Pension Benefit Guaranty Corporation

Directive

Subject: Guidelines for the Usage of Foreign Nationals in PBGC Contracts

Directive Number: GA-10-12

Effective Date: 06/15/2015 **Originator: PD**

Alice C. Maroni
Acting Director

1. **PURPOSE**: This Directive establishes the Pension Benefit Guaranty Corporation's (PBGC) responsibilities governing the usage of Foreign Nationals, residing outside the United States (U.S.), in PBGC contracts. More specifically, this directive prescribes the policies for contracting with companies employing Foreign Nationals when the performance of services is designated to occur in foreign territories outside the U.S.

2. **EFFECTIVE DATE**: This directive is effective as of the date noted above.

3. **SCOPE:**

   a. This directive applies to all procurement actions which involve contracting with companies who may employ Foreign Nationals residing and performing PBGC services outside the U.S. and its territories.

   b. This directive does not apply to:

      (1) The federal employment of Foreign Nationals by the PBGC. (See PBGC PM-05-01, *PBGC Entrance on Duty and Separation Procedures for Federal Employees and Contractors*)

      (2) Contracts with companies who employ Foreign Nationals who reside and perform PBGC services within the U.S. and its territories. (See PBGC PM-05-6, *Personnel Security and Suitability Program*)

4. **AUTHORITIES:**

   a. Privacy Act of 1974, 5 U.S.C. §552.
   b. Federal Information Security Management Act, 44 U.S.C. §3541.
   c. Federal Acquisition Regulation, 41 C.F.R. §3.104
   d. Federal Information Processing Standard Publication 140-2.
   e. National Institute of Standards (NIST) Special Publication 800-53,

Recommended Security Controls for Federal Information Systems and Organizations.

f. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006).

g. OMB Memorandum M-15-01, *Guidance on Improving Federal Information Security and Privacy Management Practices* (Oct. 3, 2014).

h. PBGC Directive FM 15-01, *Requisition, Acquisition and Payment for Goods and Services.*

i. PBGC Directive IM 05-02, *PBGC Information Security Policy*.

j. PBGC Directive IM 05-07, *PBGC's Information Technology Solutions Life Cycle Methodology (ITSLCM).*

k. PBGC Directive IM 10-03, *Protecting Sensitive Information.*

l. PBGC Directive PM 05-01, *Entrance on Duty and Separation Clearance Procedures for PBGC Employees and* Contractors.

m. PBGC Directive PM 05-06, *Personnel Security and Suitability Program.*

n. PBGC Directive PM 25-05, *Selection, Appointment, Training and Management of Contracting Officer's Representatives (CORs).*

o. The Office of Information Technology Security Authorization Guide.

5. **BACKGROUND**: As the Federal government contracts with companies with a global presence and whose employees reside outside the United States (U.S.), we are faced with ensuring those individuals are adequately vetted prior to accessing government facilities, data, or information systems. Before PBGC decides to contract with firms who will use Foreign Nationals residing in foreign territories in performance of the contract, it must ensure that staffing and contracting decisions fit with its strategic planning process and comply with applicable law. The Standard Operating Procedures (SOP) attached to this Directive outlines a uniform systematic process that allows program managers to appropriately identify, evaluate and mitigate risk with respect to contracts which may employ Foreign Nationals residing and performing PBGC services outside the U.S. and its territories.

6. **DEFINITIONS**

a. **Adjudication**. Objective analysis of all available, relevant information, obtained during a background investigation, both favorable and unfavorable.

b. **Advance Procurement Plans**. Plans submitted by PBGC departments to the Procurement Department detailing new procurement actions valued over the Simplified Acquisition Threshold. *See* FAR 2.101.

c. **Authorizing Official (AO)**. Department Director or Senior Level (SL) official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, assets and individuals. AOs typically have budgetary oversight for an information system or are responsible for the mission and/or business operations supported by the system. Please see Directive IM 05-02, *PBGC Information Security Program* for a full set of responsibilities and activities.

d. **Background Investigation**. An examination of personal traits and qualifications, including education, reputation, suitability, loyalty, and other pertinent factors, conducted by personal contact, written inquiry, letter, or electronic linkage with the sources of information.

e. **Chief Information Security Officer (CISO) (formerly Senior Agency Information Security Officer (SAISO)).** Senior Level (SL) official with the authority formally responsible for ensuring that the appropriate operational security posture is maintained for an information system and works in close collaboration with the Information System Owner (ISO) and Information System Security Officer (ISSO).

f. **Contracting Officer's Representative (COR).** An employee designated in writing by a Contracting Officer to represent the Contracting Officer in the administration of a specific contract.

g. **Executive Sponsor**. Department Director or Senior Agency Official who has a vested interest in seeing a project to completion. Ideally, the executive sponsor should be the highest-ranking manager possible, relative to the size of the project. Often, the same senior official will serve as both the AO and Executive Sponsor.

h. **Foreign National.** An individual who is a citizen of any country other than the U.S.

i. **Information Owner (IO).** An agency employee with statutory, management, or operational authority for specified information. If not the same person, the IO provides input to the Information System Owner regarding the security requirements and security controls for the system where the information is processed, stored, or transmitted.

j. **Information System Owner (ISO).** An agency employee who may be responsible for or associated with the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. Please see Directive IM 05-02, *PBGC Information Security Program* for a full set of responsibilities and activities, which include ensuring compliance with information security requirements and providing documented acceptance of risk for the information system.

k. **Information System Security Officer (ISSO).** An individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and works in close collaboration with the ISO. Please see Directive IM 05-02, *PBGC Information Security Program*, for a full set of responsibilities and activities.

l. **Mitigating Control**. A compensating control or countermeasure employed by an organization in order to reduce risk. *See* NIST Special Publication 800-53.

m. **Program/Project Manager (PM).** An individual responsible for planning, organizing the necessary resources, and executing a project or program (group of related projects).

n. **Risk Management:** The process of identification, analysis and either acceptance or mitigation of uncertainty in decision-making.

o. **Sensitive PBGC information**. Information that has a degree of confidentiality such that loss, misuse, unauthorized access, or modification of it could compromise the element of confidentiality and thereby adversely affect PBGC's business operations, plans or participants of pension plans insured or trusteed by PBGC, or the privacy of individuals covered under the Privacy Act. *See also* Appendix B of the Standard Operating Procedure (SOP) "The Usage of Foreign Nationals in PBGC Contracts".

p. **Standard Operating Procedure (SOP).** Established or prescribed methods to be followed routinely in designated situation.

q. **Suitability**. Identifiable character traits and past conduct which are significant to determine whether an individual is likely or not likely to be able to carry out the duties of a Federal job or contractor position with appropriate efficiency, effectiveness, and integrity. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities.

7. **POLICY**:

a. PBGC shall ensure that Foreign Nationals performing services for the PBGC are favorably adjudicated before permitting access to PBGC's sensitive information, materials or technologies.

b. Foreign Nationals shall not be granted/eligible for access to any greater level of sensitive information, materials or technologies than PBGC has determined releasable based on favorable adjudication, signed non-disclosure agreement, and need-to-know in the performance in their duties.

c. Where there are compelling reasons in furtherance of PBGC's mission, a Foreign National may be permitted to have temporary access to PBGC sensitive information, materials or technologies, pending completion of a favorable adjudication.

d. All acquisition planning includes a Risk Management component. Program offices shall ensure that utilization of established PBGC policies and procedures and project management best practices for risk identification, assessment and mitigation are practiced during the acquisition planning process and throughout the life cycle of a contract. The risk management component shall be applied and documented for all

PBGC procurement actions.

e. The contract clauses associated with this policy shall apply to all new contract awards, and shall be negotiated into existing contracts within 12 months of the date of this directive, or upon exercise of the next option, whichever provides the greatest flexibility to meet mission requirements.

8. **RESPONSIBILITIES**:

a. **Authorizing Official (AO)/Executive Sponsor shall:**
Approve any risk assessment memoranda or risk acceptance documents that support decisions to contract with companies who may employ Foreign Nationals residing and performing services outside the U.S.

b. **Chief Information Security Officer (CISO) (formerly SAISO) shall:**
(1) Establish, maintain and monitor PBGC information security policies, procedures, control techniques, training and auditing requirements as elements of the PBGC Information Security Program.
(2) Oversee and enforce compliance with and execution of information security policy.
(3) Ensure the Information System Security Officer (ISSO) is involved in all the new projects concerning the development or acquisition of systems, equipment or services and participates in risk analysis and security requirements development.

c. **Contracting Officer's Representative (COR) shall:**
(1) Determine and assign an appropriate suitability risk level for any Contract employee with access to government facilities, sensitive data, or information systems who are working under PBGC Contracts assigned to the COR.
(2) Ensure contractor compliance to any PBGC entrance-on duty, background investigation or separation clearance procedure.
(3) Provide continuous oversight in accordance with PM 25-05, *Selection, Appointment, Training and Management of Contracting Officer's Representatives (CORs)*. Annual reviews will include inspection of all documentation pertinent to Foreign Nationals residing and performing PBGC services outside the U.S.

d. **Information System Owners (ISO) and/or Information Owner (IO) shall:**
Determine if contractors or third party services require access to PBGC information in the performance of the contract, the sensitivity of that information, and recommend to the Authorizing Official whether the operation of the contract could be performed outside the U.S. by Foreign Nationals

residing outside the U.S.

e. **Information System Security Officer (ISSO) shall:**

(1) Support the Program or Project Manager or ISO during the requirements analysis phase by evaluating requirements and providing advice on appropriate security measures.

(2) Review Statement of Work (SOW) (or similar requirements document) for proposed acquisitions which may include Foreign Nationals residing outside the U.S. to ensure the resulting contracts and service providers sufficiently define information security responsibilities and provide a means to respond to information security problems.

(3) Participate in the review and completion of Appendix A of the SOP "The Usage of Foreign Nationals in PBGC Contracts", and any associated risk management memorandum or risk acceptance form.

f. **Procurement Department (PD) shall:**

Ensure the inclusion of applicable contract clauses in all contracts where the potential exists for the employment of foreign nationals who reside and perform services for PBGC outside the U.S., and its territories.

g. **Office of General Counsel (OGC) shall:**

Review the completed Sensitive Information Form (Appendix B of the SOP "The Usage of Foreign Nationals in PBGC Contracts"), conduct a legal risk assessment based on the type of information at issue with the potential contract in which the foreign national may perform work, and provide the written assessment to the PM.

h. **Program/Project Manager(PM) shall:**

(1) Review and complete the decision guidelines provided in Appendix A of the SOP "The Usage of Foreign Nationals in PBGC Contracts" to decide whether Foreign Nationals residing and performing PBGC Services in foreign territories may be used to meet program demands.

(2) Review and complete the PBGC Sensitive Information Form provided in Appendix B of the SOP "The Usage of Foreign Nationals in PBGC Contracts", if it has been determined that Foreign Nationals outside the U.S. and performing in foreign territories may be used to meet program demands.

(3) Adhere to PBGC Directives IM-05-07, *PBGC's Information Technology Solutions Life Cycle Methodology (ITSLCM)* (for IT system acquisitions) and IM-05-02, *PBGC Information Security Policy.*

(4) Ensure that the SOW prompts contractors to address whether any or all services will be provided by Foreign Nationals residing and performing

PBGC services outside the U.S.

(5) Draft risk acceptance memorandum for review and approval by the AO/Executive Sponsor.

(6) Document the risk management process, implementation and conduct continuous monitoring to ensure consistency in implementing mitigating controls.

i. **Workplace Solutions Department (WSD), Personnel Security Officer shall:**

(1) Establish minimum background investigation requirements for the vetting of Foreign Nationals residing and performing PBGC services in foreign territories that will be provided access to PBGC data or property.

(2) Review and adjudicate all completed background investigations. Candidates put forth by contractor shall not be permitted to support a PBGC contract if WSD's final adjudication decision is "unfavorable".

9. **PROCEDURES:**

The SOP for this Directive is available on the PBGC Intranet. They must be completed by the PM initiating any procurement action that may employ Foreign Nationals residing and performing PBGC services outside the U.S. and its territories.