[7590-01-P]

NUCLEAR REGULATORY COMMISSION

[NRC-2016-0033]

Nuclear Regulatory Commission Insider Threat Program Policy Statement

AGENCY: Nuclear Regulatory Commission.

ACTION: Policy statement; issuance.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is issuing its Insider Threat Program Policy Statement that establishes the NRC Insider Threat Program in accordance with Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." The purpose of the policy statement is to ensure the responsible sharing and safeguards of classified information, including restricted data and safeguards information, by deterring employees, contractors, and detailees holding national security clearances from becoming insider threats, detecting insiders who pose a risk to protected information, and mitigating risks.

DATES: The NRC's Insider Threat Program Policy Statement is effective February 25, 2016.

ADDRESSES: Please refer to Docket ID NRC-2016-0033 when contacting the NRC about the availability of information for this policy statement. You may access publicly-available information related to this policy statement by any of the following methods:

- **Federal Rulemaking Web Site:** Go to http://www.regulations.gov and search for Docket ID NRC-2016-0033. Address questions about NRC dockets to Carol Gallagher; telephone: 301-287-3422; e-mail: Carol.Gallagher@nrc.gov. For technical questions, contact the individual listed in the FOR FURTHER INFORMATION CONTACT section of this document.
- **NRC's Agencywide Documents Access and Management System (ADAMS):** You may obtain publicly-available documents online in the ADAMS Public Documents collection at http://www.nrc.gov/reading-rm/adams.html. To begin the search, select "ADAMS Public Documents" and then select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, 301-415-4737, or by e-mail to pdr.resource@nrc.gov. The ADAMS accession number for each document referenced in this document (if that document is available in ADAMS) is provided the first time that a document is referenced.
- **NRC's PDR:** You may examine and purchase copies of public documents at the NRC's PDR, Room O1-F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852.

FOR FURTHER INFORMATION CONTACT: Denis Brady, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; telephone: 301-415-5768; e-mail: Denis.Brady@nrc.gov.

SUPPLEMENTARY INFORMATION:

I. Background

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," directs all executive branch departments and agencies that have access to classified information to implement reforms to ensure responsible sharing and safeguarding of classified information on computer networks, consistent with appropriate protections for privacy and civil liberties (76 FR 63811; October 13, 2011). The E.O. also established the National Insider Threat Task Force, which issued the "National Insider Threat Policy" and the "Minimum Standards for Executive Branch Insider Threat Programs" on November 21, 2012 (*see* https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand, last visited February 8, 2016). In order to execute its primary mission essential functions, the NRC has access to and possesses classified information, including classified information on computer networks, which it protects through appropriate security procedures. This policy statement establishes the NRC's Insider Threat Program in accordance with E.O. 13587.

II. Discussion

The purpose of this policy statement is to ensure the responsible sharing and safeguards of classified information, including restricted data and safeguards information, by deterring employees, contractors, and detailees holding national security clearances from becoming insider threats, detecting insiders who pose a risk to protected information, and

mitigating risks. The policy statement addresses the background, purpose, applicability, policy components, and references. This policy statement is not applicable to members of the public.

The NRC's Insider Threat Program Policy Statement is published in its entirety in the attachment to this document, and is also available in ADAMS under Accession No. ML16039A282.

III. Procedural Requirements

Paperwork Reduction Act Statement

This policy statement does not contain information collection requirements and, therefore, is not subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

Congressional Review Act

This policy statement is not a rule as defined in the Congressional Review Act (5 U.S.C. 801-808).

Dated at Rockville, Maryland, this 18th day of February, 2016.

For the Nuclear Regulatory Commission.

/RA/

Annette L. Vietti-Cook,
Secretary of the Commission.

ATTACHMENT – NUCLEAR REGULATORY COMMISSION INSIDER THREAT PROGRAM POLICY STATEMENT

1. Background. Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," directs all executive branch departments and agencies that have access to classified information to implement reforms to ensure responsible sharing and safeguarding of classified information on computer networks that are consistent with appropriate protections for privacy and civil liberties (October 7, 2011). The Executive Order also established the National Insider Threat Task Force, which issued the "National Insider Threat Policy" and the "Minimum Standards for Executive Branch Insider Threat Programs" on November 21, 2012. In order to execute its primary mission essential functions, the Nuclear Regulatory Commission (NRC) has access to and possesses classified information, including classified information on computer networks, which it protects through appropriate security procedures.

2. Purpose. This document establishes the NRC Insider Threat Program (ITP) Policy in accordance with E.O. 13587 and the Atomic Energy Act of 1954, as amended (AEA). The primary purpose of the ITP is to protect information classified under E.O. 13526 or section 142 of the AEA (restricted data), or that is safeguards information under section 147 of the AEA, as well as any such information on classified networks, by deterring employees holding national security clearances from becoming insider threats, detecting insiders who pose a risk to the protected information, and mitigating risks. The establishment of an NRC ITP is intended to achieve these goals with respect to all NRC employees, contractors, and detailees with national security clearances and access to information classified under E.O. 13526 or section 142 of the AEA or that is safeguards information under section 147 of the AEA.

3. Applicability. This policy is applicable to all NRC employees, contractors, and detailees to the NRC from other government agencies who have national security clearances and access to information classified under E.O. 13526 or section 142 of the AEA or that is safeguards information under section 147 of the AEA.

4. Policy. It is NRC policy that:

(a) All NRC employees, contractors, and detailees must comply with the requirements of all current and applicable Federal laws, regulations, and policies concerning the responsible sharing and safeguarding of classified information. This includes reporting insider threat information related to potential espionage, violent acts against the Government or the Nation, and unauthorized access to or disclosure of information classified under E.O. 13526 or section 142 of the AEA or that is safeguards information under section 147 of the AEA, and any such information that is available on interconnected U.S. Government computer networks and systems.

(b) Consistent with established law and policy, including the Privacy Act, the ITP uses information made available to it to identify, analyze, and respond to potential insider threats at the NRC. The ITP itself does not maintain or store any personal information. The information is maintained by the program office in which the information resides.

(c) All NRC employees, contractors, and detailees involved in any ITP actions (including, but not limited to, gathering information or conducting inquiries) do so in accordance with all applicable Federal laws, regulations, and policies, including those pertaining to whistleblower protections, civil liberties, civil rights, criminal rights, personnel records, medical records, and privacy rights. The ITP consults with and obtains the concurrence of the NRC's Office of the General Counsel (OGC) on questions concerning these legal protections in insider threat activities, inquiries, assistance in investigations by law enforcement authorities, and other matters.

(d) The ITP refers to the U.S. Federal Bureau of Investigation (FBI) information indicating that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power, in accordance with 50 U.S.C. § 3381(e). Subject to an appropriate inquiry by the ITP, other information indicating unauthorized access to or misuse of classified information, classified networks, or safeguards information is referred to the NRC's Office of Inspector General (OIG). OGC will provide ongoing legal advice to the ITP as appropriate.

5. References.

A. The Atomic Energy Act of 1954, as amended; 42 U.S.C. § 2011 *et. seq.*

B. 50 U.S.C. § 3381(e).

C. Inspector General Act of 1978, as amended; 5 U.S.C. Appx § 1 *et seq.*

D. Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953 (18 FR 2489; April 29, 1953).

E. Executive Order 12333, "United States Intelligence Activities," dated December 4, 1981 (as amended by Executive Orders 13284 (2003), 13355 (2004), and 13470 (2008) (46 FR 59941; December 8, 1981).

F. Executive Order 12829, "National Industrial Security Program," dated January 6, 1993 (58 FR 3479; January 8, 1993).

G. Executive Order 12968, "Access to Classified Information," dated August 4, 1995 (60 FR 40245; August 7, 1995).

H. Executive Order 13526, "Classified National Security Information," dated December 29, 2009 (75 FR 707; January 5, 2010).

I. Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," dated October 7, 2011 (76 FR 63811; October 13, 2011).

J. NRC Management Directive 7.4, "Reporting Suspected Wrongdoing and Processing of OIG Referrals."

K. NRC Management Directive, Volume 12, "Security."