Pension Benefit
Guaranty Corporation

Directive

Subject: PBGC Insider Threat Program

Directive Number: IM 05-11 **Originator: OIT**

Alice C. Maroni
Chief Management Officer

ALICE MARONI
Digitally signed by ALICE MARONI
Date: 2020.02.25 17:16:39 -05'00'

1. **PURPOSE:** This Directive establishes an integrated, multi-stakeholder Program and framework to prevent, detect, deter, and remediate Insider Threats, in accordance with applicable standards set forth by the National Insider Threat Task Force (NITTF), National Institute of Standards and Technology (NIST), and other persuasive authority.

2. **EFFECTIVE DATE:** This Directive is effective as of the date shown above.

3. **SCOPE:** This Directive applies to all PBGC employees and contractors.

4. **AUTHORITIES:**

   a. 5 U.S.C. § 301 (Departmental Regulations)
   b. 5 U.S.C. § 552a (The Privacy Act of 1974)
   c. 29 U.S.C. § 1302(b)(3) (Pension Benefit Guaranty Corporation)
   d. 44 U.S.C. § 3101 (Information Security, Federal Agency Responsibilities)
   e. Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011))
   f. Executive Orders 13488 and 13467, as amended by 13764 (To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters)
   g. Executive Order 13356 (Controlled Unclassified Information (Nov. 4, 2010))
   h. Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012)
   i. Office of Management and Budget (OMB) Circular A-130 (Managing Information as a Strategic Resource)

j. NIST Special Publication (SP) 800-53
k. NITTF, Insider Threat Hub Operations Course Manual
l. PBGC Directive FM 15-03 (Suspension and Debarment Program)
m. PBGC Directive IM 05-02 (PBGC Information Security Policy)
n. PBGC Directive IM 05-04 (Use of Information Technology Resources)
o. PBGC Directive IM 05-09 (PBGC Privacy Program)
p. PBGC Directive IM 10-03 (Protecting Sensitive Information)
q. PBGC Directive PM 05-17 (Personnel Security and Suitability Program)
r. PBGC Directive PM 30-01 (Disciplinary and Adverse Action Procedures)
s. PBGC Breach Response Plan
t. PBGC Security Incident Management Plan

5. **BACKGROUND:** Executive Order 13587 requires national security agencies and other organizations that handle classified information to implement an insider threat detection and prevention program. As noted by NIST, the Minimum Standards for Executive Branch Insider Threat Programs can also improve the security of Controlled Unclassified Information.[1] As such, PBGC has elected to establish a permanent, multi-stakeholder Insider Threat Program modelled after the Minimum Standards and NITTF guidance to detect, prevent, and remediate internal threats to PBGC Assets.

6. **DEFINITIONS:**

a. **Anomalous Activity.** Physical and/or Logical Activity that is inconsistent with, or deviates from, what is usual, normal, or expected.

b. **Asset**. Any resource – including facilities, information, equipment, and systems – at the disposition of an organization for use in an operational or support role.

c. **Controlled Unclassified Information (CUI).** Information that requires safeguarding and/or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding classified information.

d. **Insider.** Any individual authorized to access PBGC Assets, including facilities, information, equipment, and systems. An Insider may be a Federal employee, contractor, intern, vendor, or visitor.

e. **Insider Threat.** When an Insider uses PBGC Assets for an improper purpose including, but not limited to, personal gain, which negatively affects the confidentiality, integrity, or availability of PBGC Assets. This threat may be posed by one or more Insiders.

[1] Nat'l Inst. for Standards & Tech., Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, app. G, Page G-7, Control PM-12 ("The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of [CUI] in non-national security systems.").

f. **Logical Activity.** Actions taken within, including access to, PBGC's network and Information Technology (IT) based services or systems.

g. **Personally Identifiable Information (PII).** Information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual. PII includes information relating not only to individual participants and beneficiaries in covered pension plans, but also to PBGC Personnel.

h. **Personnel.** All persons employed by, or contracted to PBGC, including Federal employees, contractors, or any other category of person authorized to act for or on behalf of PBGC.

i. **Physical Activity.** Actions taken with respect to, including access to, PBGC's physical Assets, as well as activity within PBGC-controlled facilities via PBGC-issued PIV cards and temporary access card badges.

j. **Sabotage.** An intentional act or acts, which deliberately and willfully destroys, damages, or obstructs PBGC activities, processes, or Assets for any reason.

k. **Subversion.** Any act inciting PBGC Personnel to violate laws, disobey, or attempt to circumvent, policies, directives, and regulations, or disrupt official activities with the willful intent to interfere with, or impair PBGC's mission.

l. **Suspicious Activity.** One or more Reportable Indicators as described in section 10, below, which identify key traits indicative of an increased risk of an Insider Threat.

7. **POLICY:**

PBGC's policy is to:

a. Develop and maintain an integrated Insider Threat Program with enterprise-wide access to information to identify risks to PBGC Assets and/or operational resources;

b. Establish reporting mechanism(s) and procedures for identifying and elevating concerns regarding Suspicious and/or Anomalous Activities that may be indicative of an actual or potential Insider Threat;

c. Leverage and centralize technological and non-technological capabilities to monitor, assess, analyze, and act upon all Suspicious and/or Anomalous Activity indicative of an actual or potential Insider Threat to PBGC Assets and/or operational resources;

d. Establish and articulate applicable Standard Operating Procedures (SOPs), which are incorporated by reference within this Directive following review by the Insider Threat Working Group and the Insider Threat Executive Committee, so as to maintain efficiency, flexibility, and responsiveness;

e. Refer suspected criminal matters to the Office of the Inspector General (OIG) for investigation, and support any subsequent law enforcement action stemming from an Insider Threat, as needed;

f. Provide Insider Threat awareness training to all Personnel following entrance-on-duty and annually thereafter, and specialized training to Insider Threat Program members;

g. Adhere to the following guiding principles:

(1) Privacy protection – Personnel privacy will be protected with stringent privacy controls, as required by law and PBGC policy;

(2) Personnel wellbeing – To the extent possible, employee support programs (for example, PBGC's Employee Assistance Program) will be leveraged, as needed;

(3) Risk-based monitoring – Anomalous Activities, both Physical and Logical, will be monitored commensurate with the level of risk posed to PBGC Assets, as evaluated by evidence-based risk metrics;

(4) Balanced approach – Mission accomplishment and workforce agility will be balanced effectively with responsible threat prevention, detection, mitigation, and deterrence; and

(5) PBGC reputation – Public confidence in PBGC will be maintained by responsible data stewardship, including by effectively mitigating risk and protecting PBGC Assets to ensure mission accomplishment.

The roles, responsibilities, and associated activities of the PBGC Insider Threat Program are governed by applicable whistleblower protections, civil rights laws, and privacy policies.

8. **RESPONSIBILITIES:**

a. **PBGC Director.**
(1) Retains overall responsibility for protecting PBGC Assets and accomplishment of PBGC's mission; and
(2) Appoints the Senior Agency Official (SAO) for Insider Threat.

b. **Senior Agency Official (SAO) for Insider Threat.**

(1) Provides guidance to the PBGC Director and senior leadership on Insider Threat Program activities, including regular reports to the Insider Threat Executive Committee;

(2) Oversees the Insider Threat Program, ensuring all activities, including incident inquiry and response, are established and operated in accordance with applicable laws, whistleblower protections, civil rights laws, and privacy policies;

(3) Authorizes procedures, processes, and guidelines – as developed by the Insider Threat Working Group, proposed by the Program Officer(s), and reviewed by the Insider Threat Executive Committee – to centralize, integrate, analyze, and respond to Insider Threat information;

(4) Ensures that the Insider Threat Working Group has necessary access to information and resources across boundaries for the effective functioning of the Insider Threat Program;

(5) Designates, and works closely with, the Insider Threat Program Officer(s), to ensure the Insider Threat Program functions efficiently, effectively, and as intended;

(6) Oversees the Insider Threat Working Group, which is chaired by the Program Officer(s); and

(7) Ensures PBGC Personnel receive appropriate training regarding Insider Threats, Program activities, their responsibility to safeguard PBGC Assets, and reporting processes.

c. **Program Officer(s).**

(1) Provides functional oversight of the Insider Threat Program activities and works closely with the SAO to fulfill Insider Threat Program functions;

(2) Chairs the Insider Threat Working Group and facilitates all activities thereof;

(3) Ensures Insider Threat Program activities are conducted in full compliance with applicable laws, whistleblower protections, civil rights laws, and privacy policies, including adherence to the guiding principles, above;

(4) Identifies the specific requirements for, and works with, the SAO for Insider Threat to ensure the Insider Threat Program obtains and maintains access to information, Agency-wide, that is necessary to prevent, detect, and remediate potential or actual Insider Threats;

(5) Coordinates approval of Insider Threat Program activities with the SAO for Insider Threat through regular communication and meetings as needed to ensure the success of the Insider Threat Program;

(6) Activates the Insider Threat Response Team following an identified Insider Threat, informing the SAO for Insider Threat of incident inquiries and/or remedial activities;

(7) Reports suspected criminal activity to the OIG, assists in any subsequent law enforcement investigation, and acts as point-of-contact for such activities;
(8) Maintains appropriate clearances and relationships to coordinate with law enforcement as needed;
(9) Identifies Insider Threat Response Team members who require clearance to conduct inquiries and/or assist law enforcement activities resulting from a potential or actual Insider Threat;
(10) Identifies Insider Threat training needs, including general awareness for PBGC Personnel and specific training for Insider Threat Program members; and
(11) Ensures PBGC Personnel complete Insider Threat Awareness Training following entrance-on-duty and complete refresher training annually thereafter.

d. **Insider Threat Working Group.**
(1) An agile, cross-discipline, standing group of federal employees focused on preventing, detecting, assessing, and mitigating Insider Threat activity through the centralized and integrated monitoring and analysis of threat information, leveraging technical and non-technical data. The primary function of the Insider Threat Working Group is to be proactive, holistic, and people-centric under the guiding principles, above;
(2) Chaired by the Insider Threat Program Officer(s) and overseen by the SAO for Insider Threat, who has final decision authority for activities undertaken by the Insider Threat Working Group;
(3) Consists of stakeholders with permanent representation from HRD, OGC, OIT, and WSD in specific functions as detailed below who, along with the Program Officer(s), meet regularly. All members of the Insider Threat Working Group must maintain, at appropriate levels, the confidentiality of certain Program activities and the specificity of certain threat indicators;
(4) Identifies Insider Threat issues affecting policies and/or procedures on an Agency-wide basis and coordinates the development or revision of SOPs or other policies, as needed;
(5) Develops objectives and priorities for integrating and analyzing applicable information to identify Insider Threats, including establishing evidence-based risk metrics and procedures to respond to Reportable Events and risk indicators;
(6) Identifies patterns of problems contributing to Insider Threat behavior, such as flawed business processes, ineffective communications, lack of support, policy gaps, and insufficient training, which may lead to recommendations (through the Program Officer(s) and SAO for Insider Threat) to change PBGC SOPs and/or processes to address those patterns;
(7) Supports the activities of the Insider Threat Response Team to gather, integrate, and centrally analyze threat related information,

including the Insider Threat Response Team's inquiries into Suspicious or Anomalous Activities;

(8) Integrates recommendations from the PBGC Director, Insider Threat Executive Committee, and/or OIG related to the improvement of the Insider Threat Program, as well as lessons-learned reporting from the Insider Threat Response Team;

(9) Maintains and promotes an intranet site accessible to all PBGC Personnel to provide Insider Threat reference material, including general categories of Insider Threat risk indicators (i.e., Anomalous and/or Suspicious Activity), and applicable reporting requirements and procedures; and

(10) Provides annual and ad-hoc training to PBGC Personnel regarding Insider Threats and the Insider Threat Program.

e. **Insider Threat Executive Committee.**

(1) A senior-level group that supports the planning and oversight of the Insider Threat Program to ensure communication and coordination among key stakeholders;

(2) Convenes quarterly (or leverages a standing meeting of senior leadership) to review progress on Insider Threat Program initiatives and when required to consider decisions presented by the Insider Threat Working Group (through the SAO for Insider Threat), or as otherwise necessary to accomplish the purposes of the Insider Threat Program;

(3) Consists of senior stakeholders, including but not limited to:

a. Chief of Benefits Administration,
b. Chief Information Officer,
c. Chief Financial Officer,
d. Chief Management Officer,
e. Chief of Negotiations and Restructuring,
f. Chief Policy Officer, and
g. General Counsel, or
h. Any designee of the above;

(4) Provides a leadership forum and governance structure for discussing pertinent issues across organizational boundaries; and

(5) Secures Agency-wide support for Insider Threat Program activities and acts to remove obstacles and resolve issues that may impede the success of the Insider Threat Program.

f. **Insider Threat Response Team.**

(1) A sub-set of the Insider Threat Working Group, which is activated by the Program Officer(s) and is reactive in nature;

(2) Consists of certain Insider Threat Working Group members who are identified by the Program Officer(s) as needing sufficient clearance to support and conduct incident inquiries for the Insider Threat Program;

(3) These standing members of the Insider Threat Response Team must maintain appropriate clearances to assist with law enforcement activities resulting from an Insider Threat;
(4) May also include ad hoc members, as determined by the Program Officer(s), who are necessary for the effective response to a given threat;
(5) Gathers, integrates, and centrally analyzes threat related information, leveraging technological and non-technological controls, including information known to HRD, OGC, OIT, and WSD, to detect, mitigate, and respond to Insider Threats, including conducting inquiries into Suspicious or Anomalous Activities, based upon defined risk metrics; and
(6) Documents lessons-learned to be discussed with the Insider Threat Executive Committee and implemented Agency-wide – through the activities of the Insider Threat Working Group – across applicable programs, policies, and/or SOPs resulting from an Insider Threat.

g. **Human Resources Department (HRD).**
(1) Ensures the success of the Insider Threat Program and its mission through stakeholder participation on the Insider Threat Working Group, lending expertise on issues pertaining to personnel and any other HRD-related Assets, systems, policies, SOPs, and operational capacity;
(2) Proactively provides any information within its operational boundaries necessary for the Insider Threat Program to achieve its purpose effectively;
(3) Provides information, advice and guidance to supervisors, managers and employees concerning misconduct, disciplinary and adverse actions;
(4) Assists supervisors and managers in the preparation of counseling memoranda, disciplinary and adverse action proposals, and decision letters; and
(5) Processes actions of a disciplinary nature in accordance with applicable guidelines.

h. **Office of General Counsel (OGC).**
(1) Ensures the success of the Insider Threat Program and its mission through stakeholder participation on the Insider Threat Working Group and Response Team, lending expertise on issues pertaining to privacy, civil liberties, other applicable laws, regulations, and policies; and
(2) Proactively provides any information within its operational boundaries necessary for the Insider Threat Program to achieve its purpose effectively.

i. **Office of Information Technology (OIT).**
(1) Ensures the success of the Insider Threat Program and its mission through stakeholder participation on the Insider Threat Working

Group and Response Team, lending expertise on issues pertaining to information security, cybersecurity, and any other IT-related Assets, systems, policies, SOPs, and operational capacity;

(2) Proactively provides any information within its operational boundaries necessary for the Insider Threat Program to achieve its purpose effectively;

(3) Leverages IT capabilities to collect, correlate, report, and alert on data pertinent to detecting Insider Threats, based on established risk indicators, across all PBGC system boundaries for the effective functioning of the Insider Threat Program, including information pertaining to Logical and Physical Activity and personnel security adjudication; and

(4) Identifies gaps in IT capabilities needed to detect and prevent Insider Threats and deploys new, and/or refines existing, IT capabilities to address those gaps.

j. **Workspace Solutions Department (WSD).**

(1) Ensures the success of the Insider Threat Program and its mission through stakeholder participation on the Insider Threat Working Group, lending expertise on issues pertaining to physical security and any other WSD-related Assets, systems, policies, SOPs, and operational capacity; and

(2) Proactively provides any information within its operational boundaries necessary for the Insider Threat Program to achieve its purpose effectively.

k. **Department Directors/Managers/CORs.** All Department Directors, Managers, and CORs are responsible for supporting the PBGC Insider Threat Program within their area of responsibility by:

(1) Ensuring subordinate employees and contractors are aware of, and held accountable for, applicable policies;

(2) Ensuring subordinate employees and contractors complete mandatory training;

(3) Collaborating with the SAO for Insider Threat and Program Officer(s) to implement courses of action recommended by the SAO in support of the Insider Threat Program, including creating new, or amending current, policies or SOPs as deemed necessary to detect, prevent, mitigate, and remediate Insider Threats; and

(4) Support the activities of the Insider Threat Response Team, including by providing necessary information and/or ad hoc representation.

l. **PBGC Personnel.** Supporting PBGC's mission, in part through the active protection of PBGC Assets, is the responsibility of all PBGC Personnel. Additionally, PBGC Personnel are responsible for:

(1) Understanding and complying with the scope of their authority to access and use PBGC Assets, in accordance with their role-based functions;

(2) Complying with PBGC policies and procedures, including as related to the Insider Threat Program;
(3) Completing Insider Threat awareness training following entrance-on-duty and annually thereafter;
(4) Assisting in reporting suspected Anomalous and Suspicious Activities that may be indicative of an Insider Threat, as well as Subversion and/or Sabotage; and
(5) Serving as ad hoc members of the Insider Threat Response Team as deemed necessary by the Program Officer(s).

9. **PROCEDURES:** All applicable policies and SOPs reviewed by the Insider Threat Executive Committee and duly authorized by the SAO for Insider Threat or otherwise developed in furtherance of the Insider Threat Program, are hereby incorporated by reference into this Directive.

a. **Training.** Training shall be provided following entrance-on-duty and annually thereafter, and shall address, at a minimum, the following:
(1) What constitutes an Insider Threat;
(2) The importance of detecting Insider Threats;
(3) The importance of reporting suspected Insider Threat activity (Anomalous and/or Suspicious Activity, Sabotage, and Subversion);
(4) Indicators of Insider Threat behavior (including Reportable Indicators, below), and procedures to report such behavior; and
(5) The existence and purpose of the PBGC Insider Threat Program.

b. **Reporting.** All PBGC Personnel may Report Anomalous or Suspicious Activities, through the intranet site maintained by the Insider Threat Working Group.

10. **Reportable Indicators:** The following factors may be considered, in conjunction with other evidence-based metrics, in determining the existence of an Insider Threat. The presence or absence of any of the following do not, alone, prove the existence of an Insider Threat, but taken individually or together, may suggest an increased risk:

a. Undue interest or attempts to exceed or expand Physical and/or Logical access to PBGC Assets.
b. Flagrant or repeated disregard for security practices.
c. Unusual or atypical behavior (Suspicious and/or Anomalous Activity).
d. Demonstration of workplace discontent or anger issues.
e. Public/candid admissions of personal problems.
f. Stressful financial or other personal matters.
g. Removing PII or sensitive information from PBGC facilities without proper authorization.
h. Printing large volumes of PII or other sensitive information.

11. **Non-Compliance and Discipline:** Individuals who have committed Insider Threat activity:

a. May be subject to criminal prosecution;
b. May be denied Physical and/or Logical access to PBGC facilities, equipment, systems, and information, including sensitive information (i.e., CUI);
c. Shall be subject to applicable PBGC disciplinary action up to and including termination (personnel), and/or suspension and debarment (contractors), as established by:

(1) PBGC Directive FM 15-03, (Suspension and Debarment Program);
(2) PBGC Directive PM 30-01, (Disciplinary and Adverse Action Procedures); and/or
(3) Other applicable PBGC Directives.