

		Security Management System Processes and Procedures	
Procedure Number/Name Local Insider Threat Working Group and Charter		Original Date: 03/28/2017	
Written by: T.I. Meyer	Reviewed and Updated By: T.I. Meyer	Date: 06/02/2017	

Revision History

Author	Description of Change	Revision Date
T.I. Meyer	Finalize formatting, list approvals	06/01/2017

PURPOSE OF THIS PROCEDURE

Pursuant to DOE Order 470.5, the purpose of the Insider Threat Program is to deter, detect, and mitigate insider threat actions by Federal employees, contractor employees, or authorized users in accordance with the requirements of Executive Order 13587, and other government-wide and DOE requirements.

This program is being developed and maintained at Fermi National Accelerator Laboratory (FNAL) to deter, detect, mitigate, analyze and respond to insider threats.

REFERENCES

- DOE Order 470.5
- Fermilab Site Security Plan
- Security Management System description

DEFINITIONS

Insider: An “Insider” is any person with authorized access to any government or contractor resource to include personnel, facilities, information, equipment, networks or systems;

Insider Threat: An “Insider Threat” is an insider that will use his/her authorized access, wittingly or unwittingly, to do harm to FNAL, or the security of the United States. This threat can include damage to FNAL, or the United States through espionage, terrorism, unauthorized disclosure of classified information, or through the loss or degradation of U.S. Government resources or capabilities. In essence, anyone that has access to FNAL, whether physical or remote, potentially poses a threat to the laboratory;

Insider Threat Response Action(s): Any activities conducted to ascertain whether certain matters or information indicates the presence of, or potential for 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 DOE;

Fermilab Local Insider Threat Working Group (LITWG): A core group of FNAL personnel whom are tasked with implementing policy actions, and exchange information and foster close working relationships with FNAL management, subject matter experts, and other essential internal/external partners to continue to detect, deter, and mitigate the insider threat.

RESPONSIBILITIES

Local Insider Threat Working Group meetings with the core group will be regularly scheduled to:

- Ensure each member is aware of their specific roles and responsibilities as a member of the group;
- Provide status of activities to detect insider threats;
- Discuss factors affecting the risks of insider threats;
- Identify specific insider threats and actions taken in response;
- The Working Group will coordinate insider threat analysis, response and mitigation actions with the DOE Fermi Site Office, Fermilab Security, Fermilab Chief Information Officer, local Counterintelligence Office, Legal Counsel, Export Control, Human Resources, Medical Department, the DOE Inspector General, as well as FBI Chicago and other cognizant organizations as appropriate;
- Agendas for meetings of the Working Group will be retained to document participation and active engagement.

Should the Local Insider Threat Working Group identify an insider threat, the Group (or a subset of the entire group as necessary) will meet and determine a course of action all of which will be thoroughly documented;

The COO as Chair of the Local Insider Threat Working Group will provide briefs to Fermilab management and DOE Fermi Site Office management as appropriate.

DETAILED PROCEDURE(S)

Pursuant to the above, the Fermilab Local Insider Threat Working Group will implement the following procedural measures:

- The Chief Operating Officer will ensure that the Local Insider Threat Working Group is established and maintained pursuant to DOE Order 470.5; including:
 - Identifying the resources to support the Insider Threat Program, and providing this information to the Insider Threat Working Group;
 - Providing access to data as required for the Insider Threat Program to successfully execute its mission; and
 - Ensuring legal, civil and privacy rights and civil liberties are preserved and protected.
- Documentation pursuant to the Insider Threat Program will be reviewed for controlled unclassified information and handled accordingly. The Insider Threat Working Group will ensure that insider threat data and records are developed, maintained, shared and protected

as required;

Responsibility for reviewing, updating and communicating changes to this procedure rests with the Security Management System Owner.

The Local Insider Threat Working Group core participation consists of:

- Fermilab Chief Operating Officer
- DOE Fermi Site Office Manager
- Fermilab Chief Information Officer
- Fermilab Cyber Security Lead
- Fermilab Emergency Planner
- Fermilab Chief of Security
- Fermilab Workforce Development and Resource Section Manager
- Local Counter Intelligence Office representative
- Fermilab General Counsel

The Core group will be augmented by representatives from the FBI, experts in various legal disciplines, human resources, local Inspector General office, local law enforcement and others as needed.

Approved: