U.S. Nuclear Regulatory Commission

INSIDER THREAT PROGRAM POLICY STATEMENT

DRAFT

1. Background. A substantial number of classified documents compromised by Bradley Manning and released to the WikiLeaks organization harmed U.S. national security and resulted in the passage of 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). The White House established the National Insider Threat Task Force, which issued the "National Insider Threat Policy" and the "Minimum Standards for Executive Branch Insider Threat Programs" (November 21, 2012). The Commission may control information pursuant to chapter 12 of the Atomic Energy Act of 1954, as amended, in order to protect the common defense and security. In order to execute its primary mission essential functions, the U.S. Nuclear Regulatory Commission (NRC) has access to and possesses classified information which it protects through appropriate security procedures.

2. Purpose. This document establishes the NRC Insider Threat Program (ITP) Policy in accordance with EO 13587 and the Atomic Energy Act of 1954, as amended. The purpose of the ITP is to: deter employees holding national security clearances and those with access to safeguards information from becoming insider threats, detect insiders who pose a risk to classified information (including restricted data under the Atomic Energy Act) and safeguards information, and mitigate the risks through administrative inquiries or other responsive actions. The establishment of an NRC ITP is intended to achieve these goals with respect to all NRC employees, contractors with National Security Clearances or access to safeguards information, and detailees with National Security Clearances or access to safeguards information (hereafter referred to as "contractors" and "detailees", respectively). While the primary purpose of the ITP is to protect classified information, information on classified networks, and safeguards information, the successful execution of this program will necessarily involve the monitoring of both classified and unclassified networks.

3. Applicability. This policy is applicable to all NRC regional offices, headquarters, training facilities, employees, contractors, and detailees to the NRC from other government agencies.

4. **Policy**. It is NRC policy that:

(a) All NRC employees, contractors, and detailees assigned to the NRC must comply with the requirements of all current and applicable Federal laws, regulations, and policies concerning the responsible sharing and safeguarding of classified and safeguards information. This includes reporting Insider Threat and related counterintelligence information related to potential espionage, violent acts against the Government or the Nation, and unauthorized access to or disclosure of classified information, classified data available on interconnected U.S. Government computer networks and systems, and safeguards information.

(b) Consistent with established law and policy, including the Privacy Act, the ITP will use information available to it necessary to identify, analyze, and respond to potential insider threats at the NRC.

(c) ITP personnel, agency personnel, contractors and all detailees at NRC facilities involved in any ITP actions (including, but not limited to, gathering information, maintaining information, or conducting inquiries) shall 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. The ITP will consult the NRC's Office of the General Counsel on questions concerning these legal protections in insider threat activities, inquiries, assistance in investigations by law enforcement authorities, and other matters.

(d) The ITP shall refer to the Federal Bureau of Investigation 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. Subject to an appropriate inquiry by the ITP, other information indicating unauthorized access to or misuse of classified information, classified networks, or safeguards information will be referred to the Office of Inspector General (OIG) and/or another appropriate authority.

5. **References**

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

B. Executive Order 13587 of October 7, 2011, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"

C. Executive Order 12968 of August 4, 1995, "Access to Classified Information"

D. Executive Order 13526 of December 29, 2009, "Classified National Security Information"

E. Section 811 of the Intelligence Authorization Act for fiscal year (FY) 1995; 50 U.S.C. § 3381 (2014)

F. Executive Order 12333 of December 4, 1981 (Amended), "United States Intelligence Activities"

G. Executive Order 10450 of April 27, 1953, "Security Requirements for Government Employment"

H. Inspector General Act of 1978

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

J. NRC Management Directives Volume 12, "Security"

K. Executive Order 12829, "National Industrial Security Program (NISP)"