Jefferson Lab

Insider Threat Plan

5 June 2023

U.S. DEPARTMENT OF ENERGY

JSA

Prepared for the U.S. Department of Energy
under Contract DE-AC05-06OR23177

Revision History		
Rev.	**Date**	**Reason**
0	24 August 2018	Embedded within the Site Security Plan
1	10 March 2020	Appendix to the Site Security Plan
2	05 June 2023	Correction to Security Plan Appendix Numbering

Table of Contents

References

- DOE O 470.5, Insider Threat Program, Attachment 1 CRD.
- TJNAF's Incidents of Security Concern Program Plan.
- Executive Order 13587, National Insider Threat Policy.
- Site-Specific Counterintelligence Support Plan.

1. Insider Threat Procedures Purpose

TJNAF's insider threat program is to help deter, detect, and mitigate insider threat actions. The procedures outlined apply to all programs in an integrated manner that may address threats to personnel, facilities, material, information, equipment and other DOE or United States Government assets.

2. Local Insider Threat Working Group (LITWG)

- Chief Operating Officer (COO). As Chair of the TJNAF LITWG, the COO is principally responsible to ensure data, information, systems, and any other support to the DOE Insider Threat Program is provided in accordance with applicable laws, regulations, policies, directives and other requirements.
- Other core members of the TJNAF LITWG include the Facility Security Officer, the Human Resources Manager, Chief Information Security Officer, and General Counsel.
- Additional TJNAF resources will be called on for support as needed. Resources that assist in the detection and mitigation of insider threats include the collection and proper documenting of data, data sources, and data formats in the regular course of cybersecurity operations.
- Designated LITWG members are responsible for developing and maintaining a collaborative environment to identify, coordinate, and integrate local activities to address insider threats. In addition, designated members ensure that DOE information system usage banners are properly approved.
- Upon detection of a potential threat from an insider, notification will be made to the Chair or FSO to convene a meeting of the LITWG to review the available information and determine a plan of action consistent with TJNAF's Incident of Security Concern Program Plan and other relevant guidance.

3. Definitions

- Access: The ability and opportunity to obtain knowledge of sensitive information.
- Classified Information: Information that has been determined to require protection against unauthorized disclosure and that is marked to indicate its classified status when in document form.
- Cleared Contractor: A person or facility operating under the National Industrial Security Program (NISP) that has an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level (and all lower levels).
- Contact: Any form of meeting, association, or communication in person; by radio, telephone, letter, computer; or other means, regardless of who initiated the contact or social, official, private, or other reasons.
- Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations' conducted for or on behalf of foreign powers, organizations, or persons, or their agents.
- Insider: Any person with authorized access to any United States resource to include personnel, facilities, information, equipment, or systems.

- Insider threat: Means the threat that an insider will use his/her 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 classified information, or through the loss or degradation of U.S. Government resources or capabilities. Insider Threat Response Actions mean activities conducted to ascertain whether certain matters or information indicates the presence of an insider threat, as well as activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of Counterintelligence, Security, Law Enforcement, or Inspector General elements depending on statutory authority and internal policies governing the conduct of such in each agency.

4. Reporting Potential Insider Threats

- DOE Reporting Procedure: Thomas Monaghan DOE Office of Intelligence and Counterintelligence (OCI), TJNAF Phone: 757-269-5989, DOE 202-586-7353, Thomas.Monaghan@doe.gov
- TJNAF's Employee Concerns Hotline/Website: 888-296-8301 or https://secure.ethicspoint.com/domain/media/en/gui/22925/index.html
- TJNAF's Facility Security Officer, 757-269-7548