POLICY ISSUE
Notation Vote

February 24, 2015 SECY-15-0026

FOR: The Commissioners

FROM: Mark A. Satorius
Executive Director for Operations

SUBJECT: INSIDER THREAT PROGRAM POLICY AND IMPLEMENTATION PLAN

PURPOSE:

The purpose of this paper is to provide the Commission with the Insider Threat Program (ITP) Policy Statement and Implementation Plan (Enclosures 1 and 2), for consideration. The development and implementation of an ITP is required by Executive Order (EO) 13587 *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (October 7, 2011).

BACKGROUND:

EO 13587 directs all executive branch departments and agencies (hereafter "agency, agencies") that have access to classified information to implement an insider threat detection and prevention program (hereafter "program"). The purpose of the program is to deter, detect, and mitigate insider threats to national security. The EO also created an interagency National Insider Threat Task Force (NITTF) to develop minimum standards and guidance for implementation of a government-wide insider threat policy. The NITTF National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs (Minimum Standards) were issued by the White House November 21, 2013.

CONTACT: Todd Masse, NSIR/DSO
301-492-3933

The National Insider Threat Policy defines an “Insider Threat” as the threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. The U.S. Nuclear Regulatory Commission’s (NRC) ITP is limited to insider threats, as defined by the National Insider Threat Policy, and does not extend to other types of threats, such as the threat of workplace violence.

EO 13587 applies to the safeguarding and sharing of classified national security information and the staff proposes to include safeguards information, protected under the *Atomic Energy Act of 1954* (AEA), as amended, in the NRC’s program. Additionally, an agency may apply the program to information that it considers sensitive but that is not classified, and/or to its other critical assets—those elements of the agency’s mission that are essential to the agency and to national security and which, if damaged, stolen, or otherwise exploited, would have a damaging effect on the agency, its mission, and national security. The staff is not proposing to include Sensitive Unclassified Non-Safeguards Information in the program.

Since mid-2013, agencies subject to EO 13587 were expected to complete three actions described in the National Insider Threat Policy. The first – the designation of the Director of the Office of Nuclear Security and Incident Response (NSIR) as the NRC Senior Agency Official (SAO) for overseeing classified information sharing and safeguarding efforts – was provided to the White House in May 2013 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML13050A465). The second and third deliverables – respectively, an NRC policy on insider threat and an NRC implementation plan on insider threat have been the subject of extensive internal discussion since 2013 and are attached here for the Commission’s consideration. The White House requested an approved agency policy and implementation plan by January 7, 2015.

DISCUSSION:

EO 13587 directs United States Government agencies to establish, implement, monitor, and report on the effectiveness of ITPs to protect classified national security information (as defined in EO 13526 “Classified National Security Information” (December 29, 2009), and requires the development of a program for the deterrence, detection, and mitigation of insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. The staff proposes to include restricted data under the AEA in the NRC’s program, and references to “classified information” in the proposed NRC program include restricted data under the AEA. The EO 13587 is applicable to all agencies with access to classified information, or that operate or access classified computer networks; all employees with access to classified information, including classified computer networks (and including contractors and others who access classified information, or operate or access classified computer networks controlled by the Federal Government); and all classified information on those networks. In a December 22, 2011, memorandum to the Commission, the Office of the General Counsel (OGC) summarized the EO and concluded that it is applicable to the NRC (ADAMS Accession No. ML11356A073).

In accordance with the Minimum Standards, the NRC ITP involves the monitoring of all classified information and networks, as well as the monitoring of personnel who have access to classified systems and information. Due to their nature, the NRC’s existing programs for

personnel security, physical security and facilities access, computer systems monitoring, personnel training, and information security all provide a baseline level of protection against insider threats at the NRC. While these programs contribute to protection against insider threats, they lack a centralized assessment function to determine if activities or behaviors, individually or collectively, indicate that an individual may be an insider threat.

The NRC ITP is an event-driven program which fully leverages existing NRC resource programs. Therefore, it focuses primarily on individuals who have high-level, broad, or frequent access to classified information and computer systems. The structure of the ITP consists of a centralized entity (also referred to as the Hub), staffed by personnel from NSIR, the Office of Administration (ADM), and OGC, to perform an appropriate level of assessment and lead follow-up. The Hub makes recommendations to the NRC's SAO for insider threat (Director, NSIR) on insider threat matters. The SAO consults with an advisory team, composed of representatives from ADM, the Office of the Chief Human Capital Officer, the Computer Security Office (CSO), the Office of Information Services, and others, as necessary, to approve or disapprove the opening of insider threat inquiries. It is expected that individuals with high-level, broad, and frequent access to classified information or networks will be more likely to be referred to the SAO by the Hub than individuals who lack such access. However, individuals who may be an insider threat, regardless of their scope of access, may be processed through the Hub to determine if a recommendation to the SAO is appropriate. It is also important to note that while not required by EO 13587, the NRC program would similarly cover personnel who have access to safeguards information systems and information. Additional details on the proposed NRC program are provided in the enclosed Implementation Plan.

Access to Records

The general rule of the Privacy Act is that an agency shall not disclose (even internally) any record about an individual without prior written consent of that individual unless a statutory exception applies. Disclosure of records in NRC Privacy Act Systems of Record to the program will be pursuant to either the "internal need to know" or the "routine use" exceptions. The NRC will establish a new Privacy Act system of records for the program. Prior to such establishment, subject to an established need or routine use, the program will review records controlled by other NRC stakeholder offices without retaining those records. Once an ITP System of Records is established, these records could be retained by the program, as part of the ITP System of Records, consistent with the new system of records notice. For this new System of Records, the Privacy Act requires publication of a System of Records Notice in the *Federal Register* (describing, among other things, the collection purpose and routine uses of the information contained in the system and a description of notification and record access procedures for individuals access to their records), for comment, as well as provide advance notice to Congress and the Office of Management and Budget.

The program also contemplates the possibility of referring information to external law enforcement entities. Prior to implementation of the program, this "routine use" must be noticed in the *Federal Register* for a given system, disclosed on any form used for direct collection of the information, and must be compatible with the purpose for which the information was originally collected for prior direct collections of information. Not all NRC systems allow for this type of external disclosure. Notably, the NRC has historically declined to allow, for policy reasons, some records to be referred to external law enforcement agencies, including: NRC-2 (Biographical Information); NRC-19 (Official Personnel Training); NRC-35 (Drug Testing); and

NRC-36 (Employee Locator Records). Of these four systems, the program contemplates the use of systems NRC-2, NRC-19, and NRC-36. The program proposes to change the use of these systems of records to include law enforcement purposes, going forward.

The Commission has the discretion to determine the categories of records that should be available to the program, and the purposes for which the program may use the records. Alternatively, the Commission may determine that other policy justifications weigh in favor of not using a particular system of records in the insider threat program.

Next Steps

While insider threat programs are inherently sensitive, given the nature of the information being considered and the need to balance national security interests with the legal rights of employees under the Privacy Act and other statutory protections, the staff has developed a policy and implementation plan that is cognizant of such needs and includes appropriate levels of legal and independent oversight. A number of issues, including the program's access to NRC records and an employee's ability to access and amend Privacy Act records[1] will continue to be discussed as the program is implemented. The enclosures provide a first step in bringing the NRC into compliance with EO 13587 requirements on insider threat. Any approved program will be subject to continual oversight and change as the program matures and is advised by outside experts, including the NITTF.

Once the Commission approves an NRC Insider Threat Policy and Implementation Plan, the NRC staff will notify the NITTF that these actions have been completed, and will begin implementing the program. In accordance with EO 13587, and the White House Memorandum transmitting the Insider Threat Minimum Standards, the ITP is required to perform internal program oversight and assessments and to facilitate external assessments by members of the NITTF. Internally, there are two annual reviews – one a self-assessment conducted by the NRC's SOA in conjunction with ITP management, and an oversight review conducted by NRC individuals independent of the ITP who would provide the independent oversight report to the NRC's Executive Director for Operations. The staff has been tasked with providing the results of the first self-assessment to the Commission (SRM-WH121121). Externally, the NITTF will conduct an independent assessment of the NRC's ITP. In the first year of program operation, the periodicity of program oversight will be reasonably frequent in order to ensure that the program is operating in compliance with applicable law and policy.

RECOMMENDATION:

The staff examined the possibility of providing options for an NRC ITP. In doing so, staff considered the White House Memorandum outlining the ITP Minimum Standards, an estimation of insider threat workload for a non-U.S. Code Title 50, "War and National Defense" (NT-50) agency, the valued input of both NITTF officials and internal NRC experts, as well as assessments of more mature NT-50 ITPs. The staff believes the roadmap for an NRC ITP outlined herein (including the enclosed policy and implementation plan documents) meets the Minimum Standards requirements, will be acceptable to NITTF officials, is reasonably scoped

[1] The NRC staff are concerned that permitting employee access to ITP records could threaten to vitiate the intent of the Executive EO; however, the NRC is limited in its ability to restrict an individual's access to Privacy Act records.

and resourced for an emerging ITP within an NT-50 organization, and fully leverages existing NRC resources.

The staff recommends that the Commission approve the proposed Insider Threat Policy Statement for publication as a final statement of policy in the *Federal Register* (Enclosure 1).

The staff recommends that the Commission approve the staff's Insider Threat Program Implementation Plan (Enclosure 2).

RESOURCES:

In developing the proposal for the program and determining the scope of the resource needs, the staff prepared a detailed estimate related to creation and implementation of an insider threat program (Enclosure 3). Given that the program relies heavily, to the extent practicable, on existing NRC programs, staff proposes an estimate of approximately $1 M and 3.5 full-time equivalent (FTE) in fiscal year (FY) 2015 and $1M and 3 FTE in FY 2016. Resources for FY 2017 and beyond will be addressed through the Planning, Budgeting, and Performance Management process.

There are three broad cost elements associated with the program: (1) personnel, (2) stand-alone computer network establishment and annual operation and maintenance, and (3) secure space for the Hub. The computer network will contain sensitive personnel information provided to the Hub to evaluate potential insider threats and the Hub's analysis of the information. The CSO will need additional equipment to enhance its network monitoring capability. Ultimately, the resources necessary to staff the program will be driven by the workload, which is difficult to assess with accuracy in the absence of a program with at least an initial operating capability. As outlined in the Implementation Plan, the ITP leverages existing NRC resources as a way to reduce the impact on staff offices, particularly those that will provide information to the Hub. The staff has asked that each participating office and region identify an individual to act as a point of contact between that office or entity and the ITP. As part of the annual self-assessment once the program is operational, all aspects of the program will be reviewed and adjustments recommended as necessary. As discussed in Enclosure 3, the staff will conduct an evaluation of the resource requirements for the program after the first year of program implementation and the program resources will be adjusted, as appropriate, based on this assessment.

The resources outlined in Enclosure 3 are pre-decisional information and should be treated as Official Use Only – Sensitive Internal Information.

COORDINATION:

OGC has reviewed this package and has no legal objection. The Office of the Chief Financial Officer reviewed this package for resource implications for NSIR only, and concurred.

/RA/

Mark A. Satorius
Executive Director
for Operations

Enclosures:
1. Draft NRC Insider Threat Program Policy Statement
2. NRC Insider Threat Implementation Plan (Official Use Only)
3. Resources to Support the NRC's Insider Threat Program (Official Use Only)

COORDINATION:

OGC has reviewed this package and has no legal objection. The Office of the Chief Financial Officer reviewed this package for resource implications for NSIR only, and concurred.

/RA/

Mark A. Satorius
Executive Director
for Operations

Enclosures:
1. Draft NRC Insider Threat Program Policy Statement
2. NRC Insider Threat Implementation Plan (Official Use Only)
3. Resources to Support the NRC's Insider Threat Program (Official Use Only)

ADAMS Accession No: Pkg: ML14338A111 Ticket No: W2013000017

OFFICE	NSIR/DSO/ILTAB	NSIR/DSO	Region I	Region II	Region III	Region IV
NAME	T. Masse	M. Layton	JTrapp for	SFlynn for	RDoornbos for	EClay for
DATE	12/18/14	12/04/14	12/15/14	12/15/14	12/15/14	12/11/14
OFFICE	NMSS	ADM	OCFO	OIG	NRR	NRO
NAME	KJones for	JShay for	LYee for	J. McMillan	BHolian for	MMayfield for
DATE	12/15/14	12/16/14	12/17/14	12/11/14	12/15/14	12/15/14
OFFICE	OI	OIP	OCHCO	CSO	RES	OIS
NAME	KFowler for	GLanglie for	M. Cohen	JFeibus	BRini for	RWebber for
DATE	12/15/14	12/10/14	12/16/14	12/17/14	12/15/14	12/16/14
OFFICE	OGC	NSIR	EDO			
NAME	MZobler - NLO	JWiggins	M. Satorius			
DATE	12/23/14	12/29/14	02/ 24 /15			

OFFICAL RECORD COPY