Pension Benefit Guaranty Corporation

Privacy Impact Assessment Methodology

PRISM

Version 1.0

July 2007

Prepared by:
PBGC Office of Information Technology (OIT)
Enterprise Information Security (EIS)
1200 K Street NW
Washington, DC 20005

ANNUAL REVIEW RECORD

The Privacy Impact Assessment Methodology and Template procedure should be reviewed at least annually and the date recorded on the table below.

Review Date	Reviewer

Change/Review Record

Document Title: Privacy Impact Assessment and Methodology Template

Date of Initial Release:

Version No.	Date Revised	Description of Revisions	
Completed by:			Date
Approved by:			Date:
Version No.	**Date Revised**	**Description of Revisions**	
Completed by:			Date:
Approved by:			Date:
Version No.	**Date Revised**	**Description of Revisions**	
Completed by:			Date:
Approved by:			Date:
Version No.	**Date Revised**	**Description of Revisions**	
Completed by:			Date:
Approved by:			Date:

TABLE OF CONTENTS

LIST OF APPENDICES

LIST OF FIGURES

LIST OF TABLES

1 PRIVACY IMPACT METHODOLOGY

1.1 Background

One of the main Federal statutes mandating protection of personal information is the *Privacy Act of 1974* (5 U.S.C. 552a as amended). The Privacy Act, together with its surrounding case law, serves as the foundation for privacy requirements. In addition to the *Privacy Act of 1974*, some of the major legislation and executive branch guidance regarding privacy issues and privacy protections include the, *Consolidated Appropriations Act of 2005.enacted on December 2004, E-Government Act of 2002,* and *Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources* and *Circular A-11 (Exhibit 300).* The Privacy Act establishes fair information practices for collecting, maintaining, and using personal information by Federal agencies. *OMB Circular A-130* provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems. Other statutory and regulatory privacy references are noted in the Privacy Impact Assessment (PIA) Questionnaire in Section 3, as well as Appendix C of this document.

1.2 Introduction

Federal agencies are required by law to ensure the protection of the personally identifiable information (PII) they collect, store, and transmit. With a thriving digital economy, agencies are collecting ever-larger amounts of personal information unlike ever before. Instances of past abuse, misuse, and egregious errors in Federal agencies' management of personal information, combined with growing public concern about the U.S. Government's ability to protect their private information, have increased congressional scrutiny and expectations for compliance with Federal privacy laws and regulations. Protection of the Government's vast accumulation of personal information begins with the responsibility of Federal employees at all levels and in all positions.

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 Methodology to assess whether a system that contains PII meets legal privacy requirements. This methodology, based on the evaluation of applicable law and executive branch guidance as well as internal policy, was the foundation for determining question sets and remediation guidance for developing the PIA Questionnaire that is to be applied to the PBGC's information technology (IT) systems. The Privacy Impact Methodology and the PIA Questionnaire, used to implement this methodology, are detailed within this document, which serves as an introduction to the IT PIA and PBGC's privacy mission and principles and offers guidance on how to use the methodology and questionnaire.

1.3 Privacy Mission Statement and Principles

The following are the Privacy Mission Statement and Privacy Principles that define both the PBGC's commitment to privacy and the goals and objectives by which PBGC plans to achieve its stated mission.

Privacy Mission Statement

The privacy mission of PBGC is to protect individuals' information with fair and consistent practices to ensure the protection of personal information.

Privacy Principles

The eight privacy principles outlined in Table 1 are significant in that they provide a basis from which PBGC makes decisions about safeguarding and protecting individuals' personal information:

Table 1: PBGC Privacy Principles

Principle 1:	The Pension Benefit Guaranty Corporation shall protect and safeguard private information about individuals to ensure public trust in the course of pursuing its mission as outlined in *The Privacy Act of 1974 and Invasions of Privacy*.
Principle 2:	PBGC shall collect only the minimum and necessary personal information from individuals in accordance with Federal and regulatory mandates.
Principle 3:	PBGC shall ensure that all personal information collected is relevant, complete, and accurate for the purpose in which it is being collected.
Principle 4:	PBGC shall instruct employees of PBGC's privacy rules of conduct and other applicable privacy laws for employees involved with the design, development, maintenance, or operation of systems containing PII.
Principle 5:	PBGC shall not disclose, nor make available, any personal data except with the consent of the individual concerned or by authority of law.
Principle 6:	PBGC shall ensure that all personal data is properly safeguarded using administrative, technical, and physical controls.
Principle 7:	PBGC shall, when appropriate and required by law, provide access to, and a process for amending, personal information in accordance with the *Privacy Act of 1974*.
Principle 8:	PBGC shall ensure that agencies comply fully with policies and procedures concerning privacy on PBGC Internets and intranets as prescribed in *PBGCMS 9 - Chapter 1500, Privacy Policy on Data Collection Over PBGC Web Sites*, *OMB Memorandum 99-18, Privacy Policies on Federal Websites*, and *OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Websites*.

1.4 Goals and Objectives

The Privacy Impact Assessment Methodology was developed to assess privacy compliance issues and identify potential threats to personal information on a system or web site. PIAs will be used to implement this methodology. PIAs will be conducted on all PBGC sensitive information systems and web sites in order to mitigate agency privacy risks and liabilities as well as to achieve compliance with Federal privacy requirements. The Privacy Impact Assessment Methodology goals include:

1. Providing senior managers with the tools necessary to make fully informed policy and system design or procurement decisions based on an understanding of privacy risk and of the options available for mitigating that risk.

2. Ensuring PBGC departments are accountable for privacy issues.

3. Ensuring that there is a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy laws and regulations, as well as accepted privacy policy.

4. Ensuring the best possible implementation of privacy protections at the start-up of PBGC information systems.

5. Identifying remedial steps necessary to improve privacy protection in existing, operational PBGC information systems.

One objective of the PIA is to assist PBGC departments in identifying personal information and addressing information privacy when planning, developing, implementing, and operating individual agency information management systems and integrated PBGC information systems. Additional objectives of conducting a PIA are:

- Detecting what PII exists on PBGC systems;
- Determining who has access to the PII and for what purposes;
- Ensuring compliance with Federal privacy laws concerning PII;
- Enabling management to make informed decisions regarding implementation of security controls and countermeasures related to privacy vulnerabilities;
- Promoting a repeatable approach to measuring the effectiveness of privacy protections; and
- Preventing the unintended mishandling, abuse, or fraudulent use of PII from creating noncompliance that could impede the overall mission of PBGC

2 PRIVACY IMPACT ASSESSMENT

2.1 Purpose of Conducting a PIA

PBGC is responsible for ensuring the confidentiality, integrity, and availability of the information contained within its information systems. PBGC must at times collect, use, analyze, and store PII from its employees and customers. PBGC remains vigilant in protecting all its information technology resources, but this is especially true of those systems containing PII. Ideally, the PIA should be performed during the development phase of a system life cycle. A PIA should also be conducted at any time when the system is significantly modified, or the sensitivity of the data contained within the system is changed.

A PIA is used to evaluate privacy vulnerabilities and risks, and their implications on information systems. The process described in this document is designed to provide ISSO and Information System Owners with guidance in assessing privacy throughout the early stages of system development, as well as assessing privacy risks of existing, operational systems. PIAs provide a number of benefits to departments that include 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 single-department or integrated information systems. The IT 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.

2.2 Scope

A Privacy Impact Assessment will be conducted on each system and application cited on the PBGC Sensitive System List and reported on the PBGC's Exhibit 53 or via capital asset plans and business cases (Exhibit 300s). Additionally, a PIA will be conducted on all PBGC websites.

2.3 Roles and Responsibilities

Roles and responsibilities for PIA activities within PBGC are provided in Table 2.

Table 2: PIA Roles and Responsibilities

Information Systems Owners	Responsible for ensuring that appropriate privacy safeguards are provided for the information contained within their systems. Information System Owners are responsible for performing the PIAs. Once any privacy vulnerabilities or areas of noncompliance have been identified, agencies must update the system Plan of Action and Milestones (POA&M) to incorporate the actions necessary to resolve privacy issues.
Chief Information Officer (CIO)	Responsible for providing agencies with the Privacy Impact Methodology and Assessment Questionnaire. The CIO will coordinate PIA activities with the agencies and provide guidance to ensure the methodology is implemented consistently. Additionally, the CIO will ensure that all identified privacy vulnerabilities and areas of noncompliance have been documented and track resolution through the POA&M process.
Office of the General Counsel (OGC)	Responsible for directing the overall implementation of the Privacy Act and privacy policy for the PBGC. OGC will field questions that departments have about privacy arising from the completion of the PIA and can answer questions about the implications of the personal information contained within their system. Copies of completed PIAs will also be forwarded to the OGC for their review.

2.4 Identifying Personal Information

One goal of Federal privacy laws and regulations is ensuring that PII is protected from unauthorized access and disclosure. For purposes of this template, PII is defined as any information that can be used to identify a specific individual. These data include, but are not limited to, social security numbers, drivers' license numbers, health records, legal records, financial records, and biometric information.

One of the first major steps in conducting a PIA is determining whether PII resides on the system, and if so, what type. The type of personal information collected, used, and maintained will determine which privacy laws are invoked, if any. The Privacy Act, for example, is potentially invoked when one or more data elements listed in Figure 1, below, are contained in a record. If, however, a record contains personal financial information about an individual, the Right to Financial Privacy, in addition to the Privacy Act, may also be applicable.

Figure 1: Privacy Act Information Categories and Data Elements

Personal Information
Privacy Act Information Categories and Data Elements
Data elements include but are not limited to: ▪ Name ▪ Social Security Number (or other identifying number originated by the Government) ▪ Date of Birth ▪ Photographic Identifier (e.g., picture, photo image, X-ray, and video) ▪ Biometric Identifier (e.g., fingerprint and voiceprint) ▪ Drivers license number ▪ Certificates (birth, death, and marriage) ▪ Mother's Maiden Name ▪ Postal and Mailing Address ▪ Phone Numbers ▪ Education Records ▪ E-mail Address ▪ Employment History (e.g., place of employment, salary, and evaluations) ▪ Medical Records and Notes (e.g., prognosis, prescriptions, treatments related to an individual, and device identifiers) ▪ Financial Account Numbers (e.g., checking account and personal identification number (PIN)

2.5 Major Steps in Conducting a PIA

The completion and remediation of PIAs will follow the process of other PBGC assessments contained in this handbook. The general PIA process includes four major steps:

1. Agencies receive the PIA Questionnaire.
2. PIA is conducted and completed within the specified time frame. In completing the PIA, Agencies may want to consult with system administrator(s) and users in an effort to obtain the most accurate characteristics about the system. Past reports regarding the system's security (such as certification and accreditation reports, Government Information Security Reform Act reports, and risk assessments) may also be helpful in answering some question sets, especially the administrative, technical, and physical controls questions. OGC will provide primary consultation to departments seeking clarification of Privacy Act-related compliance issues and interpretation of Federal case law.

3. Once the PIAs have been conducted, departments should identify the security-related mitigation actions in their agency security POA&M.
4. Departments will then perform the mitigation actions in accordance with the POA&M and update the POA&M as necessary.

2.6 Organization of the PIA Questionnaire

A PIA helps to ensure PII is adequately safeguarded and the information system complies with existing legislation, executive guidance, and PBGC policy. To ensure that a system complies with the appropriate authorities, the PIA first characterizes the system.

Once the system is characterized, the type of information contained on the system is then identified; information-sharing practices are evaluated; and system controls for administrative, technical, and physical safeguards are assessed to ensure the system is adequately protected. Where relevant, any Federal privacy law(s) or PBGC privacy policies driving the business requirement is referenced in that question set.

Additionally, questions that carry consequence for noncompliance provide high-level remediation guidance for implementing privacy corrective actions. Most questions are answered "yes" or "no." However, clarification or system details may be required. When this is necessary, the question box notes the need for more information and asks the PIA user to elaborate in the comments section.

2.7 Submitting the PIA

In addition to completing the questionnaire in Section 3, an executive summary outlining the high-level findings of the PIA will accompany the completed PIA. Please refer to Section 4 for a sample outline of this executive summary. The executive summary should be submitted as a cover memorandum with the completed PIA attached. The completed PIA and executive summary will be reviewed by both the CIO and OGC.

Upon completion of the PIA, the document is considered "sensitive but unclassified". In the footer of the document, edit the text from "FOR OFFICIAL USE ONLY UPON COMPLETION" to read "FOR OFFICIAL USE ONLY".

3 PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

The PBGC Privacy Impact Assessment Questionnaire is presented in Figure 2.

Figure 2: PBGC Privacy Impact Assessment Questionnaire

NOTE: Based on current privacy regulation and guidance, the PIA should be performed on the production environment. For those systems that have test and development environments, those environments may or may not warrant their own Privacy Impact Assessment (PIA). The test and development environments generally do not necessitate a separate PIA; however, the assessor may need to consult information technology (IT) system policy guidance and/or his or her security officer and/or the Chief Information Officer (CIO) to confirm such decisions. For those systems that have performed risk assessments and defined system boundaries and scope, the system characterization will likely be the same for both that risk assessment and this PIA. PIAs performed at the initiation of the system development life cycle will require conducting another PIA at intervals stipulated by this handbook and when significant changes occur to the system.

The PIA attempts to determine what kind of personal information is contained within a system, what is done with that information, and how that information is protected. There are many requirements for systems containing personal information, based on an extensive list of privacy laws, regulations, and guidance. The remediation guidance provided gives users a starting point for meeting certain requirements. However, users should be informed that privacy case law decisions have updated certain provisions of the Privacy Act statute. The Office of the General Counsel (OGC) can answer questions related to the technicalities of privacy law. The CIO can answer questions related to the administrative, technical, and physical controls of the system, and inquiries seeking clarification of Questionnaire questions

System Name:	_PRISM_____
System Environment (production, test, development, or other. If other, please explain):	Production_____
System Location (entity/contractor name of site, building, room, city, and state):	PBGC, Computer Operations Center (room L719) located at 1200 K Street NW, Washington, D.C.
Activity/Purpose of System:	PRISM is used to process and reconcile customer information. _____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
System Characterization					
1	**Does** PBGC **own the system?** Note: If no, identify the Information System Owners in the Comments column.	☒	☐	☐	Owner: _____
2	**Does** PBGC **operate the system?** Note: If no, identify the system operator in the Comments column.	☐	☒	☐	Operator: Contractor_____
3	**Identify in the Comments column the life-cycle phase of this system.**				☐ Initiation ☐ Develop/Acquisition ☐ Implementation ☒ Operations/Maintenance ☐ Disposal
4	**Is the system a stand-alone system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?**	☐	☒	☐	
5	**Is the system network-connected (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire)?**	☒	☐	☐	
6	**Is the system a General Support System (GSS), Major Application or sensitive system (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire or on the PBGC Sensitive System List)?** Note: If yes, identify whether the system is a GSS, MA or sensitive system in the Comments column.	☒	☐	☐	Major Application

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	System Characterization				
7	**Does the system *contain* PII within any database(s), record(s), file(s) or document(s)?** Note: If yes, check all that apply in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category. **Remediation Guidance:** If the system contains no records with any data elements listed in the comments section, the system is not subject to Federal privacy laws or regulations such as the *Privacy Act of 1974*. Questions 8-18 may be marked with an "N/A." If data elements are checked under the personal information category in the comments column, then the *Privacy Act of 1974* is invoked. Agencies must meet all requirements of the Privacy Act listed under *5 U.S.C. 552a. (4)* as amended, listed under "Records Maintained On Individuals." If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the *HIPAA Privacy Rule 67 FR 14775* may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements. If personal information on the system contains Financial Account Information and/or Numbers, then the *Right to Financial Privacy Act of 1978* (*12 U.S.C. 3401 et seq.*) privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.	☒	☐	☐	**Personal Information:** ☒ Name ☒ Date of Birth ☒ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic Identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's License ☐ Biometric Identifiers (e.g., fingerprint and voiceprint) ☒ Mother's Maiden Name ☐ Vehicle Identifiers (e.g., license plates) ☒ Mailing Address ☒ Phone Numbers (e.g., phone, fax, and cell) ☐ Medical Records Numbers ☐ Medical Notes ☒ Financial Account Information and/or Numbers (e.g., checking account number and PINs) ☒ Certificates (e.g., birth, death, and marriage) ☐ Legal Documents or Notes (e.g., divorce decree, criminal records, or other) ☐ Device Identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web URLs ☒ Email Address ☐ Education Records ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
System Characterization					
8	**Has a Privacy Act Systems of Records Notice (PARN) been published in the Federal Register?** **Remediation Guidance:** If no, and the system meets the definition of a System of Records, then the *Privacy Act of 1974* requirements are invoked. Agencies must develop a PARN and publish the notice in the Federal Register with appropriate specifications listed in *5 U.S.C. Section 552a* as amended. The Office of the General Counsel (OGC) can provide guidance on developing and publishing the PARN	☒	☒	☐	PII in the PRISM system is covered by: PBGC-6, Participant and Beneficiary Data, 68 Fed. Reg.. 12,389 (Mar. 14, 2003).
9	**Have major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system been made since publication of the PARN?** **Remediation Guidance:** If yes, then the *Privacy Act of 1974* requires that agencies publish in the Federal Register a notice of any, and all revisions to the existence and character of the system of records with appropriate specifications listed in *5 U.S.C. Section 552a* as amended.	☐	☒	☐	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
System Characterization					
10	**Does the PARN address all required categories of information?** Note: Check all that apply in the Comments column. **Remediation Guidance:** If no, then the notice specifying the existence of the system of records will include all criteria listed in the Comments column.	☒	☐	☐	☒ System Name ☒ Security Classification ☒ System Location ☒ Categories of Individuals Covered by the System ☒ Categories of Records in the System ☒ Authority of Maintenance of the System ☒ Purpose ☒ Routine Uses of Records Maintained in the System ☒ Disclosure to Consumer Reporting Agencies ☒ Policies and Practices for Storing, Retrieving, Accessing, Retaining and Disposing of Records ☒ System Manager(s) and Address ☒ Notification Procedure ☒ Record Access Procedure ☒ Contesting Record Procedure ☒ Record Source Categories ☒ Systems Exempted From Certain Provisions of the Act

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
Information Sharing Practices					
11	**Does the system *collect* PII from individuals?** Note: If yes, identify the PII the system collects directly from individuals in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category. **Remediation Guidance:** Each agency maintaining system of records is required to collect information to the greatest extent practicable directly from the individual when information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the PBGC Disclosure Officer may be required to authorize sharing of medical PII. Additionally, *HIPAA Privacy Rule 67 FR 14775* may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements. If personal information on the system contains Financial Account Information and/or Numbers, then *Right to Financial Privacy Act of 1978* (*12 U.S.C. 3401 et seq*.) privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.	☒	☐	☐	**Personal Information:** ☒ Name ☒ Date of Birth ☒ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic Identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's License ☐ Biometric Identifiers (e.g., fingerprint and voiceprint) ☒ Mother's Maiden Name ☐ Vehicle Identifiers (e.g., license plates) ☒ Mailing Address ☒ Phone Numbers (e.g., phone, fax, and cell) ☐ Medical Records Numbers ☐ Medical Notes ☒ Financial Account Information and/or Numbers (e.g., checking account number and PINs) ☒ Certificates (e.g., birth, death, and marriage) ☐ Legal Documents or Notes (e.g., divorce decree, criminal records, or other) ☐ Device Identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web URLs ☒ E-mail Address ☐ Education Records ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Information Sharing Practices				
12	**Does the system *collect* PII from *other resources* (i.e., databases, websites, etc.)?** Note: If yes, specify the resource(s) and PII in the Comments column. **Remediation Guidance:** If yes, then each agency is required to maintain records on systems that are used for making determinations about an individual with accuracy, relevance, timeliness, and completeness as reasonably necessary to assure fairness to the individual. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the *Privacy Act of 1974*.	☐	☐	☒	☐ _____ ☐ _____ ☐ _____ ☐ _____ ☐ _____
13	**Does the system *populate* data for *other resources* (i.e., do databases, web sites, or other resources rely on this system's data)?** Note: If yes, specify resource(s) and purpose for each instance in the Comments column. **Remediation Guidance:** If yes, then section (e) (6) of the *Privacy Act of 1974* is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, the agency must make reasonable efforts to assure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.	☐	☒	☐	☐ _____ ☐ _____ ☐ _____ ☐ _____ ☐ _____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
Information Sharing Practices					
14	**Does the system *share* PII with internal or external parties of PBGC?** Note: If yes, specify with whom and for what purposes, and identify which data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category. **Remediation Guidance:** If yes, then section (e) (6) of the *Privacy Act of 1974* is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act. In addition, the *HIPAA Privacy Rule, 67 FR 14775* may be invoked. PBGC should review these rules to determine exact applicability and compliance requirements. If personal information on the system contains Financial Account Information and/or Numbers, then *Right to Financial Privacy Act of 1978* (*12 U.S.C. 3401 et seq.*) privacy requirements may be invoked. PBGC should review this law to determine exact applicability and compliance requirements.	☒	☒	☐	With whom and for what purposes: ☒ Users for Processing ☐ __ _____ ☐ _____ ☐ _____ ☐ _____ PII shared: **Personal Information:** ☒ Name ☒ Date of Birth ☒ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic Identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's License ☐ Biometric Identifiers (e.g., fingerprint and voiceprint) ☐ Mother's Maiden Name ☐ Vehicle Identifiers (e.g., license plates) ☒ Mailing Address ☐ Phone Numbers (e.g., phone, fax, and cell) ☐ Medical Records Numbers ☐ Medical Notes ☒ Financial Account Information and/or Numbers (e.g., checking account number and PINs) ☒ Certificates (e.g., birth, death, and marriage) ☒ Legal Documents or Notes (e.g., divorce decree, criminal records, or other) ☐ Device Identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web URLs ☒ E-mail Address ☐ Education Records ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
Information Sharing Practices					
15	**Are records on the system retrievable?** Note: If yes, specify in the Comments column what method is used in retrieving the records (i.e., using a record number, name, social security number, or other data element or record locator methodology). If the category of personal information is not listed, please check "Other" and identify the category. **Remediation Guidance:** If yes, then a system of records in which information is retrieved using one or more of an individual's "identifying information" invokes *Privacy Act of 1974* requirements. All requirements under *5 U.S.C. of Section 552a* as amended must be met by an agency for this system.	☒	☐	☐	**Personal Information:** ☒ Name ☐ Date of Birth ☒ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic Identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's License ☐ Biometric Identifiers (e.g., fingerprint and voiceprint) ☐ Mother's Maiden Name ☐ Vehicle Identifiers (e.g., license plates) ☐ Mailing Address ☐ Phone Numbers (e.g., phone, fax, and cell) ☐ Medical Records Numbers ☐ Medical Notes ☐ Financial Account Information and/or Numbers (e.g., checking account number and PINs) ☐ Certificates (e.g., birth, death, and marriage) ☐ Legal Documents or Notes (e.g., divorce decree, criminal records, or other) ☐ Device Identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web URLs ☐ E-mail Address ☐ Education Records ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Information Sharing Practices				
16	**Is there a notification process in place when changes occur (i.e., revisions to PII or when the system encounters a major change or is replaced) for alerting other resources dependent upon PII contained on this system?** Note: If yes, please describe briefly the notification process in the Comments column. **Remediation Guidance:** If a department is a recipient department or a source department in a matching program with a non Federal agency, a notice must be published in the Federal Register of any revision of a matching program (or system of records) as defined by the Privacy Act. Develop or update enterprise-wide, streamlined process for procedures to alert interagency and intra-department users of PII contained on the system.	☒	☐	☐	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Information Sharing Practices				
17	**Are processes in place for periodic review of PII contained in the system to ensure it is timely, accurate, and relevant?** Note: If yes, please describe briefly the review process, including the process of retention and destruction of files deemed untimely, inaccurate or irrelevant in the Comments column. **Remediation Guidance:** If no, then section (e) (6) of the *Privacy Act of 1974* is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. PBGC are responsible for ensuring processes are in place to verify and validate PII as directed by the Act.	☒	☐	☐	
18	**Are rules of conduct in place for access to PII on the system?** Note: If yes, identify in the Comments column all users with access to PII on the system, and for what purposes they use the PII. **Remediation Guidance:** If no, then Section (e) (9-10) of the *Privacy Act of 1974* is invoked. The Act requires rules of conduct for persons involved in the design, development, operations, or maintenance of a system's PII.	☒	☐	☐	☒ Users ☒ Administrators ☐ Developers ☒ Contractors For what purposes: ☐ _____ ☐ _____ ☐ _____ ☐ _____ ☐ _____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Information Sharing Practices				
19	**Does the system host a web site either as an Internet, an intranet, or both?** Note: If yes, identify what type of site in the Comments column. **Note: If no, check N/A for all subsequent questions in the "Web Site Host Question Sets" section and answer questions starting with the "Administrative Controls" section beginning with Question #28.** **Remediation Guidance:** If yes, then *OMB M-99-18* is invoked requiring that for every federal, public web site agencies include a privacy policy statement, even if the site does *not* collect any information and does not create a Privacy Act record.	☐	☒	☐	Type of site: ☐ Internet_____ ☐ Intranet _____ ☐ Both_____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Web Site Host – Question Sets				
20	**Is the web site accessible by the public or other entities (i.e., contractors, third party administrators, state, or local agencies, etc.)?** **Remediation Guidance:** If yes, then *OMB M-99-18* is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, and any web page where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.	☐	☐	☒	
21	**Is a privacy policy statement posted on the web site?** **Remediation Guidance:** If no, then *OMB M-99-18* is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agencies will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.	☐	☐	☒	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Web Site Host – Question Sets				
22	**Are web links posted anywhere on the web site?** **Remediation Guidance:** If no, then *OMB M-99-18* is invoked. Agencies must post privacy policies on their principal web sites, any known major entry points, as well as any web pages where substantial personal information is collected from the public. The privacy policy must state what information is being collected, why it is being collected, and how the agency will use the information. Privacy policies must be clearly labeled and easily accessed when an individual visits a web site.	☐	☐	☒	
23	**Are cookies present on the web site?** Note: If yes, identify types of cookies in the Comments column. **Remediation Guidance:** If yes, persistent cookies are prohibited. Alternatively, session cookies are allowed as long as use of session cookies are indicated in the privacy policy statement and the agency is able to demonstrate a valid need for use of these session cookies. Cookies will not knowingly be transferred to third parties unless explained in the Privacy and Security Statement.	☐	☐	☒	☐ Session Cookies ☐ Persistent Cookies

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Web Site Host – Question Sets				
24	**Does the web site have any information or pages directed at children?** **Remediation Guidance:** If yes, then the *Children's Online Privacy Protection Act (COPPA), OMB M-00-13*, are all invoked. Agency systems hosting web sites are mandated by OMB to comply with COPPA. This law places restrictions on the collection and use of information on any web site or online service directed to children and requires parental consent before any such collection and provides the parent with the right to see what is collected about his/her child and to restrict dissemination or use or further collection of any information about the child.	☐	☐	☒	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
Web Site Host – Question Sets					
25	**Does the web site *collect* PII from individuals?** Note: If yes, identify what PII the system collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category. **Remediation Guidance:** If yes and data elements are checked under both the Identifier and Personal Information categories, then the *Privacy Act of 1974* is invoked. Agencies must meet all requirements of the Privacy Act listed under *5 U.S.C. 552a. (4)* As amended listed under "Records Maintained On Individuals." If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then the *HIPAA Privacy Rule, 67 FR 14775* may be invoked. Agencies should review this rule to determine exact applicability and compliance requirements. If personal information on the system contains Financial Account Information and/or Numbers, then the *Right to Financial Privacy Act of 1978* (*12 U.S.C. 3401 et seq*.) privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.	☐	☐	☒	**Personal Information:** ☐ Name ☐ Date of Birth ☐ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic Identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's License ☐ Biometric Identifiers (e.g., fingerprint and voiceprint) ☐ Mother's Maiden Name ☐ Vehicle Identifiers (e.g., license plates) ☐ Mailing Address ☐ Phone Numbers (e.g., phone, fax, and cell) ☐ Medical Records Numbers ☐ Medical Notes ☐ Financial Account Information and/or Numbers (e.g., checking account number and PINs) ☐ Certificates (e.g., birth, death, and marriage) ☐ Legal Documents or Notes (e.g., divorce decree, criminal records, or other) ☐ Device Identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web URLs ☐ E-mail Address ☐ Education Records ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Web Site Host – Question Sets				
26	**Does the web site *share* PII with internal or external parties of the PBGC?** Note: If yes, specify with whom and for what purposes, and identify the data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category. **Remediation Guidance:** If yes, then section (e) (6) of the Privacy Act is invoked. Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of the Act, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes. Agencies are responsible for ensuring processes are in place to verify and validate PII as directed by the Act. If personal information on the system contains medical records numbers or medical notes (including medical images such as x-rays), then Disclosure Officer may be required to authorize sharing of medical PII. Additionally, the *HIPAA Privacy Rule, 67 FR 14775* may be invoked. Agencies should review these rules to determine exact applicability and compliance requirements. If personal information on the system contains Financial Account Information and/or Numbers, then *Gramm-Leach-Bliley Act (GLBA) of 1999 Pub. Law No. 106-102, 113 Stat. 1338 (1999)* privacy requirements may be invoked. Agencies should review this law to determine exact applicability and compliance requirements.	☐	☐	☒	With whom and for what purposes: ☐ _____ ☐ _____ ☐ _____ ☐ _____ ☐ _____ PII shared: **Personal Information:** ☐ Name ☐ Date of Birth ☐ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic Identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's License ☐ Biometric Identifiers (e.g., fingerprint and voiceprint) ☐ Mother's Maiden Name ☐ Vehicle Identifiers (e.g., license plates) ☐ Mailing Address ☐ Phone Numbers (e.g., phone, fax, and cell) ☐ Medical Records Numbers ☐ Medical Notes ☐ Financial Account Information and/or Numbers (e.g., checking account number and PINs) ☐ Certificates (e.g., birth, death, and marriage) ☐ Legal Documents or Notes (e.g., divorce decree, criminal records, or other) ☐ Device Identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web URLs ☐ E-mail Address ☐ Education Records ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____ ☐ Other:_____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
Web Site Host – Question Sets					
27	**Are rules of conduct in place for access to PII on the website?** Note: If yes, identify in the Comments column all categories of users with access to PII on the system, and for what purposes the PII is used.	☐	☐	☒	☐ Users ☐ Administrators ☐ Developers ☐ Contractors For what purposes: ☐ _____ ☐ _____ ☐ _____ ☐ _____ ☐ _____

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
Administrative Controls					
Note: This PIA Guide uses the terms "Administrative," "Technical and "Physical" to refer to security control questions—terms that are used in several Federal privacy laws when referencing security requirements. PBGC recognizes the slight difference in terminology used in this guide from those that are used in other documents such as the *National Institute of Standards and Technology (NIST) SP 800-26, Security Self-Assessment Guide for Information Technology Systems*.					
28	**Has the system been authorized to process information?** **Remediation Guidance:** If no, then the system may be required as directed by *OMB Circular A-130* to complete an accreditation for each system. Agencies should engage in an assessment process that ensures technical security features are built into the life cycle of a system.	☐	☒	☐	
29	**Have there been major changes (as defined in Appendix A, "Glossary of Terms" of the PIA Questionnaire) to the system since it was last certified and accredited?** **Remediation Guidance:** If yes, then agencies are required by *OMB Circular A-130* to complete an update of the certification and accreditation for each system that has been modified. Agencies should engage in an assessment process that ensures existing technical security features are appropriate to the modified system.	☐	☒	☐	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Administrative Controls				
30	**Are security controls routinely reviewed?** **Remediation Guidance:** Security controls need to be routinely reviewed to ensure sustained effectiveness even when no changes to the system have occurred. *OMB Circular A-130* stipulates a system's security controls should be reviewed "when significant modifications are made to a system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system."	☒	☐	☐	
31	**Is there a system security plan for this system?** **Remediation Guidance:** The *Privacy Act of 1974* and *OMB Circular A-130* require procedures be in place for implementing administrative, technical, and physical security controls for systems containing a system of records. Agencies should develop a plan that demonstrates security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.	☒	☐	☐	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Administrative Controls				
32	**Is there a contingency (or backup) plan for the system?** **Remediation Guidance:** The *Privacy Act of 1974* and *OMB Circular A-130* require procedures be in place for implementing a contingency plan for systems containing a system of records. Agencies should develop a plan that demonstrates contingency security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.	☒	☐	☐	
33	**Are files backed up regularly?** **Remediation Guidance:** *OMB Circular A-130* requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should devise a method for backing up information contained on the system at regular intervals.	☒	☐	☐	
34	**Are the backup files stored offsite?** **Remediation Guidance:** *OMB Circular A-130* requires procedures be in place for protecting data on systems in the event the system and the information it contains is attacked or rendered unavailable. Agencies should identify an alternative site for housing backup files.	☒	☐	☐	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Administrative Controls				
35	**Are there user manuals for the system?** **Remediation Guidance:** If no, *OMB Circular A-130* requires that each agency assure the security of information contained on each system to include training of users and employees of security controls in place. Agencies should provide user reference manuals for each system.	☒	☐	☐	
36	**Have personnel using the system been trained and made aware of their responsibilities for protecting personal information being collected and maintained**? **Remediation Guidance:** If no, *OMB Circular A-130* requires that each agency ensure the security of information contained on each system to include training of users and employees of security controls in place. Agencies should provide users with training of their roles and responsibilities for protecting PII collected and maintained on the system.	☒	☐	☐	
37	**Who will have access to the PII on the system?** Note: Check all that apply in the Comments column.				☒ Users ☒ Administrators ☐ Developers ☒ Contractors
38	**Are methods in place to ensure least privilege (i.e., "need to know" and accountability)?** Note: If yes, please specify method(s) in the Comments column.	☒	☐	☐	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
	Technical Controls				
39	**Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?** Note: If yes, check all that apply in the Comments column. **Remediation Guidance:** If no, *OMB Circular A-130* requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.	☒	☐	☐	☒ User ID ☒ Passwords ☒ Firewall ☐ Virtual Private Network (VPN) ☒ Encryption ☒ Intrusion Detection System (IDS) ☐ Common Access Cards (CAC) ☐ Smart Cards ☐ Biometrics ☐ Public Key Infrastructure (PKI) ☐ Other _____ ☐ Other _____ ☐ Other _____
40	**Are the following password controls in place?** Note: Check all that apply in the Comments column. **Remediation Guidance:** If no, *OMB Circular A-130* requires that each agency ensure the security of information contained on each system. Agencies should implement one or more of the password controls for each system to protect the PII it contains.	☒	☐	☐	☒ Passwords expire after a set period. ☒ Accounts are locked after a set period of inactivity. ☒ Minimum length of passwords is eight characters. ☐ Passwords must be a combination of uppercase, lowercase, and special characters. ☒ Accounts are locked after a set number of incorrect attempts.
41	**Is a process in place to monitor and respond to incidents?**	☐	☐	☐	

No.	Privacy Question Sets	User Responses			Comments
		Yes	No	N/A	
Technical Controls					
Physical Controls					
42	**Are physical access controls in place?** Note: If yes, check all that apply in the Comments column. **Remediation Guidance:** If no, *OMB Circular A-130* requires that each agency ensure the security of information contained on each system by implementing technical security controls. Agencies should devise administrative, technical, and physical controls for each system to protect the PII it contains.	☒	☐	☐	☒ Guards ☒ Identification Badges ☐ Key Cards ☐ Cipher Locks ☐ Biometrics ☐ Closed Circuit TV (CCTV) ☐ Other _____ ☐ Other _____ ☐ Other _____
- END -					

Privacy Impact Assessment
Contact Information

_____ _____

Signature of Assessor ***Date***
(i.e., Information System Owners, Operator, Developer, or Other)

_____ _____

Print Name ***Title/Position***

_____ _____

Signature of Program Manager (if not Assessor) ***Date***

_____ _____

Print Name ***Title/Position***

_____

PBGC and Office/Department

_____

Street Address

_____

Street Address

_____

City, State and Zip Code

_____ _____

Phone Number ***Fax Number***

4 SAMPLE PIA EXECUTIVE SUMMARY REPORT OUTLINE

The following outline should be used to develop a one- to two-page overview of the findings of the PIA. It should be submitted on top of the completed PIA Questionnaire (Section 3).

I. INTRODUCTION TO THE PIA

- Purpose
- Scope

Identify the system and the agency where it is located. Also, describe the system components, elements, users, field site locations (if any), and any other details about the system to be considered in this assessment.

II. PIA APPROACH

Briefly, describe the approach used to conduct the risk assessment, such as:

- Participants (e.g., PIA team members)
- Technique used to gather information (e.g., the use of tools and questionnaires)

III. SYSTEM CHARACTERIZATION

Characterize the system, including hardware, software, system interfaces, data, and users. Consider providing a connectivity diagram or system input and output flowchart to delineate the scope of this PIA effort.

IV. THREAT STATEMENT (Optional)

Consider compiling a list of the potential threat sources and associated threat actions applicable to the system assessed.

V. PIA RESULTS

Document findings and mitigation actions to be taken.

VI. SUMMARY

Conclude the PIA Executive Summary Report and direct the reader to the attached, completed PIA Questionnaire.

Appendix A: Glossary of Terms

TERM	DEFINITIONS
Administrative Controls	Safeguards to ensure proper management and control of information and information systems. These safeguards include policy, PIAs, and certification and accreditation programs. (*NIST Special Publication 800-12*)
Availability	A requirement intended to assure that systems work promptly and service is not denied to authorized users. (*NIST SP 800-12*)
Child/Children	The *Children's Online Privacy Protection Act (COPPA) of 1998* defines a "child" as a person under the age of 13.
Confidentiality	A requirement that private or confidential information not be disclosed to unauthorized individuals. (*NIST SP 800-12*,)
Cookie	Information that a web site puts on an individuals computer so that it can remember something about the user later. *See also: persistent cookie, session cookie*.
General Support System	An interconnected information resource under the same direct management controls that shares functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from different or the same organizations. (*NIST SP 800-16*)
Integrity	Information that is timely, accurate, complete, and consistent. Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (*NIST SP 800-12*)
Major Application	An application that requires special attention to security because of the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a MA might compromise many individual application programs and hardware, software, and telecommunications components. MAs can be either a major software application or a combination of hardware and software where the only purpose of the system is to support a specific mission-related function. For purposes of this PIA Questionnaire, an MA is expanded to include software programs capable of storing PII in file documents such as those provided in Microsoft Office (i.e., Word and Excel).
Major Change	Any change that is made to the system environment or operation of the system. The following are examples of major changes: • Network, hardware, or software applications that alter the mission, operating environment, or basic vulnerabilities of the system • Increase or decrease in hardware, application programs, external users, or

TERM	DEFINITIONS
	hardware upgrades • Addition of telecommunications capability • Change to program logic of application systems • Relocation of system to new physical environment or new organization.
Network Connected	A general support system having either modem connection capability or a network connection to a server or to one or more computers.
Persistent Cookie	A cookie that is stored on the user's hard drive and remains there until the user deletes it or it expires.
Personally Identifiable Information	Any item, collection, or grouping of information about an individual that is maintained by an agency, including education, financial transactions, medical history, and criminal or employment history. The data may also contain his or her name, other identifying number or symbol, or other identifying information unique to the individual, such as a fingerprint or a photograph. This data may be found at PBGC in the form of medical records or reports on citizens or pay and benefits information on employees.
Physical Security Controls	Measures taken to protect systems buildings and related supporting infrastructure against threats associated with their physical environment. These safeguards might include protections against fire, structural collapse, plumbing leaks, physical access controls, and controls against the intercept of data. (*NIST SP 800-12*)
Privacy Act Systems of Records Notice (PARN)	All systems with Privacy Act information contained within them are required to publish in the Federal Register Records Notice informing the public as to, among other things, what information is contained in the system, how it is used, and how an individual may gain access to information regarding him or herself.
Privacy Impact Assessment (PIA)	A methodology that provides IT security professionals with a process for assessing whether appropriate privacy policies, procedures, and business practices—as well as applicable administrative, technical and physical security controls—have been implemented to ensure compliance with Federal privacy regulations.
Record	Any item, collection, or grouping of information about an individual identifiable to that individual and maintained by an agency. (*IRS Model IT PIA*)
Retrievable	A characteristic describing the ability to obtain or "pull up" a record in such a way that would allow a person to reasonably identify the subject of the record.
Routine Use	With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected. (*IRS Model*)
Sensitive System	A system that is not classified as an MA or GSS but still requires special management attention. These systems process, transmit, or store data

TERM	DEFINITIONS
	protected under the scope of the *Privacy Act of 1974*, *Trade Secrets Act*, *OMB Order on Statistical Confidentiality*, *OMB Statistical Policy Directive #3*, the *Financial Management Improvement Act of 1996*, or the system's failure would impair public confidence in PBGC.
Session Cookie	A small file, stored in temporary memory, containing information about a user that disappears when the user's browser is closed. Unlike a persistent cookie, no file is stored on the user's hard drive.
Stand-Alone System	A system that is neither network-connected nor connected to any other system or group of systems.
System	A system is an organized assembly of IT resources and procedures integrated and regulated by interaction or interdependence to accomplish a set of specified functions.
System of Records	A group of records under the control of any agency where information is retrieved by the name of the individual, by some identifying number or symbol, or by other identifiers assigned to the individual. (*IRS Model IT PIA*)
Technical Controls	Safeguards that are generally executed by the computer system. Technical safeguards include password protection, firewalls, and cryptography. (*NIST SP 800-12*)
Web Site	A collection of interlinked web pages (on either Internet or intranet sites) with a related topic, usually under a single domain name, which includes an intended starting file called a "home page." From the home page, access is gained to all the other pages on the web site.

Appendix B: Acronyms

CAC	Common Access Cards
CCTV	Closed Circuit TV
CIO	Chief Information Officer
COPPA	Children's Online Privacy Protection Act
PBGC	Pension Benefit Guaranty Corporation
GLBA	Gramm-Leach-Bliley Act
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IDS	Intrusion Detection System
IT	Information Technology
ITSLCM	Information Technology Solutions Life Cycle Methodology
MA	Major Application
NIST	National Institute of Standards and Technology
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OSHA	Occupational Safety and Health Administration
PARN	Privacy Act System of Records Notice
PBGC	Pension Benefit Guaranty Corporation
PKI	Public Key Infrastructure
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Actions and Milestones
SP	Special Publication
VPN	Virtual Private Network

Appendix C: References

Privacy Act	Privacy Act of 1974 5 U.S.C. 552a As Amended http://www4.law.cornell.edu/uscode/5/552a.html (for full text of the law**)** http://www.usdoj.gov/04foia/04_7_1.html (for an overview and summary of Privacy Act case law)
COPPA	Children's Online Privacy Protection Act http://www.ftc.gov/ogc/coppa1.htm
HIPAA	Health Insurance Portability and Accountability Act of 1996 Privacy Rule, 67 FR 14775 http://thomas.loc.gov/cgi-bin/query/z?c104:H.R.3103.ENR:
RFPA	Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.) http://www4.law.cornell.edu/uscode/12/ch35.html
OMB Memorandum No. M-99-18	Office of Management and Budget Memorandum No. M-99-18 "Privacy Policies on Federal Web Sites," June 2, 1999 http://www.whitehouse.gov/omb/memoranda/m99-18.html
OMB Memorandum No. M-00-13	Office of Management and Budget Memorandum No. M-00-13 "Privacy Policies and Data Collection on Federal Web Sites," June 22, 2000 http://www.whitehouse.gov/omb/memoranda/m00-13.html
OMB A-130	OMB Circular A-130, Management of Federal Information Resources http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
OMB A-11	OMB Circular A-11 (Exhibit 300) http://www.whitehouse.gov/omb/circulars/a11/2002/S300.pdf