Facilities Services Program
(FSP)
Privacy Impact Assessment (PIA) Summary

I. BACKGROUND

Federal agencies are required to ensure the protection of the personally identifiable information (PII) they collect, store, and transmit. The Pension Benefit Guaranty Corporation (PBGC) is responsible for ensuring proper protections of the information contained within its information systems, including PII. To that end, PBGC developed a Privacy Impact Assessment (PIA) to evaluate whether a system that contains PII meets legal privacy requirements.

II. PURPOSE AND SCOPE

- Purpose

PBGC is responsible for ensuring the confidentiality, integrity, and availability of the information contained within the Facilities Services Program (FSP). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on FSP.

The PIA provides a number of benefits to PBGC; enhancing policy decision-making and system design, anticipating the public's possible privacy concerns, and generating confidence that privacy objectives are addressed in the development and implementation of FSP. The PIA Questionnaire provides a framework by which agencies can ensure that they have complied with all relevant privacy policies, regulations, and guidance, both internal and external to PBGC.

- Scope

A Privacy Impact Assessment was conducted on the FSP system. FSP functions as a Major Applications System within the direct management control of the Workplace Solutions Department. FSP is comprised of the following subsystems and devices; Personnel Investigation Manager (PI Manager), Statisticard, Mutare, eDelivery, Wallace Incident Communicator (WIC), and FACIPlan. FSP is located at 1200 K Street NW, Washington, DC and Wilmington, DE, and is accessed by both PBGC and contractors with Federal oversight. FSP is listed as a Major Application on the PBGC's Federal Information Security Management Act (FISMA), and its security needs are consistent with those of PBGC.

III. PIA APPROACH

A questionnaire was developed in accordance with the FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems, Office of Management and Budget (OMB) requirements, Section 208 of the E-Government Act of 2002, The National Institute of Standard and Technology (NIST) recommendations, and the Federal Enterprise Architecture Business Reference Model (BRM). The questionnaire was developed in order to identify any PII.

The questionnaire was given to the Information System Owner (ISO) and Information System Security Officer (ISSO) of FSP for their response. An Information Security Analyst from PBGC's Enterprise Cybersecurity Division (ECD) met with the ISO and ISSO of FSP to discuss the questionnaire. Responses from the ISO and the ISSO of FPS were obtained and used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

The FSP is a group of components which function individually or in conjunction to complete the processing of PBGC's personnel and to enable WSD to carry out its mission. FSP is also used to assist in PBGC's notification process of Continuity of Operations (COOP) Essential Staff, to track the status of background investigations, creation of interim identification cards and credentials, to transfer background investigation information from OPM to PBGC, and update agency floor plans.

V. PIA RESULTS

The primary privacy risk identified is a potential data breach and subsequent loss or unauthorized disclosure of PII. The risk of a data breach is mitigated by security controls implemented and documented for FSP. These controls are in accordance with those recommended by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 for a moderate risk system in accordance with Federal Information Processing Standards (FIPS) 199 evaluation. The PIA evaluation revealed that FSP contains PII due to the business need to conduct background investigation, process Interim Identification Cards, distribute COOP documentation to the COOP Essential Staff and assist WSD with their mission. Only those who support the components that make up FSP are authorized to access these components and any data residing thereon, such as network administrators. Based on the analysis performed here, no discrepancies have been discovered.