POLICY ISSUE
(Notation Vote)

April 29, 2016 SECY-16-0057

FOR: The Commissioners

FROM: Victor M. McCree
Executive Director for Operations

SUBJECT: INSIDER THREAT PROGRAM IMPLEMENTATION PLAN

PURPOSE:

The purpose of this paper is to provide the Commission with a draft Insider Threat Program (ITP) Implementation Plan for approval. This paper also discusses current initiatives or activities by the Office of Administration (ADM) and the Office of Nuclear Security and Incident Response (NSIR) to reduce the U.S. Nuclear Regulatory Commission's (NRC's) classified holdings, access points, safes, and number of employees with access to classified information.

BACKGROUND:

Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" (October 7, 2011), directs all executive branch departments and agencies that have access to classified information to implement an ITP. The purpose of the program is to deter, detect, and mitigate insider threats to national security. The E.O. also created an interagency National Insider Threat Task Force (NITTF) to develop minimum standards and guidance for implementation of a governmentwide insider threat policy. On November 21, 2012, the White House issued the NITTF's "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs."

CONTACT: Denis Brady, ADM/DFS
(301) 415-5768

On February 24, 2015, the staff submitted SECY-15-0026, "Insider Threat Program Policy and Implementation Plan," (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14338A123) for Commission consideration. The Commission approved the ITP Policy Statement and it was published in the *Federal Register* on February 25, 2016. The scope of the NRC's program includes classified information, including restricted data, and safeguards information. The policy statement applies to all NRC employees, contractors, and detailees to the NRC from other government agencies who have national security clearances and access to classified information, including restricted data, and/or safeguards information. Note that the NRC's ITP and implementation plan do not cover NRC licensees, licensee contractors or subcontractors, certificate holders, or permittees with access to classified and/or safeguards information. These entities are required to protect classified and/or safeguards information in accordance with the requirements set forth in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 95, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," and/or 10 CFR Part 73, "Physical Protection of Plants and Materials."

In addition, the Commission disapproved the proposed implementation plan provided with SECY-15-0026 and directed the staff to submit a revised plan for Commission approval consistent with the policy statement. The Commission also directed the staff to examine options for reducing the NRC's classified holdings, access points, safes, and the number of employees with access to classified information.

DISCUSSION:

The staff convened the ITP Working Group which consisted of staff from various offices, as well as staff from the Office of the Inspector General, to develop a revised program implementation plan. The working group focused on developing an implementation plan that is consistent with the Commission-approved ITP policy statement and that does not require the creation of a new Privacy Act system of records, as was previously proposed. The working group focused its efforts on also ensuring that implementation plan is aligned with the NITTF standards issued by the White House. Consistent with NRC's Project AIM initiative, the staff's implementation plan creates a program that leverages existing resources and processes as much as possible without creating new ones. For example, the ITP will rely on existing computer networks, and the implementation plan establishes the Insider Threat Assessment Team (ITAT), which is modeled after the processes included in the Protective Threat Assessment Team model. This interoffice group will have the role of discussing and assessing potential insider threats as detailed in the enclosure. The implementation plan also provides a procedure for conducting insider threat response actions that the ITAT would follow. The proposed implementation plan also establishes the training requirements for employees, contractors, detailees, and those who are a part of the NRC's Insider Threat Assessment Team. Working group members from the Office of the General Counsel and the Office of the Chief Human Capital Officer worked to ensure that employees' civil liberties, civil rights, and privacy rights are protected throughout the process. Additionally, OGC developed a legal standard to begin an inquiry which has been incorporated into the enclosed implementation plan throughout the program's response process.

Finally, the staff examined options for reducing the NRC's classified holdings, access points, safes, and the number of employees with access to classified information. ADM and NSIR have planned numerous initiatives to reduce the NRC's classified holdings, access points, and number of safes. Beginning in April 2016 and annually thereafter, ADM will lead the agency in conducting classified and safeguards information clean-up days. On these clean-up days, headquarters and regional office staff are encouraged to go through their materials and determine if anything needs to be destroyed, archived, or reviewed by NSIR for declassification.

The first clean-up day was held on April 14, 2016, and the staff collected a total of 32 boxes of paper material and two boxes of media including hard drives for destruction. Additionally, ADM and NSIR have developed a General Services Administration (GSA) safe security plan for agencywide implementation by September 2016. This plan places training requirements on safe owners and requires annual inventory/cataloging of information being stored in each safe. Furthermore, ADM will issue a yellow announcement that provides clarifying language for the definition of need-to-know in Management Directive (MD) 12.0, "Glossary of Security Terms," and MD 12.1, "NRC Facility Security Program," to better assist staff in making need-to-know determinations for any category of information. Also, on a continuous basis, NSIR conducts reviews of staff with access to sensitive computer systems to ensure those with access continue to require access. The staff has also developed a paper proposing to reduce the number of employees with clearances and access to classified information; that paper is currently with the Commission for consideration.

RECOMMENDATION:

The staff recommends that the Commission approve the enclosed ITP Implementation Plan.

RESOURCES:

In order for the staff to implement the user activity monitoring portion of the enclosed implementation plan, the agency would need to reallocate in Fiscal Year (FY) 2017 and subsequent years less than a full-time equivalent (FTE) staff split between ADM and NSIR. These resources will be reallocated from lower priority work and will be used to conduct near real-time (i.e., next business day) review and analysis of the monitoring data of classified and safeguards information computer systems as required by the NITTF's minimum standards. Elimination of lower priority work will offset the long-term annual projected resource need. All other actions and assignments in the enclosed implementation plan are collateral duties. Therefore for the purposes of this resource estimate they are not considered as a change from the current level of effort.

COORDINATION:

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

This paper is marked "Official Use Only – Sensitive Internal Information" due to the sensitive nature of the enclosure. Not only does the enclosure contain predecisional information, it also

contains internal processes and positions that will be used to implement the program. If the information is released to the public or widely distributed internally, a person could exploit the program's techniques and procedures and possibly thwart the program. When separated from the enclosure, the staff believes this paper is suitable for public release.

/RA/

Victor M. McCree
Executive Director
for Operations

Enclosure:
Draft Insider Threat Program
Implementation Plan

contains internal processes and positions that will be used to implement the program. If the information is released to the public or widely distributed internally, a person could exploit the program's techniques and procedures and possibly thwart the program. When separated from the enclosure, the staff believes this paper is suitable for public release.

/RA/

Victor M. McCree
Executive Director
for Operations

Enclosure:
Draft Insider Threat Program
Implementation Plan

ADAMS Accession No.: ML16075A120 **Ticket No.: SRM-S15-0026-2**

OFFICE	ADM/DFS/FSB	QTE	ADM/DFS/FSB/BC	ADM/DFS/DD	ADM/DFS/D	OI/D
NAME	ARoundtree	CHsu	DBrady	SSchoenmann	TPulliam	KFowler
DATE	03/16/2016	03/16/2016	03/18/2016	03/18/2016	03/18/2016	03/29/2016
OFFICE	NSIR/D	OIG/D	OCHCO/D	ISD/D	OCIO/D	OCFO
NAME	BHolian	JMcMillian	MGartman for MCohen	TRich	FBrown	RAllwein for MWylie
DATE	03/29/2016	03/24/2016	03/25/2016	03/29/2016	03/29/2016	03/30/2016
OFFICE	ADM/DD	ADM/D	OGC/D	DEDM	EDO	
NAME	SStewart-Clark	CCarpenter	MMaxin	DDorman	VMcCree	
DATE	03/31/2016	03/31/2016	04/11/2016	04/ 27 /2016	04/ 29 /2016	

OFFICIAL RECORD COPY