reprocessing (ENR) technology and diversion of nuclear materials. The examples or considerations may also be considered for the design of future ENR facilities.

DESCRIPTION OF CIRCUMSTANCES

On November 10, 2010, Dr. Francis Slakey, on behalf of the American Physical Society, submitted a petition for rulemaking (PRM-70-9) to the NRC. The petition requested that the NRC amend its regulations to require each applicant for an ENR facility license to include in its application an assessment of the proliferation risks associated with the construction and operation of the proposed facility, since new ENR technologies could pose unique proliferation risks.

The Commission denied the petition PRM-70-9, but recognized it provided information indicative of the degree of proliferation risk in authorizing an ENR facility to be constructed and eventually operated. The NRC is providing a discussion of areas of consideration, which while not necessary for the NRC to review to ensure public health and safety or common defense and security, are areas that may be addressed by the licensee/applicant to complement the NRC's requirements with respect to proliferation risks.

The NRC's primary concern is to ensure that the facilities it regulates that manufacture or use enriched uranium and plutonium do so safely and securely. The NRC's regulations on physical security, information security, material control and accounting, cyber security, and export control address proliferation risks of ENR technology and facilities. However, regulations are not intended to limit licensees from going beyond NRC regulatory requirements, if appropriate, to further protect against unauthorized access to ENR technology, equipment, and nuclear material.

In addition to these activities being covered by the NRC in its review of ENR license applications, the U.S. is a party to international treaties and agreements that address non-proliferation obligations. The most notable are the Non-Proliferation Treaty, the U.S. – International Atomic Energy Agency (IAEA) Safeguards Agreement, and Additional Protocol to the U.S. – IAEA Safeguards Agreement. These agreements place requirements on the U.S. Government that the NRC helps to implement through Title 10 of the *Code of Federal Regulations* (10 CFR) Part 75 – "Safeguards on Nuclear Material – Implementation of U.S./IAEA Agreement," and 10 CFR Part 110 – "Export and Import of Nuclear Equipment and Material."

DISCUSSION

The NRC's regulatory requirements in 10 CFR Parts 25, 73, 74, 75, 95, and 110 address proliferation concerns by imposing requirements for the protection of sensitive/classified information, technologies, and materials, including that related to ENR facilities.

The NRC has seen, through its oversight program, industry practices not specifically required by the regulations, which provide additional layers of protection against unauthorized access and disclosure of ENR technology, equipment, and nuclear material. In an effort to keep licensees informed of proactive measures to foster the nonproliferation of nuclear material and technology, below is a set of considerations in the area of information security, cyber security, physical protection, and material control and accounting.

Information Security

- Enhancements set forth in the Nuclear Energy Institute's (NEI) 08-11, "Information Security Program Guidelines for Protection of Classified Material at Uranium Enrichment Facilities" and NEI 13-04, "Counterintelligence Program for Uranium Enrichment Facilities." These documents, endorsed by the NRC, include the following programs for the protection of classified information and matter:

    1. Operations Security Program.
    2. Telecommunications Electronic Materials Protected from Emanating Spurious Transmissions Program.
    3. Technical Surveillance Countermeasures Program.
    4. Counterintelligence Program.
    5. Information Technology Security requirements for classified networks.
    6. Classified Item Control and Inventory requirements.
    7. Counterintelligence Program.

- Segregation of Unrelated Classified Elements. The need-to-know principles may be applied to classified information, equipment, and materials in a manner that minimizes the potential agglomeration of information. For example, a machinist might machine a classified part, but not be informed of its intended use. Similarly, the operator of the machine in which the classified part is a component may know how to operate the machine, but not be informed of the internal classified components. In the development of the technology, components or steps in the classified processes could be separated physically or visually, so that individuals would only be allowed access to that part of the process that is required for them to perform their function, without providing an overarching understanding of the interrelatedness of the different processes in the technology. A similar approach could be taken for the design and layout of the facility.

Cyber Security

- Guidelines in National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cyber Security, February 12, 2014. The National Institutes for Standards and Technology (NIST) Cyber Security Framework is a voluntary risk-based cyber security framework of industry standards and best practices to help organizations

manage cyber security risks and designed to allow management of cyber security risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. The NIST Framework focuses on identification of digital assets, protection measure that can be employed, detection capabilities, response actions, and recovery of operations. The NIST Framework applies to non-classified systems/networks only. Specific requirements exist for classified networks, with which licensees must comply with.

- Isolation of Critical Systems. Critical digital assets performing safety, security (physical and information), emergency preparedness, and material control and accounting functions may be afforded additional protection by isolation of the systems from unrelated systems, many of which may present vulnerabilities due to connection to the Internet.

Physical Security

- Maximized Line-Of-Sight Through Building Designs/Layouts. Buildings may be designed to minimize inset doorways, protruding support structures, or similar impediments to visual pathways to ensure a clear line-of-sight for security staff, closed circuit cameras and alarm sensors, and limit potential locations for individuals to hide or divert material.

- Additional Access Controls. Access controls beyond those required by the regulations may serve as "administrative controls" to further restrict personnel access to areas containing ENR-related information, materials and equipment. These additional "administrative controls" may be useful to further segregate the facility to minimize the risk of unauthorized access, movement, or removal of information, material, and equipment and serve as a deterrent to potential theft and diversion scenarios due to the increased likelihood of timely detection and ready ability to identify individuals who have accessed the specific area.

- Closed Circuit Cameras and/or Additional Alarm Sensors. The use of closed circuit cameras and/or additional alarm sensors may serve as a significant deterrent against possible malevolent acts. They may also provide early indications of potential unauthorized activities and assist in the investigation and resolution of potential incidents.

Material Control and Accounting

- Multiple Material Balance Areas or Additional Key Measurement Points. Dividing a facility into multiple material balance areas or establishing additional key measurement points may allow a facility to more easily identify, isolate, and resolve inventory differences. These actions may also serve as a deterrent to potential theft and diversion scenarios because of the increased likelihood of timely detection.

- Tamper Protection and Measurement Equipment/Systems. Most measurement systems rely on mechanical components or electrical signals that can be adjusted as part of the routine calibration process. While designed to allow an operator to ensure accurate

measurements, this also introduces system vulnerabilities, allowing the measurement system to be manipulated to mask a potential theft or diversion of material. Utilizing enclosures or a tamper-indicating device may prevent these actions.

- Two-Person Rule Beyond Regulatory Requirements. Application of a two-person rule at critical points in a process can serve multiple purposes. It can provide assurance that certain actions (e.g., conducting measurements, applying tamper-indicating devices, recording information, etc.) are performed correctly. The presence of the second individual also protects against potential theft and diversion scenarios by a malevolent insider.

Other Resources for Safeguards Guidance

- The National Nuclear Security Administration: Next Generation Safeguards Initiative (NGSI) sponsors a project promoting international Safeguards by Design (SBD). NGSI has developed a series of facility-specific guidance documents for designers and operators to be used as SBD reference documents. They can be found on the NNSA website at: http://nnsa.energy.gov/aboutus/ourprograms/dnn/nis/safeguards/sbd.

- The IAEA has a listing of its documents to assist its member States in understanding the implementation of IAEA safeguards. These documents can be found at: http://www.iaea.org/safeguards/resources-for-states/additional-documents.html.