



PENSION BENEFIT GUARANTY CORPORATION
OFFICE OF INSPECTOR GENERAL
EVALUATION REPORT

EVALUATION OF PBGC'S SECURITY POLICIES, PROCEDURES, AND STANDARDS

MAY 4, 2000

2000-9/23137-4



**Evaluation of PBGC's Security Policies,
Procedures, and Standards**

Evaluation Report 2000-9/23137-4

CONTENTS

	<u>Page</u>
Executive Summary	2
Background	3
Scope and Methodology	3
Summary of Issues based on AISSP Evaluation	4
Next Steps	6

TABS

Analysis of Existing Policy	A-1
Implementation of Procedures and Standards	B-1
New Systems Security Development Policy	C-1
Major Application/General Support system Security Plans - (NIST 800-18/OMB A-130 Compliance Review)	D-1
Internet/Intranet Security Policy	E-1
Windows NT Security Plan	F-1
Windows NT Security Standards	G-1
Unix Security Plan	H-1
Unix Security Standards	I-1
Oracle Security Plan	J-1
Oracle Security Standards	K-1

FIGURES

Figure 1	Overview	7
Figure 2	Issues	8

**Evaluation of PBGC's Security Policies,
Procedures, and Standards**

Evaluation Report 2000-9/23137-4

EXECUTIVE SUMMARY

The Office of Inspector General (OIG), assisted by PricewaterhouseCoopers LLP, (PricewaterhouseCoopers) performed an evaluation of PBGC's security policies, procedures, and standards that are documented in PBGC's *Automated Information Systems Security Plan* (AISSP). The objectives of this evaluation were to evaluate the adequacy of PBGC's security policies and practices and to compare them against Federal Government and private sector security standards and practices to identify possible security gaps at the policy level.

Our work used current security information available from the Federal Government and the private sector. Because of audit timing, the version of the AISSP reviewed by us may have undergone significant change or revisions by PBGC. If this is so, then PBGC could compare the guidelines and practices presented in this report to the updated version of AISSP. This would result in the almost up-to-date security requirements and practices being incorporated in PBGC's security policies, procedures, and standards.

Suggestions for Improvement

Below, we have listed several security issues (See Figure 1) needing improvements that PBGC should consider to strengthen its security policies, procedures and standards.

1. Establish One Set of Entity-Wide Security Policies, Procedures, and Standards. (See TAB A - "Analysis of Existing Policy" and TAB B - "Implementation of Procedures and Standards")
2. Security Standards over New Systems Development. (See TAB C - "New Systems Security Development Policy")
3. The AISSP Does Not Establish the Risks and Controls Over the Technology Infrastructure at PBGC and Does Not Comply With NIST and OMB Guidance. (See TAB D - "Major Application/General Support System Security Plans - NIST 800-18/OMB A-130 Compliance Review")
4. An Internet/Intranet Security Policy. (See TAB E - "Internet/Intranet Security Policy")
5. An Entity-Wide Security Plan For Windows NT. (See TAB F - "Windows NT Security Plan" and TAB G - "Windows NT Security Standards")
6. An Entity-Wide Security Plan For UNIX. (See TAB H - "UNIX Security Plan" and TAB I - "UNIX Security Standards")
7. An Entity-Wide Security Plan For Oracle. (See TAB J - "Oracle Security Plan" and TAB K - "Oracle Security Standards")

Evaluation of PBGC's Security Policies, Procedures, and Standards

Evaluation Report 2000-9/23137-4

Background

The Office of Inspector General (OIG), assisted by PricewaterhouseCoopers, performed an evaluation of PBGC's security policies, procedures, and standards that are documented in the PBGC's *Automated Information Systems Security Plan (AISSP)*. This evaluation helped us to obtain an understanding of the adequacy of the formal documentation used to establish the information security "blueprint" for PBGC. The objectives of this evaluation were to evaluate the adequacy of PBGC's security policies and practices and to compare them against Federal and private sector security standards and practices to identify possible security gaps at the policy level. In addition, this evaluation provided a residual benefit where we were exposed to PBGC's overall security culture and employee security awareness.

Scope and Methodology

Our scope included determining PBGC's technological infrastructure and evaluating what Federal criteria and private sector standards were applicable to serve as a baseline that PBGC could use as guidance and a point of reference in developing and enhancing security policies, procedures and standards. The primary areas we evaluated included, but were not limited to:

- ◆ Assessing the adequacy of the AISSP;
- ◆ Evaluating any functional gaps within the AISSP when compared with Federal security guidance and private sector practices;
- ◆ Determining the existence and adequacy of the policy planning and maintenance process in identifying existing security risks and controls; and
- ◆ Determining whether on-going maintenance of the security policies, procedures, and standards exist to reflect updates to address new inherent technological risks and controls.

We baselined PBGC's security policies, procedures and standards against key criteria that included guidance and standards from the following sources:

- ◆ National Security Agency (NSA);
- ◆ National Institute of Standards and Technology (NIST);
- ◆ The Information Systems Audit and Control Association and Foundation (ISACA); and
- ◆ Reference materials available from industry as well as software vendors covering various technologies used at PBGC.

Summary of Issues based on AISSP Evaluation

Our work uses current security information available from the Federal Government and private industry. Because of audit timing, the version of the security plan reviewed by us may have undergone significant change or revisions. If this is so, then PBGC could compare our guidelines and practices presented in this report with updated versions of the AISSP and be up-to-date with Federal security requirements and industry security practices. When we completed our review of the AISSP, we found areas where security policies, procedures, and standards were not current and could be improved by incorporating Federal guidelines and private industry practices.

This document's scope is comprehensive and contains suggestions for improving PBGC's security policies, procedures and standards. It should be used as a framework for beginning PBGC's information security process. In each of the TAB attachments, we have provided a page layout format so PBGC can easily determine which security policies, procedures, or standards require updating. The following describes the column headings:

- **Industry Practices.** This column lists current Federal security policies, procedure, and standards and private sector practices used to benchmark the AISSP.
- **Current PBGC Policy.** This column details the results of our review of PBGC's ASSIP to determine what security policies, procedure, and standards were currently being used and enforced by PBGC, and what may need to be added to strengthen PBGC's security environment.
- **Gaps.** This column describes the resultant from our comparison of current PBGC security policies, procedures, and standards against applicable Federal and industry security guidance and practices. Based on professional judgment, we recorded significant differences (gaps).
- **Suggested Corrective Action.** This column formulates our suggested improvements to strengthen PBGC security program.

Figure 1, *Overview*, graphically portrays several areas of improvement that we identified during our evaluation. These issues are key to strengthening PBGC's security policies, procedures, and standards. Figure 2, *Issues*, are specific corrective actions PBGC should implement to better position the agency in a more secure information technology environment. Below, we have provided a discussion on the identified issues.

1. **Establish a Single Entity-Wide Security Policies, Procedures, and Standards.** The effectiveness of one entity-wide security policy at PBGC is contingent upon the development and adherence to one uniform security policy (AISSP) throughout the agency. The risk of not developing uniform Security Policies, Procedures, and Standards may result in increased security risks through inconsistent interpretation and application of PBGC standards, which could impair the agency's reputation.

Reference: See TAB A – “Analysis of Existing Policy” and TAB B – “Implementation of Procedures and Standards”

2. **Security Standards Over New Systems Development** needs to be incorporated within the SDLC policy currently being developed. The existence of security standards throughout an application/systems development will serve as a preventive control for ensuring security is built into each phase of a program's

development and reduce the technology risk and expense of building these controls into an application and system after it is in production.

Reference: See TAB C – “New Systems Security Development Policy”

3. The AISSP Does Not Establish the Risks and Controls Over the Technology Infrastructure at PBGC and Does Not Comply With NIST and OMB Guidance for developing minimum security plan standards for major applications and general support systems. Some omissions within the plan include: (1) A detailed explanation of levels of management and user responsibilities, e.g., system owners, custodians and users; (2) enforcement standards; and (3) the process used for communicating, implementing and maintaining the information security policies, and standards in written form at PBGC.

Application Security Plans need to be developed and comply with NIST 800-18 and OMB A-130 guidelines for all management designated sensitive and mission-critical applications. This would include, but may not be limited to the following PBGC systems: Trust Accounting, CASR-R, Performance Accounting, IPS, LMS, ACT 1.0, MPP, FRS and MES. The plans need to address system identification, management, operational, and technical controls.

Application Security Plans covering CASE Administration System (CAS) Application Security Plan, Integrated Present Value of Future Benefits (IPVFB) and Genesis Production Instance do not comply with NIST 800-18 and OMB A-130 guidelines. The plans need to address system identification, management, operational, and technical controls.

Reference: See TAB D – “Major Application/ General Support System Security Plans – NIST 800-18/OMB A-130 Compliance Review”

4. An Internet and Intranet Security Policy needs development. The policy at the minimum, should address password management, authentication, data privacy, encryption and integrity, software import controls, remote access, incident response, appropriate use of the internet, firewall security and e-mail.

Reference: See TAB E – “Internet/Intranet Security Policy”

5. An Entity-Wide Windows NT Security Plan needs development that complies with NIST 800-18 and OMB A-130 guidelines and industry practices. The plans need to address system identification, management, operational, and technical controls. Specifically, NT security standards should address user set-up and administration controls, NT account and system policies, auditing policies, standards over the protection of files and directories, remote access service, monitoring and updating security and responding to incidents, security standards covering user rights, responsibilities and practices and security standards covering system services.

Reference: See TAB F – “Windows NT Security Plan” and TAB G – “Windows NT Security Standards”

6. An Entity-Wide UNIX Security Plan needs development that complies with NIST 800-18 and OMB A-130 guidelines and industry practices. The plan needs to address system identification, management, and operational and technical controls over basic UNIX security standards. Specifically, standards should address the technical controls over accounts administration of users and groups

(e.g. root account), technical controls over password management, guidelines for directory/file system access and security along with audit and monitoring standards.

Reference: See TAB H – “UNIX Security Plan” and TAB I – “UNIX Security Standards”

7. An Entity-Wide Oracle Security Plan needs development that complies with NIST 800-18 and OMB A-130 guidelines and industry practices. There are no uniform standards that govern basic Oracle security. The Oracle security standards are fragmented amongst several technical documents and offer no standardization for the risks and controls over this database. Specifically, the Oracle security plan should include a high-level discussion on general Oracle database standards, which identifies the roles and responsibilities of the various people involved, levels of authority, user identification & integrity, profiles, roles, system privileges, object-level privileges in addition to system and object auditing responsibilities.

Reference: See TAB J – “Oracle Security Plan” and TAB K – “Oracle Security Standards”

Next Steps

We encourage PBGC to use this report in its security planning process. The first step will require PBGC to review this document and understand its impact on each business process within PBGC. The challenge and opportunity for PBGC is to be cognizant that information security is the responsibility of every employee and its success can only be facilitated through each employees' understanding and practice of the basic guidelines contained within this document.

Additionally, security is an on-going process and its content goes well beyond the contents of this document. We encourage PBGC not only to review the contents of this document, but also to incorporate the importance of information security within the culture of this agency. In addition, PBGC is encouraged to provide continual input into the security planning process to ensure the criteria outlined within this document is continually updated to reflect PBGC technology, and reflects PBGC's contribution to the effectiveness and importance of information security.

Figure 1

Overview

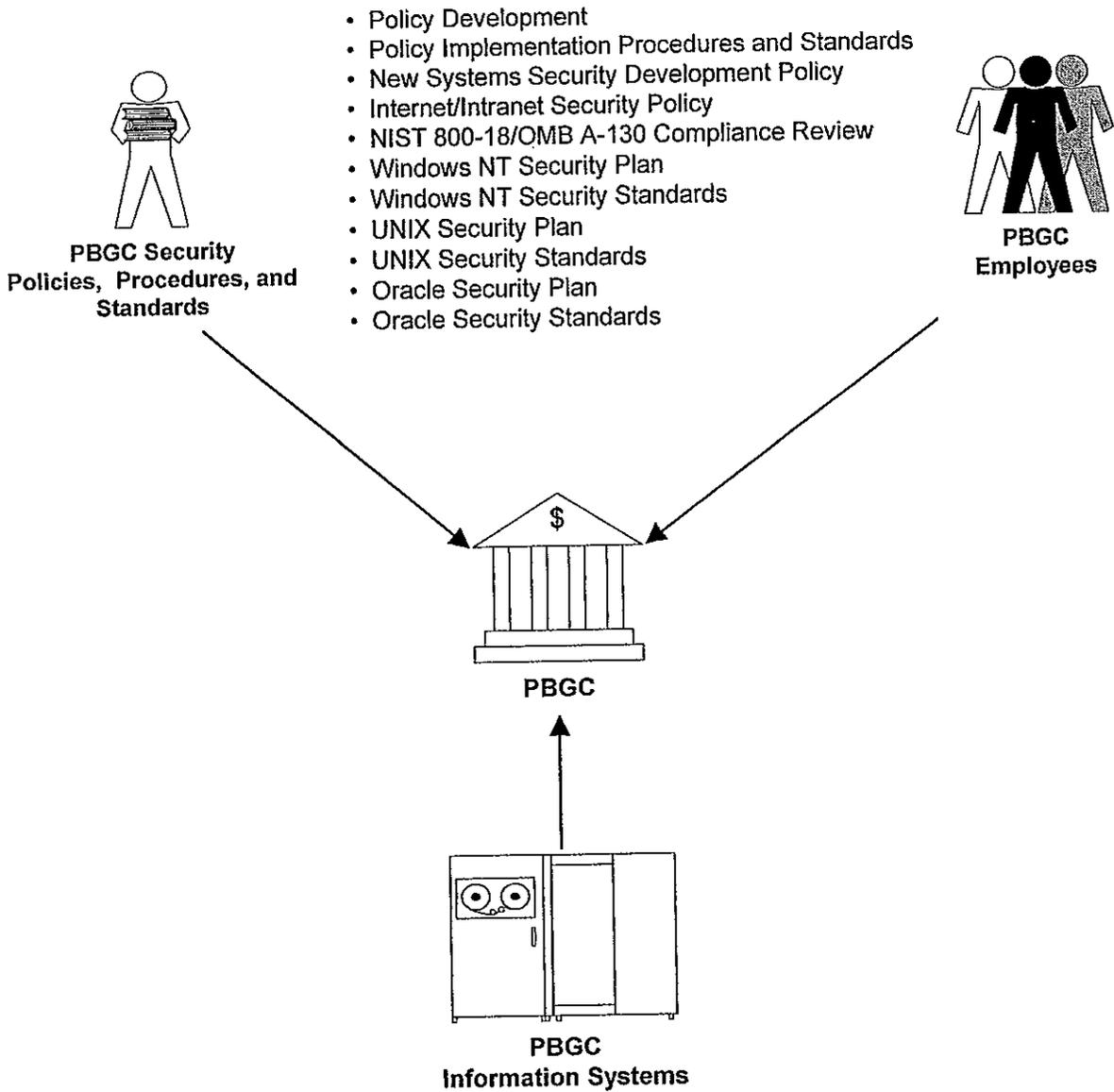
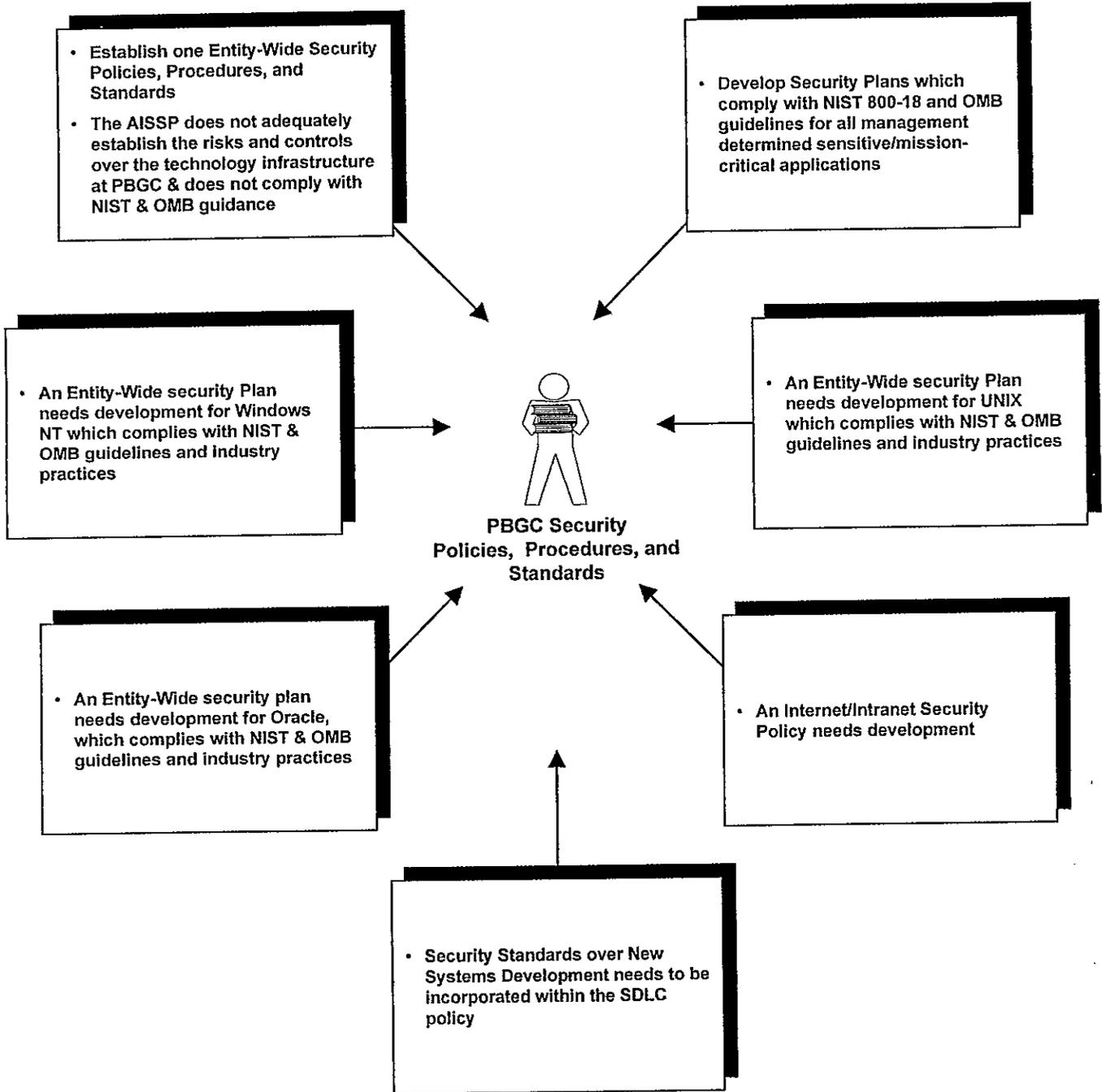


Figure 2

Issues



ANALYSIS OF EXISTING POLICY

Tab A

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
The existence of a comprehensive entity-wide Information Security POLICY Manual	<ul style="list-style-type: none"> Source document: The existence of the Automated Information Systems Security Program (AISSP) 	<ul style="list-style-type: none"> The AISSP does not adequately provide a high-level enterprise-Wide Security Plan which identifies technology risk and protection and information security standards 	<ul style="list-style-type: none"> Develop Corporate Strategic goals and link those goals to the further development of PBGC's Entity-Wide Information Security Policies, Procedures, and Standards Manual
a. Identification of applicable federal guidance over security plans (e.g., NIST Special Publication 800-18)	<ul style="list-style-type: none"> Source document: AISSP Reference made to OMB Circular A-130 	<ul style="list-style-type: none"> NIST Special Publication (SP) 800-18, "Guide for Developing Security Plans for Information Technology Systems" dated 12/98 is not mentioned 	<ul style="list-style-type: none"> Identify & provide a high level summary of NIST 800-18 guidelines within the AISSP (cross-reference to the individual security plans for all major applications and general support systems for a detailed breakout of 800-18 requirements)
b. Introduction and Scope	<ul style="list-style-type: none"> Source document: AISSP The purpose statement includes: <i>"This directive establishes policy responsibilities for assuring adequate resource protection/security for automated information systems (AIS), applications, and facilities. This document addresses issues relating to overall AIS security, including issues concerning the mainframe and minicomputer system environment(s). IM-05-3, PC and LAN Security Policy and Standards, addresses issues relating to the PBGC personal computer and local area network environments"</i> 	<ul style="list-style-type: none"> Policy limitations includes the lack of a high level discussion on: <ul style="list-style-type: none"> ➤ Network Infrastructure* ➤ Operating Systems/General Support Systems (e.g., NT & UNIX)* ➤ Major Applications* ➤ General Security Standards* ➤ General Database Security Standards ➤ *Internet Security Standards ➤ Virus Protection ➤ Access Security Controls ➤ End-User Computing ➤ Electronic Data Interchange – (EDI) ➤ Sensitivity of Data ➤ Employee Hiring and Termination Practices ➤ MIS disposition based on sensitivity ➤ Security Officer responsibilities ➤ Information retention and backup ➤ Document Filing and Retention ➤ Training ➤ Incident Reporting * Each item within this entity-wide policy statement should cross-reference to the appropriate security plan document which provides further detail in addressing NIST 800-18 & OMB – A130 requirements 	<ul style="list-style-type: none"> Include a brief discussion on the components of PBGC's technological environment to address the aforementioned categories and other categories deemed appropriate

ANALYSIS OF EXISTING POLICY

Tab A

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
c. Background	Same	<ul style="list-style-type: none"> The background comments do not address a general background policy statement on data security 	<ul style="list-style-type: none"> Include a general background statement, which addresses the background of PBGC and its focus on data security An example of such a statement may include the following: <i>"PBGC relies heavily on automated systems to meet its operational, financial and information requirements. These systems, their related data objects (e.g., files) and information derived from them are significant assets to, and proprietary to PBGC. As such, these systems and all related data must be adequately secured and protected against accidental and/or intentional disclosure or damage. To ensure the adequate safeguarding of systems and data, PBGC has instituted a system of internal controls, which are stated in this manual"</i>
d. An Information Security Statement	<ul style="list-style-type: none"> Source document: AISSP The Policy statement states: <i>"It is the policy of the PBGC that sensitive information, systems, applications, and facilities be secured to at least the minimum level of security defined in this and other related PBGC directives"</i> 	<ul style="list-style-type: none"> No general discussion on information security which addresses: <ul style="list-style-type: none"> > Accountability > Awareness > Integration > Timeliness 	<ul style="list-style-type: none"> Refer to the International Federation of Accountants document: "International accountancy releases technology guidance on managing security" for a complete listing of potential policy criteria
e. A Confidentiality and Acceptance Statement	<ul style="list-style-type: none"> Source Document: AISSP The Policy statement is entitled "Obtaining and Removing Access to Automated Data Systems" which identifies various forms used at PBGC (e.g. "PBGC Systems Access Request Form and PBGC Systems Access Request Form" 	<ul style="list-style-type: none"> The statement provides no explanation of which computer processing platforms this applies (e.g. mainframe, servers, personal computers), electronic media or hard copy documents proprietary to PBGC. Additionally, no discussion is made on who should be following the PBGC policies (e.g. Full-time, part-time employees, contractors and external consultants) There is no comment on who is responsible for the enforcement of this policy 	<ul style="list-style-type: none"> Develop a policy statement that addresses the aforementioned points and require that all PBGC users read this policy and verify that they understand and will follow the information security policies, procedures, and standards by signing the Confidentiality and Acceptance Agreement. A discussion should include who is responsible for the enforcement of the Information Security Policies, Procedures, and Standards Manual

ANALYSIS OF EXISTING POLICY

Tab A

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>f. Levels of responsibility</p>	<ul style="list-style-type: none"> • Source document: AISSP • The policy statement is entitled: Ownership and Management "Responsibility" <p>The responsibility of designated owner is outlined in addition to the responsibility of the Director for Information Resources Management Department</p>	<ul style="list-style-type: none"> • Levels of responsibility do not identify custodians, users and those responsible for performing periodic risk assessments 	<ul style="list-style-type: none"> • The levels of responsibility should address not only the owners of each system, but the custodians and users. • The custodian is responsible for the administration of controls as specified by the Data Owner, which includes the following: <ul style="list-style-type: none"> ➢ Providing and enforcing physical and logical standards ➢ Providing procedural guidelines for employees ➢ Administering access to information ➢ Evaluating cost effectiveness of controls • Users are responsible for the following: <ul style="list-style-type: none"> ➢ Adhering to all of established security policies, procedures, and standards ➢ Complying with controls established by the owner ➢ Ensuring that critical or sensitive data is not disclosed without permission from the owner ➢ Ensuring that their passwords are regularly changed and not disclosed or used by others ➢ The Information Security Officer needs to address his/her responsibility for communicating, implementing and maintaining the Information security policies, and Standards Manual. • The Director, Information Resources Management Department (IRMD) shall be responsible for: <ul style="list-style-type: none"> ➢ performing periodic risk assessments
<p>g. Review of the Security Policies, Procedures, and Standards Manual</p>	<ul style="list-style-type: none"> • Source document: AISSP • The policy statement is silent in addressing the review requirements of the AISSP 	<ul style="list-style-type: none"> • The policy does not specify the frequency for reviewing, revising and reissuing the PBGC Security Policies, Procedures and Standards Manual 	<ul style="list-style-type: none"> • The policy should clearly state the frequency for reviewing, revising and reissuing the PBGC Security Policies, Procedures and Standards Manual

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of a comprehensive entity-wide POLICY IMPLEMENTATION PROCEDURES AND STANDARDS</p>	<ul style="list-style-type: none"> • Source document: AISSP • The existing Automated Information Systems Security Program document needs expansion to address the primary components of a comprehensive policy implementation procedures and standards manual 	<ul style="list-style-type: none"> • The policy implementation procedures and standards are either absent or need further expansion on the following primary topics: <ul style="list-style-type: none"> ➢ Information Security Standards ➢ Information Security Enforcement & Maintenance ➢ Information Security Awareness ➢ Terminated and Transferred Users ➢ PBGC Systems Authorization & User Access Levels ➢ User-id and Password Control ➢ Compromised Passwords ➢ Personal Use ➢ Program and Library Access ➢ Virus Protection ➢ User Workstations, Microcomputers and Notebooks ➢ Remote Access ➢ Overview of technological infrastructure (Network, operating systems, Database & the use of the Internet) 	<ul style="list-style-type: none"> • There is a need for either enhancing existing standards or developing new standards to address the Gaps noted
<p>a. Development of Information Security Standards covering:</p> <ul style="list-style-type: none"> • Authorization to access information • Responsibility for risk evaluation • User-id and password • Safeguarding of user-id and password • Role of logical security officer • User responsibilities relative to security • Confidentiality • Sharing of Information • Disciplinary action 	<ul style="list-style-type: none"> • Source document: AISSP • The information security standards satisfactorily addresses the aforementioned standards: <ul style="list-style-type: none"> ➢ Authorization to access information ➢ Responsibility for risk evaluation ➢ User-id and password ➢ Safeguarding of user-id and password ➢ Role of logical security officer ➢ User responsibilities relative to security 	<ul style="list-style-type: none"> • The information security standards do not address the requirement of PBGC AIS User relating to their role and responsibility concerning confidentiality, sharing of information and disciplinary action. 	<ul style="list-style-type: none"> • Include within the information security standards statements which stress the following areas: <ul style="list-style-type: none"> ➢ Confidentiality - A statement may include: "All PBGC employees and contracted third parties must comply with all PBGC security policies, procedures and standards and must comply with legal, statutory and regulatory requirements, both domestic and international, pertaining to the protection, sharing, or disclosure of PBGC information. The "Information Security Acknowledgement" form is used to document PBGC employee and contracted third parties compliance to treating PBGC information as a confidential asset and understanding and following the Security Policies, Procedures, and Standards."

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<ul style="list-style-type: none"> > Sharing of Information: A statement may include: "Users are prohibited from sharing data with individuals who are not PBGC employees unless authorized to do so by their Business Unit Management and the Data Owner. This includes computer diskettes or hard copy documents." > Disciplinary Action: A statement may include: "Unauthorized dissemination of PBGC data by PBGC employees to non-PBGC persons will result in immediate disciplinary action."
<p>b. Development of Information Security Standards covering <i>Enforcement & Maintenance</i></p>	<ul style="list-style-type: none"> • Source document: AISSP • The Policy states that the Automated Information Systems Security Manager (AISSM) shall implement and manage the AIS Security Program 	<p>Enforcement</p> <ul style="list-style-type: none"> • No specific identification within the AISSM's role relative to their role in the enforcement of the information security policies, procedures, and standards <p>Maintenance</p> <ul style="list-style-type: none"> • No specific discussion relative to who is responsible for maintaining and updating the Information Security Standards and Maintenance 	<ul style="list-style-type: none"> • There should be a statement that identifies both enforcement and maintenance. A statement may include: <ul style="list-style-type: none"> > PBGC security policies, procedures, and standards are maintained and updated by the AISSM, with input from Business Unit Management > PBGC security policies, procedures, and standards are maintained and updated by the AISSM, with input from Business Unit Management > PBGC management must proactively support, maintain, and monitor the effectiveness of and compliance with the PBGC Information Security Policies, Procedures, and Standards
<p>c. Development of Information Security Standards covering <i>security awareness, training, and education</i></p>	<ul style="list-style-type: none"> • Source document: AISSP • Reference is made to the roles and responsibilities of the Automated Information Systems Security Manager (AISSM) implementing and managing the AIS security program and developing corporate AIS security objectives, procedures, and guidelines 	<ul style="list-style-type: none"> • The AISSP do not address: <ul style="list-style-type: none"> > The method of communicating security awareness 	<ul style="list-style-type: none"> • There should be a statement that identifies the method of communicating security awareness: <ul style="list-style-type: none"> > Issuance of the Security policies, procedures and standards to all new employees > Existing PBGC employees periodically receive information & security awareness updates and are responsible for placing these updates in the proper section(s) of their manual > The Information Security

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<p>Acknowledgement form must be completed and signed by each full-time or part-time PBGC employee and contracted third party every year and forwarded to the AISSM every year.</p> <ul style="list-style-type: none"> ➤ Ongoing training which covers security awareness and training, which includes software licensing and copyright infringement.
<p>d. Development of Information Security Standards covering <i>Terminated and Transferred Users</i></p>	<ul style="list-style-type: none"> • Source document: AISSP <ul style="list-style-type: none"> ➤ The policy is silent in addressing formal transfers, resignations, or termination procedures. ➤ The only policy comment made relative to human resources involvement states: "The Director, Human Resources Department, as Personnel Security Officer, will arrange for investigations of PBGC personnel in AIS-related positions to determine security eligibility" 	<ul style="list-style-type: none"> • Policy discussions are either limited or do not exist for the following areas: <ul style="list-style-type: none"> ➤ Human Resource involvement ➤ Discharge of individuals ➤ Review of user's account ➤ Computer equipment of departed employees ➤ Access cards 	<ul style="list-style-type: none"> • There should be a statement that discusses each of the aforementioned topics, for example: <ul style="list-style-type: none"> ➤ HR or PBGC management must immediately notify the AISSM of all employee terminations either via e-mail or memo. ➤ Upon the discharge of individuals responsible for system administration (i.e. DBA's, SA's, AISSM, etc.), their user access accounts should be disabled and the passwords changed until the accounts can be reviewed by PBGC management ➤ PBGC management should review the disposition of the user's account(s) (e.g. data and files residing on the network or application directories with the user), prior to the user's departure or transfer. PBGC management will notify the AISSM in writing of which files or directories should be destroyed or saved and appropriately documented. ➤ Any computer equipment assigned to the employee will be obtained by PBGC management prior to their departure ➤ All access cards are retrieved by PBGC management from the employee prior to his/her departure

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>6. Development of Information Security Standards covering PBGC Systems Authorization & User Access Levels</p>	<ul style="list-style-type: none"> • Source document: AISSP • Reference is made to the following areas within the Access Controls section: <ul style="list-style-type: none"> > User Identification and Authentication > Password Controls > Application and Data Controls > Uploading and Downloading Data > Dial-up Access > PC and LAN Business Recovery 	<ul style="list-style-type: none"> > Communication by PBGC management to the AISSM, regarding any significant changes in end-user duties which affects a user's access levels • Policy discussions are either limited or do not exist for the following areas covering Systems Authorization: <ul style="list-style-type: none"> > Reference to the "PBGC Systems Access Request Form" > Requirements for non-PBGC employees (i.e. consultants, contractors) > Controls surrounding the use of emergency access user-id and passwords 	<p style="text-align: right;">and the cards are deactivated</p> <ul style="list-style-type: none"> > PBGC management must promptly report any significant changes in end-user duties which affects a user's access levels to the AISSM • There should be a statement that discusses each of the aforementioned topics, which addresses Systems Authorizations: <ul style="list-style-type: none"> > All users accessing any part of the PBGC technological infrastructure need to complete the "PBGC Systems Access Request Form" > All "PBGC Systems Access Request Forms" must be approved by the Data Owner, the Department Manager and the AISSM > Systems access for non-PBGC employees must be approved by the Data Owner and the Business Unit Management to whom the individual will report, with access revoked at the completion of the individual's assignment > The use of emergency access user-ids and passwords will be used on an as-needed basis as determined by the AISSM. Once the emergency user-ids and passwords are utilized to resolve an emergency, they should be revoked and the activity associated with use of the emergency access user-id and password reviewed by the user's Business Unit Management in coordination with the AISSM

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
		<ul style="list-style-type: none"> • Policy discussions are either limited or do not exist for the following areas involving <i>User Access Levels</i>: <ul style="list-style-type: none"> > Reviews of access levels > System privileges assigned and defined > Restricting access to data and files of other users 	<ul style="list-style-type: none"> • There should be a statement that discusses each of the aforementioned topics, which addresses <i>User Access Levels</i>, for example: <ul style="list-style-type: none"> > Reviews of authorized user access levels will be performed annually by the Business User Management in coordination with the AISSM. Assigned access levels should be commensurate with established job responsibilities of the intended user > System privileges must be assigned and defined so that non-production staff are prohibited from updating production data, unless specifically authorized by Business Unit Management, the data owner, and the AISSM > The ability to access and examine security data and files of other users must be restricted to those responsible for System Management and/or Security (e.g., DBA, SA, AISSM) > Computer Operators and Programmers will not be given access to or be permitted to modify production data, programs or operating systems beyond their normal job functions
<p>f. Development of Information Security Standards covering <i>User-id and Password Control</i></p>	<ul style="list-style-type: none"> • Source document: AISSP • Reference is made to the following areas within the <i>Access Controls</i> section: <ul style="list-style-type: none"> > User Identification and Authentication > Password Controls 	<ul style="list-style-type: none"> • Policy discussions are either limited or do not exist for the following areas covering <i>User Identification and Password Controls</i> <ul style="list-style-type: none"> > User-ID requirements & Robust passwords – (policy indicates that passwords should not be easily guessed, but no specific criteria or examples provided) 	<ul style="list-style-type: none"> • There should be a statement that discusses each of the aforementioned topics, for example: <ul style="list-style-type: none"> > All PBGC users must use user-ids and robust passwords to gain access to PBGC systems and networks

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
		<ul style="list-style-type: none"> ➤ Responsibility of the AISSM relative to password issuance and user-ids administration ➤ Restrictions on Sharing and group passwords ➤ Allowing others to perform activities using another users user-id and password ➤ Writing down passwords 	<ul style="list-style-type: none"> ➤ Ensuring the AISSM enforces compliance with PBGC standards (Reference should be to the appendix of the plan for examples) ➤ Restrictions on shared and group passwords ➤ Users should not allow others to perform any activity with their user-ids or passwords ➤ Restrictions on writing down passwords and procedures for users to follow if this practice is detected
g. Development of Information Security Standards covering <i>compromised passwords</i>	<ul style="list-style-type: none"> • Source document: AISSP • The AISSP is silent on addressing this topic 	<ul style="list-style-type: none"> • Policy discussions do not exist for the following areas covering <i>Compromised passwords</i>: <ul style="list-style-type: none"> ➤ Vendor-supplied passwords ➤ Access by an unauthorized party (either internal or external) ➤ Process to follow if the an individual who has knowledge of the user passwords terminates employment or changes functions (e.g. AISSP and Systems Administrator) 	<ul style="list-style-type: none"> • There should be a statement that discusses each of the aforementioned topics, for example: <ul style="list-style-type: none"> ➤ All vendor-supplied default passwords must be changed before any computer or communication system or application is placed into the production environment. ➤ Develop a communication procedure in the event of having an unauthorized party compromise the system and the subsequent steps that would ensue should be detailed (e.g. all passwords must be changed and the O/S being reloaded) ➤ Requirement that all user passwords be changed
h. Development of Information Security Standards covering <i>personal use</i>	<ul style="list-style-type: none"> • Source document: AISSP • The AISSP is silent on addressing this topic 	<ul style="list-style-type: none"> • Policy discussions do not exist for the following areas covering: <ul style="list-style-type: none"> ➤ General restrictions on personal use 	<ul style="list-style-type: none"> • There should be a statement that discusses each of the aforementioned topics, for example: <ul style="list-style-type: none"> ➤ Users of PBGC computing and communications services are not allowed to use their facilities for

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
		<ul style="list-style-type: none"> ➤ Enforcement ➤ Internet & business use ➤ Prohibition of users in attempting to compromise the information security systems employed by PBGC ➤ Prohibition in the use of hardware or software to compromise information systems security 	<p>soliciting business, selling products, or otherwise engaging any commercial activities other than those expressly permitted by Business Unit Management</p> <ul style="list-style-type: none"> ➤ PBGC Unit Management reserves the right to revoke user access privileges of any user at any time due to inappropriate use of PBGC hardware or software ➤ Access to the WWW & other internet services is granted for business use ➤ A restriction should exist which prohibits users from compromising security, unless the AISSM approved for legitimate purposes (i.e. penetration testing) ➤ Same
<p>1. Development of Information Security Standards covering Program and Library Access</p>	<ul style="list-style-type: none"> • Source document: AISSP • The AISSP is silent on addressing this topic 	<ul style="list-style-type: none"> • Policy discussions do not exist for the following areas covering: <ul style="list-style-type: none"> ➤ Audit trails ➤ Restrictions on program altering utilities ➤ Prohibiting unauthorized access to PBGC operating systems, program libraries, and data libraries 	<ul style="list-style-type: none"> • There should be a statement that discusses each of the aforementioned topics, for example: <ul style="list-style-type: none"> ➤ All production application systems that process sensitive PBGC data must maintain records (e.g. audit trails) showing addition, modification or deliver of sensitive information ➤ Program utilities can only be accessed by authorized personnel ➤ Prohibits unauthorized access to PBGC operating systems, program libraries, and data libraries

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>j. Development of Information Security Standards covering <i>Virus Protection</i></p>	<ul style="list-style-type: none"> • Source document: AISSP and the PBGC Intranet guidelines ➢ Anti-Virus Guidelines exist which discuss*: <ul style="list-style-type: none"> ➢ Backing-up data files at least once a month ➢ Never download programs or games from recreational bulletin boards to the office PC <p>* Several other guidelines are also included within the PBGC Intranet site and the AISSP</p>	<ul style="list-style-type: none"> • Policy discussions do not exist for the following areas covering: <ul style="list-style-type: none"> ➢ New software and virus scan requirements ➢ No restrictions on end-users from installing non-standard PBGC approved software on their machines ➢ No discussion on restricting the downloading from external electronic mail systems, external communication networks or other non PBGC systems ➢ No integration of PBGC Intranet information on Virus Protection into the AISSP 	<ul style="list-style-type: none"> • There should be a statement that addresses, for example: <ul style="list-style-type: none"> ➢ All new software should undergo a virus scan prior to initial use ➢ Incorporate a statement within the PBGC Policy that states the restrictions on end-users from installing non-standard PBGC approved software on their machines ➢ Ensure a policy statement exists that restricts the downloading from external electronic mail systems, external communications networks or other non PBGC systems ➢ Virus protection is covered in two places at PBGC. The first within the AISSP & the second within the Intranet. While the Intranet is a good place for placing updates to the policy, there should be one uniform policy
<p>k. Development of Information Security Standards covering <i>User Workstations, Microcomputers and Notebooks</i></p>	<ul style="list-style-type: none"> • Source document: AISSP • The AISSP is silent on addressing this topic 	<ul style="list-style-type: none"> • Workstations and screen savers <ul style="list-style-type: none"> ➢ Procedures for back-up 	<ul style="list-style-type: none"> ➢ All workstations should have screen saver or other time out software that is activated after a period of inactivity ➢ Users will be responsible for the backup of data on the hard drives of their workstation(s). For backup assistance, users should contact the AISSM
<p>l. Development of Information Security Standards covering <i>Remote Access</i></p>	<ul style="list-style-type: none"> • Source document: AISSP • The following major point is covered within the AISSM: <ul style="list-style-type: none"> • Dial-up ports should be protected 	<ul style="list-style-type: none"> ➢ Policy discussions do not exist for the following areas covering: <ul style="list-style-type: none"> ➢ The role of the AISSP in monitoring remote access activity 	<ul style="list-style-type: none"> • There should be a statement that discusses each of the aforementioned topics, which states: <ul style="list-style-type: none"> ➢ The AISSM will log and monitor remote access activity to ensure protocols are following and that activity is in conformance with established security policies and procedures

IMPLEMENTATION OF PROCEDURES AND STANDARDS

Tab B

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>Overview of technological infrastructure (Network, operating systems, Database & the use of the Internet)</p> <p><i>Note: Separate security plans should be developed for NT, UNIX & the Internet</i></p>	<ul style="list-style-type: none"> • Source document: AISSP • The AISSP is silent on addressing this topic 	<ul style="list-style-type: none"> ➤ Confidentiality of dial-in access phone numbers ➤ No discussion of technological infrastructure (Network, O/S, database & the use of the internet) ➤ No specific security configuration standards for NT, UNIX and the Internet 	<ul style="list-style-type: none"> ➤ Users should keep dial-in access phone numbers confidential • There should be a policy statement which discusses: <ul style="list-style-type: none"> ➤ The network topology ➤ User set-up & administration ➤ Physical controls ➤ High-level discussion on the NT & UNIX operating systems with linkage back to those specific applications and databases

NEW SYSTEMS SECURITY DEVELOPMENT POLICY

Tab C

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of a policy which requires the use of additional <i>User Authentication</i> requirements – (Complex Passwords)</p>	<ul style="list-style-type: none"> Source document: The Application Development Security Guide. The guide currently has a vague reference to a <i>User Authentication</i> restriction, which states password patterns should be 6 to 8 alphanumeric characters, with at least one of each type (e.g. PQT1FYX)* A Systems Development/SDLC policy was requested, but not provided during this security review, as the document was currently under development at PBGC 	<ul style="list-style-type: none"> Policy discussions do not exist for the following areas covering <i>User Authentication</i>: <ul style="list-style-type: none"> > Passwords do not require the use of <i>Special Characters</i> and <i>Required Positions</i> 	<ul style="list-style-type: none"> There should be a policy statement that requires for example: <ul style="list-style-type: none"> > Special Characters (#, @, /, ? and) > Required Positions (Specify the type of character must appear in each password position. (e.g. ANV) <p>A – Alphabetic character N – Alphanumeric character V – Numeric character</p>
<p>The existence of a Systems Development–(SDLC) methodology which incorporates <i>Logical Access Control Levels</i></p>	<ul style="list-style-type: none"> Source document: The Application Development Security Guide* * Source document: The Application Development Security Guide 	<ul style="list-style-type: none"> There is no completed Systems Development/SDLC policy which addresses <i>logical access control levels</i> 	<ul style="list-style-type: none"> A determination should be made regarding the type of logical access controls for each application or system, which includes the following: <p>Logical Access Control Levels:</p> <ul style="list-style-type: none"> > System: (e.g. Once identified and authenticated, the user may access any data, function, or resource within the computer) > Application: (e.g. Once identified and authenticated, the end user accesses all capabilities within an automated application, however, may not be permitted access to another application) > Function: (e.g. The access within an application itself, such as adding new customers, but not deleting existing customers) <ul style="list-style-type: none"> ✓ ✓ Field: (e.g. The end user adding a new customer has all of the fields related to that task on one screen, but either cannot see the edit fields or can see those fields but cannot access them)
<p>The existence of a Systems Development–(SDLC) methodology which incorporates <i>Logical Access Types</i></p>	<ul style="list-style-type: none"> Source document: The Application Development Security Guide 	<ul style="list-style-type: none"> There is no completed Systems Development/SDLC policy which addresses <i>Logical Access Types</i> 	<p>Logical Access Types:</p> <ul style="list-style-type: none"> A determination should be made regarding the identification and use of <i>Logical Access Types</i> for each

NEW SYSTEMS SECURITY DEVELOPMENT POLICY

Tab C

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			application or system, for example: > The ability only to see and read information > The ability to add new information > The ability to change existing information > The ability to delete existing information
The existence of <i>End-User Log-In controls</i>	<ul style="list-style-type: none"> Source document: The Application Development Security Guide. Specific reference to the "Security Activities in the System Life-Cycle" matrix within the guide 	<ul style="list-style-type: none"> There is no completed Systems Development/SDLC policy which addresses <i>End-User Log-In Controls</i> 	<ul style="list-style-type: none"> A policy statement should exist, that requires each system and/or application to detect the existence of invalid identification codes, in conjunction with the use of other settings, such as: <ul style="list-style-type: none"> > Limit on unsuccessful attempts > Action to be taken <ul style="list-style-type: none"> ✓ Temporary device lockout ✓ Permanent device lockout > Notification
The existence of a Systems Development – (SDLC) methodology which <i>identifies Preliminary Information Protection Requirements</i> within the <i>Project Definition Phase</i> of a new project	<ul style="list-style-type: none"> Source document: The Application Development Security Guide. Specific reference to the "Security Activities in the System Life-Cycle" matrix within the guide Existing explanation within the <i>Initiation</i> phase details the identification of every system professional and their role related to systems security. 	<ul style="list-style-type: none"> Policy discussions do not exist for the following areas covering: <ul style="list-style-type: none"> > The identification of Preliminary Information Protection Requirements 	<ul style="list-style-type: none"> A simplified policy statement should exist, which requires each system and/or application to: <ul style="list-style-type: none"> > Determine high-level global information access needs > Identify information sensitivity and security concerns
The existence of a Systems Development – (SDLC) methodology which includes a project phase for <i>Business Systems Analysis</i> , which addresses <i>Information Access and Security Approaches</i>	<ul style="list-style-type: none"> Source document: The Application Development Security Guide. Specific reference to the "Security Activities in the System Life-Cycle" matrix within the guide 	<ul style="list-style-type: none"> Policy discussions do not exist for the following area: <ul style="list-style-type: none"> > Business Systems Analysis <p>The "Security Activities in the System Life-Cycle" describes the SDLC migrating from Initiation, Development, Operations and Termination, without the benefit of a <i>Business Systems Analysis</i> phase of a project, which discusses security</p>	<ul style="list-style-type: none"> A policy statement should exist, which includes a Business Systems Analysis Phase, that addresses, for example: <ul style="list-style-type: none"> > Reviews information protection and security requirements > Reviews detailed descriptions of data and processes with respect to: <ul style="list-style-type: none"> ✓ Information criticality ✓ Information sensitivity ✓ Identify information protection and security criteria for User Acceptance Testing – (UAT) ✓ Define the technical security architecture and design for the hardware, software database, network and telecommunications

NEW SYSTEMS SECURITY DEVELOPMENT POLICY

Tab C

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of a Systems Development-(SDLC) methodology which includes a project phase for <i>Detailed Systems Design</i> as it relates to information security</p>	<ul style="list-style-type: none"> • The existing explanation within the <i>Development Phase</i> of the matrix provides responsibilities relating to security for each person involved in the systems development process 	<ul style="list-style-type: none"> • Policy discussions do not exist for the following area: <ul style="list-style-type: none"> > Detailed System Design <p>The "Security Activities in the System Life-Cycle" describes the SDLC migrating from Initiation, Development, Operations and Termination, without the benefit of a Detailed Systems Design phase of a project, which discusses security</p>	<ul style="list-style-type: none"> • A policy statement should exist, that includes a Detailed System Design Phase, which: <ul style="list-style-type: none"> > Refines data access architecture > Procedures for information access and security > Procedures for training for support staff, users, System and Security Administrators and Help Desk personnel

MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS – (NIST 800-18/OMB A-130 Compliance Review)

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of an application security plan which complies with NIST 800-18/OMB A-130 guidelines, which addresses the primary elements covering:</p> <ul style="list-style-type: none"> • System Identification • Management Controls 	<p>Sources:</p> <ul style="list-style-type: none"> • Security Plans Reviewed included CASE Administration System (CAS) Application Security Plan, Integrated Present Value of Future Benefits (IPVFB) & Genesis Production Instance • Security Plans in Need of Development include: <ul style="list-style-type: none"> > Trust Accounting > CASR-R > Performance Accounting > IPS > LMS > ACT 1.0 > MPP > FRS > MES <p>No issues noted within the System Identification.</p> <p>A security plan for the CASE Administration (CAS) Application exists, which includes:</p> <ul style="list-style-type: none"> • CASE Security Policy and Objectives • Security Responsibilities <ul style="list-style-type: none"> > Security Planning > Risk Management > System Administration <ul style="list-style-type: none"> ✓ Password and User ID Guidelines ✓ Personnel Surety Program Guidelines > Critical Positions > Contingency Planning • Security Implementation Approach <ul style="list-style-type: none"> > Application Environment > Client Workstation Environment > Network Environment > Database Environment 	<p>The CASE Administration System (CAS) Application Security Plan, IPVFB & Genesis Production Instance are in substantive non-compliance with NIST 800-18 guidelines. The security plans need enhancements to address the following key areas:</p> <ul style="list-style-type: none"> • System Identification <ul style="list-style-type: none"> > General description/Purpose which includes a description of the processing flow of the application, System Environment, System Interconnection/Information Sharing, Applicable laws or regulations affecting the system and a general description of information sensitivity • Management Controls <ul style="list-style-type: none"> A) Address the Risk Assessment and Management process B) Rules of Behavior C) Planning for Security in the Life Cycle 	<p>The policy should include for example:</p> <p>Management Controls:</p> <ul style="list-style-type: none"> • A) Risk Assessment and Management <ul style="list-style-type: none"> > Threats & vulnerabilities > Projected system risk assessment (No frequency date specifically noted within the security plan) • Review of security controls over the past 3 years: (Performed by purpose, date & findings) • B) Rules of Behavior <ul style="list-style-type: none"> > Made available to every user prior to receiving access to system > Identified consequence of inconsistent behavior or non-compliance > Limits on interconnections to other systems • C) Planning for Security in the Life Cycle (e.g. Initiation, Development/Acquisition, Implementation, Operation/Maintenance and disposal)

MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS – (NIST 800-18/OMB A-130 Compliance Review)

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
	<ul style="list-style-type: none"> • Configuration Management Policy 		<p>phases:</p> <ul style="list-style-type: none"> > Initiation Phase <ul style="list-style-type: none"> ✓ Completion of a sensitivity assessment > Development/Acquisition Phase <ul style="list-style-type: none"> ✓ Security requirements identified > Security controls were evaluated & Test procedures developed prior to the purchase <ul style="list-style-type: none"> ✓ RFP included security requirements & evaluation/test procedures ✓ Security requirements allows for updating new threats/vulnerabilities ✓ Security requirements identified & included in the acquisition specifications > Implementation Phase <ul style="list-style-type: none"> ✓ Design reviews and systems test were completed, documented & certification prior to placing the system in production ✓ Security controls have been added since development ✓ The application has received a technical evaluation to ensure that it meets federal laws, Regulations, policies, guidelines and standards ✓ Projected date for certification & accreditation > Operation/Maintenance Phase <ul style="list-style-type: none"> ✓ Security related activities should be identified > Disposal Phase <ul style="list-style-type: none"> ✓ A description of how data is moved to another system ✓ Encryption of sensitive data ✓ Process for clearing & purging data
<p>The existence of an application security plan which complies with NIST 800-18/OMB A-130 guidelines, which addresses the primary elements covering <i>Operational Controls</i></p>	<ul style="list-style-type: none"> • There is no operational section within the CAS application security plan 	<ul style="list-style-type: none"> • The security plan needs enhancements to address the following key areas for <i>Operational Controls</i>, which includes: <ul style="list-style-type: none"> > Personnel Security > Physical and Environmental 	<ul style="list-style-type: none"> • The policy should include, for example <i>Operational Controls</i>: <ul style="list-style-type: none"> > Personnel Security <ul style="list-style-type: none"> ✓ Positions evaluated for sensitivity level

**MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS –
(NIST 800-18/OMB A-130 Compliance Review)**

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
		<p>Protection</p> <ul style="list-style-type: none"> ➤ Production, Input/Output Controls ➤ Contingency Planning ➤ Application Software & hardware maintenance controls ➤ Data Integrity/Validation Controls ➤ Documentation ➤ Security Awareness and Training ➤ Incident Response Capability 	<ul style="list-style-type: none"> ✓ Background screenings ✓ User Access levels identified ✓ Process for requesting, establishing, issuing, and closing user accounts ✓ Separation of duties User accountability for actions ✓ Termination procedures <ul style="list-style-type: none"> • Physical and Environmental Protection <ul style="list-style-type: none"> ➤ Locks on terminals, physical barriers ➤ Around the bldg ➤ Physical access, fire safety, failure of supporting utilities, structural collapse, interception of data and mobile and portable systems, etc. • Production, Input/Output Controls <ul style="list-style-type: none"> ➤ User Support (e.g. help desk) ➤ Procedures to ensure that only authorized users pick up, receive, or deliver input and output information and media ➤ Audit trails for receipt of sensitive inputs/outputs ➤ Procedures for restricting access to Output ➤ Procedures & controls for transporting or mailing media or printed output ➤ Internal/external labeling for sensitivity (e.g. Privacy Act, Proprietary) ➤ External labeling with special handling instructions (e.g. log/inventory ID, etc.) ➤ Audit trails for inventory management ➤ Media storage vault or library-physical, environmental protection ➤ Controls/procedures ➤ Procedures for sanitizing electronic media for reuse ➤ Procedures for controlling storage, handling, or destruction of spoiled

**MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS –
(NIST 800-18/OMB A-130 Compliance Review)**

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
--------------------	---------------------	------	-----------------------------

			<p>media or media that cannot be effectively sanitized for reuse</p> <ul style="list-style-type: none"> ➤ Procedures for shredding or other destructive measures for hardcopy media when no longer required <ul style="list-style-type: none"> • Contingency Planning <ul style="list-style-type: none"> ➤ Agreements of backup processing ➤ Documented backup procedures including frequency and scope ➤ Location of stored backups and generations of backups ➤ Tested contingency/disaster recovery plans in place ➤ Employees trained in their roles and responsibilities ➤ Coverage of backup procedures • Application Software & hardware maintenance controls <ul style="list-style-type: none"> ➤ Policies against illegal use of copyright software, shareware? ➤ Periodic audits conducted of users computers to ensure only legal licensed copies of software are installed? ➤ Products and procedures used to protect against illegal use of software ➤ Existence of software warranties ➤ Restriction/controls on those who perform maintenance and repair activities. ➤ Special procedures for performance of emergency repair and maintenance. ➤ Procedures used for items serviced through on-site maintenance (e.g. escort of maintenance personnel, sanitation of devices removed from the site). ➤ Procedures used for controlling remote maintenance services where diagnostics procedures or
--	--	--	--

**MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS –
(NIST 800-18/OMB A-130 Compliance Review)**

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
--------------------	---------------------	------	-----------------------------

			<p>maintenance is performed through telecommunications arrangements</p> <ul style="list-style-type: none"> ➤ Version control that allows association of system components to the appropriate system ➤ Procedures for version control that allows association of system components to the appropriate system version ➤ Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production ➤ Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software ➤ Change identification, approval, and documentation procedures ➤ Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes ➤ Are test data "live" ➤ Are test data "made-up" data ➤ Are there organizational policies against illegal use of copyrighted software or shareware <ul style="list-style-type: none"> • Data Integrity/Validation Controls <ul style="list-style-type: none"> ➤ Is virus detection and elimination software installed ➤ Are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting ➤ Is reconciliation routines used by the system, (i.e., checksums, has totals, record counts?
--	--	--	--

**MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS –
(NIST 800-18/OMB A-130 Compliance Review)**

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<ul style="list-style-type: none"> ➤ Are password crackers/checkers used? ➤ Is integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? ➤ Are intrusion detection tools installed on the system? ➤ Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, attacks, system and network slowdowns and crashes ➤ Penetration testing performed on the system? ➤ Are procedures in place to ensure they are conducted appropriately? ➤ Are message authentication used in the system to ensure that the sender of a message is known and that the message has not been altered during transmission? • Documentation <ul style="list-style-type: none"> ➤ Vendor documentation maintained for the application • Security Awareness and Training <ul style="list-style-type: none"> ➤ The awareness program for the system or application ➤ The type & frequency of application-specific and general support system training is provided to employees and contractor personnel (e.g. seminars, workshops, etc.) ➤ Describe the procedures for assuring that employees and contractor personnel have been provided adequate training • Incident Response Capability <ul style="list-style-type: none"> ➤ Are there procedures for reporting incidents handled either by system

MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS – (NIST 800-18/OMB A-130 Compliance Review)

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of an application security plan which complies with NIST 800-18/OMB A-130 guidelines, which addresses the primary elements covering <i>Technical Controls</i>.</p>	<p>There is no operational section within the CAS application security plan.</p>	<p>The security plan needs enhancements to address the following key areas for <i>Technical Controls</i>, which includes:</p> <ul style="list-style-type: none"> • Identification & Authentication • Logical access controls • Public Access Controls 	<p>personnel or Externally?</p> <ul style="list-style-type: none"> ➤ Are there procedures for recognizing and handling incidents, e.g., what files and logs should be kept, who to contact, and when? ➤ Who receives and responds to alerts/advisories, (e.g., vendor patches, etc.) ➤ Exploited vulnerabilities? ➤ What preventative measures are in place, i.e., intrusion detection tools, Automated audit logs, penetration testing? <p>The policy should include for example:</p> <ul style="list-style-type: none"> • Identification & authentication <ul style="list-style-type: none"> ➤ Authentication control mechanisms ➤ Method of user authentication (password, token, and biometrics) ➤ Password length (min & max) ➤ Allowable character set ➤ Password aging time frames and enforcement approach ➤ Number of generations of expired passwords disallowed for use ➤ Password changes ➤ Password compromise ➤ Frequency of password changes ➤ Access control mechanism ➤ User authentication mechanism ➤ Invalid access attempts ➤ Changing of system-provided administrative default passwords ➤ Limits on access scripts with embedded passwords ➤ Controls in place governing user bypassing authentication requirements (e.g. single sign-on) ➤ Use of digital or electronic signatures and standards used • Logical access controls <ul style="list-style-type: none"> ➤ Hardware & Software features

MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS – (NIST 800-18/OMB A-130 Compliance Review)

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<p>designed to permit only authorized access to or within the application</p> <ul style="list-style-type: none"> > Process used for granting access rights (e.g. job function) > ACL or register capability > Restrictions on O/S use > Controls to detect unauthorized transaction attempts > System timeout feature based on inactivity. Encryption used to prevent access to sensitive files > Are warning banners used & if so, who provides the authorization (e.g. DOJ Computer Crime and Intellectual Properties Section, etc.) <ul style="list-style-type: none"> • Public Access Controls <ul style="list-style-type: none"> > Process used for identification and authentication > Access control to limit what the user can read, write, modify, or delete > Controls to prevent public users from modifying information on the system > Digital signatures > CD-ROM for on-line storage of information for distribution > Public access on a separate system > Prohibit public to access live databases > Verify that programs and information distributed to the public are virus-free > Audit trails and user confidentiality > System and data availability > Legal considerations <ul style="list-style-type: none"> > Audit trail supports accountability > Audit trails assist in intrusion detection > Audit trail includes sufficient information to establish what events occurred and who (or what) caused them > Access to online audit logs are strictly enforced > Confidentiality of audit trail information

**MAJOR APPLICATION/GENERAL SUPPORT SYSTEM SECURITY PLANS –
(NIST 800-18/OMB A-130 Compliance Review)**

Tab D

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			is protected: > Frequency of use of audit trails & guidelines > System level or application level administrator review of audit trails for known user violations

INTERNET/INTRANET SECURITY POLICY

Tab E

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of a Internet/Intranet Security Policy</p>	<ul style="list-style-type: none"> • Source: N/A • There is currently no Internet/Intranet Security Policy. 	<ul style="list-style-type: none"> • A policy should be developed which discusses at the minimum the following criteria: <ul style="list-style-type: none"> ➢ Password Management ➢ Authentication ➢ Data Privacy, encryption and integrity ➢ Software Import Control ➢ Remote Access ➢ Incident Response ➢ Appropriate use of the Internet ➢ Firewall Security ➢ E-mail 	<ul style="list-style-type: none"> • There is a need to develop new standards to address the Gaps noted
<p>The existence of an Internet/Intranet Security Policy which addresses Password Management</p>	<ul style="list-style-type: none"> • Same 	<ul style="list-style-type: none"> • There is no policy statement governing password management. 	<ul style="list-style-type: none"> • The policy should include Password Management criteria, which should include requirements, such as: <ul style="list-style-type: none"> ➢ Minimum of 6 – 8 characters (no common names) ➢ Passwords are kept private ➢ Frequency of password changes (e.g. 90 days) ➢ Unsuccessful attempts (e.g. 3 failed logon attempts) ➢ Time-out restrictions (e.g. 10 mins) ➢ Logons should display the date and time of the last logon and logoff ➢ Logon Ids and passwords should be suspended after a specified period of disuse ➢ After excessive violations, the system should generate an alarm and continue to allow the user to simulate a continuing session (with dummy data, etc.), while personnel investigate the incoming connection
<p>The existence of an Internet/Intranet Security Policy which addresses Authentication</p>	<ul style="list-style-type: none"> • Source: N/A • There is currently no Internet/Intranet Security Policy. 	<ul style="list-style-type: none"> • There is no policy statement governing Authentication 	<ul style="list-style-type: none"> • The policy should include Authentication criteria, which should include requirements, such as: <ul style="list-style-type: none"> ➢ Dynamic password generators ➢ Cryptography-based challenge/response tokens and software ➢ Digital signatures and certificates ➢ User training on the use of the safe handling and storage of all

INTERNET/INTRANET SECURITY POLICY

Tab E

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of an Internet/Intranet Security Policy which addresses <i>Data Privacy, encryption and integrity</i></p>	<ul style="list-style-type: none"> • Source: N/A • There is currently no Internet/Intranet Security Policy 	<ul style="list-style-type: none"> • There is no policy statement governing Data Privacy, encryption and integrity 	<p>authentication devices</p> <ul style="list-style-type: none"> > Certificate Authorities > Password protection for certificates that are stored on PCs <ul style="list-style-type: none"> • The policy should include Data Privacy, encryption and integrity criteria, which at the minimum should address: <ul style="list-style-type: none"> > Encryption. (Policy should mandate the use of algorithms that have been in use commercially long enough to provide some assurance of security. Encryption using keys of 40 or fewer bits is only acceptable for use behind the firewall. Cryptographers recommend businesses use key lengths of at least 75 bits, with 90 bits being preferable. DES uses 56 bit keys and preferable triple DES of 112 bits).
<p>The existence of an Internet/Intranet Security Policy which addresses <i>Software Import Control</i></p>	<ul style="list-style-type: none"> • Source: N/A • There is currently no Internet/Intranet Security Policy 	<ul style="list-style-type: none"> • There is no policy statement governing <i>Software Import Control</i> 	<ul style="list-style-type: none"> • The policy should include Data Privacy, encryption and integrity criteria, which at the minimum should address: <ul style="list-style-type: none"> > Controls over the use of Java & Active X > Software Licensing risks and controls > Threat types (e.g. executable program, macro, applet, violation of licensing agreement, disclosure of information, masquerade or spoofing, unauthorized access, loss of integrity, denial of service and theft of service and resources) > Virus prevention, detection, and removal > Maintaining Back-ups of data with off-site storage > Obtain software only through approved channels > Running a virus scanner once a day every day, when you first turn on your computer > Running a virus scanner on every diskette that has come from a computer other than your own > Always use the write-protect tab to

INTERNET/INTRANET SECURITY POLICY

Tab E

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of an Internet/Intranet Security Policy which addresses <i>Remote Access</i></p>	<ul style="list-style-type: none"> • Source: N/A • There is currently no Internet/Intranet Security Policy 	<ul style="list-style-type: none"> • There is no policy statement governing <i>Remote Access</i> 	<p>protect your diskettes</p> <ul style="list-style-type: none"> > Segregate executable files into directories where users cannot modify them. <ul style="list-style-type: none"> • The policy should include Remote Access Policy controls and restrictions, which at the minimum should address, for example: <ul style="list-style-type: none"> > All remote access to PBGC's computer systems, whether via dial-up or Internet access must use encryption services to protect the confidentiality of the session. > All users who access the company system through dial-in connections periodically change their passwords. For high-risk systems, all users who access the company system through dial-in connections must use one-time passwords, with approval from the Network Services Manager and the Information Security Manager. The use of desktop modems to support dial-in access to company systems is prohibited. > Direct dial-in connections to company production systems must be approved by the Network Services Manager
<p>The existence of an Internet/Intranet Security Policy which addresses <i>Incident Response</i></p>	<ul style="list-style-type: none"> • Same 	<ul style="list-style-type: none"> • F) There is no policy statement governing <i>Incident Response</i> 	<ul style="list-style-type: none"> • The policy should include Incident Response controls, such as: <ul style="list-style-type: none"> > O/S and application software logging processes shall be enabled on all host and server systems > Alarm and alert functions, as well as logging, of any firewalls and other network perimeter access control systems shall be enabled > Administration System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis > Users are trained to report any anomalies in system performance to

INTERNET/INTRANET SECURITY POLICY

Tab E

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<p>their system administration staff, as well as relevant network or information systems security staff</p> <ul style="list-style-type: none"> > All trouble reports received by system administration personnel should be reviewed for symptoms that might indicate intrusive activity > Suspicious symptoms should be reported to Network or Information Systems security personnel > Host based intrusion tools such as tripwire will be checked on a routine basis > Security personnel should establish relationships with other incident response organizations, such as other IRCs within the agency or FIRST (See www.first.org) and share relevant threats, vulnerabilities, or incidents > Unless critical systems have been compromised, the origination will first make an attempt to track intruders before correcting systems > All critical servers shall have redundant intrusion detection tools installed, which operate on a different principle from the primary tool that is installed on all servers > At logical network concentration points, intrusion detection tools will be installed which monitor for traffic patterns consistent with known attacks > System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis > Audit logs from the perimeter access control systems shall be reviewed daily > Audit logs for servers and hosts on the internal protected network shall be reviewed on a daily basis > Audit logs for servers and hosts on the internal protected network shall

INTERNET/INTRANET SECURITY POLICY

Tab E

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<ul style="list-style-type: none"> ➢ be reviewed on a daily basis ➢ User education provided in order to train end users of computing systems to report any anomalies in system performance to their system administration staff, as well as relevant network or information systems security staff.
<p>The existence of an Internet/Intranet Security Policy which addresses the appropriate use of the Internet</p>	<ul style="list-style-type: none"> • Same 	<ul style="list-style-type: none"> • There is no policy statement governing the appropriate use of the Internet 	<ul style="list-style-type: none"> • The policy should include the appropriate use of the Internet, which at the minimum addresses: <ul style="list-style-type: none"> ➢ Employees may not use the Internet for personal commercial purposes ➢ No access to obscene or pornographic sites ➢ Restricted from accessing or using information that would be considered harassing. ➢ Actions for non compliance (e.g. verbal reprimands vs termination or legal prosecution) ➢ Users posting to Usenet newsgroups, Internet mailing lists, etc. must include a company disclaimer as part of each message
<p>The existence of an Internet/Intranet Security Policy which addresses Firewall Security</p>	<ul style="list-style-type: none"> • Same 	<ul style="list-style-type: none"> • There is no policy statement governing the Firewall Security 	<ul style="list-style-type: none"> • The policy should include Firewall Security, which at the minimum addresses: <ul style="list-style-type: none"> ➢ Background and Purpose ➢ Authentication ➢ Firewall functioning as either a router or a forwarder of Internet packets ➢ Firewalls used (e.g. Packet Filtering vs Application Gateways) ➢ Firewall Architectures ➢ Creation of an Intranet (firewall used to create a subnet of the network) ➢ Firewall Administration ➢ Physical Firewall Security ➢ Firewall Incident Handling ➢ Restoration of Services ➢ Upgrading the firewall ➢ Revision/Update of Firewall Policy ➢ Logs and Audit Trails

INTERNET/INTRANET SECURITY POLICY

Tab E

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of an Internet/Intranet Security Policy which addresses <i>E-Mail Security</i></p>	<ul style="list-style-type: none"> • Source: N/A • There is currently no Internet/Intranet Security Policy 	<ul style="list-style-type: none"> • There is no policy statement governing <i>E-Mail Security</i> 	<ul style="list-style-type: none"> • The policy should include Firewall Security, for example: <ul style="list-style-type: none"> ➤ Use of electronic mail services for purposes constituting clear conflict of corporation interests are in violation of company information security policies is expressly prohibited, as is excessive personal use of email ➤ Use of corporation email to participate in chain letters or moonlighting is not acceptable ➤ The corporation provides electronic mail to employees for business purposes. Limited personal use may be acceptable as long as it doesn't impact the operations ➤ The use of email in any way to facilitate the conduct of a private commercial purposes is forbidden ➤ If the corporation provides access to electronic mail to external users such as consultants, temporary employees, or partners, they must read and sign the email policy statement ➤ The contents of email messages will be considered confidential, except in the case of criminal investigations ➤ Electronic mail is provided by the PBGC for employees to conduct PBGC business. The use of email for personal business is not allowed ➤ Confidential or company proprietary information will not be sent by email ➤ Only authorized email software may be used ➤ Anonymous retailer software, downloadable via e-mail cannot be installed ➤ Employees may not use anonymous retailers for any purpose ➤ Consequences of employee non-compliance with policy standards

WINDOWS NT SECURITY PLAN

Tab F

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of a Windows NT Security Plan which provides <i>high-level</i> guidance on this <i>General Support System</i>, which addresses NIST SP 800-18 & OMB requirements, which cover:</p> <ul style="list-style-type: none"> • System Identification • Management Controls • Operational Controls • Technical Controls 	<p>Source: There is currently no Windows NT plan</p>	<p>The lack of a entity-wide Windows NT security plan, which addresses <i>System Identification</i> information</p>	<p>The security plan should address the same key components previously identified during the review of NIST 800-18 compliance for Major applications (e.g. CASE Administration System)</p> <p>A few specifics that could be discussed within the <i>System Identification</i> section of the plan may include a more detailed discussion on:</p> <ul style="list-style-type: none"> • Design of the local network – (e.g. PDC's/BDC's, general architecture of the domains, single domain, single master domain, multiple master domain, trusts, etc.) <p>A few topics to introduce within the <i>NT Security Standards</i> may include a brief high-level discussion on <i>Technical Controls</i>, which may include:</p> <ul style="list-style-type: none"> • User Set-up and Administration • Account & System Policies • Auditing Policy • Protection of Files and Directories • Remote Access Service • Monitoring and updating security and responding to incidents • User Rights, Responsibilities and Practices • System Services

WINDOWS NT SECURITY STANDARDS

Tab.G

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of a Windows NT Security Standards which provides technical controls over NT security for User Set-Up and Administration Controls</p>	<p>Source: There is currently no Windows NT Standards</p>	<p>There are no NT Security Standards covering User Set-Up and Administration controls</p>	<p>The NT Security Standards should address <i>User Set-up and Administration</i>, for example:</p> <ul style="list-style-type: none"> • Criteria for establishing <i>Global groups</i> having global access to the entire domain vs <i>Local Groups</i> having access only to their local PC workstation • Criteria for evaluating the adequacy and reasonableness of granted privileges for all NT default groups (e.g. Account Operations, Domain Administrators & Guests, Users, etc.)
<p>The existence of a Windows NT Security Standards which provides technical controls over NT Account & System Policies</p>	<p>There are no NT Security Standards covering NT Account & System Policies</p>	<p>There are no NT Security Standards covering NT Account & System Policies</p>	<p>The NT Security Standards should address <i>NT Account & System Policies</i>, for example:</p> <p>Account Policy:</p> <ul style="list-style-type: none"> • Maximum Password Age • Minimum Password Age • Minimum Password Length • Password Uniqueness <p>System Policy:</p> <p>Evaluating the appropriateness of default user policies for non-administrative users:</p> <ul style="list-style-type: none"> • Restricting "Display" Control Panel • Removing the Run Command • Disabling ShutDown Command • Disabling Registry editing tools • Controls over Windows NT Remote Access (e.g. max number of authentication retries, max time limit for authentication & Auto Disconnect)
<p>The existence of a Windows NT Security Standards which provides technical controls over NT Auditing Policies</p>	<p>There are no NT Security Standards covering NT Account & System Policies</p>	<p>There are no NT Security Standards covering NT Auditing Policies</p>	<p>The NT Security Standards should address the <i>NT Auditing Policy</i>, for example:</p> <ul style="list-style-type: none"> • Criteria for security logging of user success & failure activity covering:

WINDOWS NT SECURITY STANDARDS

Tab G

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<ul style="list-style-type: none"> > Logon and Logoff > File and Object Access > Use of User Rights > User and Group Management > Security Policy Changes > Restart, Shutdown, and System > Process Tracking
<p>The existence of a Windows NT Security Standards covering Remote Access Service</p>	<p>There are no NT Security Standards covering NT Account & System Policies</p>	<p>There are no NT Security Standards covering Remote Access Service</p>	<p>The NT Security Standards should address <i>Remote Access Service</i> for example:</p> <ul style="list-style-type: none"> • The existence of "Microsoft encrypted authentication" on the RAS server and all clients. This assures that unencrypted passwords never pass over the communication media • The use of data encryption • Granting of remote access capabilities only to those users who require it • User password complexity
<p>The existence of a Windows NT Security Standards covering Monitoring and updating security and responding to incidents</p>	<p>There are no NT Security Standards covering NT Account & System Policies</p>	<p>There are no NT Security Standards covering Monitoring and updating security and responding to incidents</p>	<p>The NT Security Standards should address Monitoring and updating security and responding to incidents, for example:</p> <p>Security Monitoring:</p> <ul style="list-style-type: none"> • Regularly Monitoring and updating domain, group, user and file security status, which may include: <ul style="list-style-type: none"> > Removing user permissions immediately upon termination of employment > Set contractor accounts to expire periodically > Establish a regular (no less often than monthly) monitoring program to review security policies, and permissions to review changes in ownership, group memberships, access permissions, file permissions, rights and abilities, trust relationships among domains and unknown or unneeded services > Disabling idle user accounts which have not been used for a period of

WINDOWS NT SECURITY STANDARDS

Tab G

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			time: Responding to incidents: <ul style="list-style-type: none"> • Establishing procedures and call lists for responding to incidents • Security Standards developed which include creating, documenting and testing a recovery procedure
The existence of a Windows NT Security Standards covering User Rights, Responsibilities and Practices	There are no NT Security Standards covering NT Account & System Policies	There are no NT Security Standards covering User Rights, Responsibilities and Practices	The NT Security Standards should address <i>User Rights, Responsibilities and Practices</i> , which include the consideration of assigning the following user rights, which are generally the default rights within NT, for example: <ul style="list-style-type: none"> • Log on locally and the ability to access the computer from the network • Backup files and directories and the ability to restore files and directories • Taking ownership of files and directories from another user's objects (e.g. files, directories, and Registry keys) • The ability to Debug Programs being run by another user • By default users have Bypass traverse checking
The existence of a Windows NT Security Standards covering System Services	There are no NT Security Standards covering NT Account & System Policies	There are no NT Security Standards covering System Services	The NT Security Standards should address <i>System Services</i> , for example: <ul style="list-style-type: none"> • Strictly limiting the services that run on a given computer. Many services are installed into the System account and can subvert security • Consider separating the ways that services can interact with one another and consider running each service under a unique account to protect directories or Registry keys from use by other services • Consider running a port scanner to help detect unknown services

UNIX SECURITY PLAN

Tab H

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of a UNIX Security Plan which provides <i>high-level</i> guidance on this <i>General Support System</i>, which addresses NIST SP 800-18 & OMB requirements, which cover:</p> <ul style="list-style-type: none"> • System Identification • Management Controls • Operational Controls • Technical Controls 	<p>Source: There is currently no UNIX Security Plan.</p>	<p>The lack of a entity-wide Windows UNIX security plan, which addresses <i>System Identification</i> information</p>	<p>The security plan should address the same key components previously identified during the review of NIST 800-18 compliance for <i>General Support Systems</i> (e.g. Windows NT)</p> <p>The security plan should include a <i>high-level</i> discussion on the following areas for <i>System Identification</i>:</p> <ul style="list-style-type: none"> • Management's responsibility • Assignment of Security Responsibility • General Description/Purpose • Applications which operate under this operating system • System Interconnection/Information Sharing • Applicable laws or regulations affecting the system • Roles and Responsibilities of the User • System Administrator • Network Administrator • User Awareness & Training • System and Security Administrators Awareness & Training <p>A few topics to introduce within the <i>UNIX Security Standards</i> may include a more detailed discussion on <i>Technical Controls</i>, which may include:</p> <ul style="list-style-type: none"> • Basic UNIX Security Procedures • Accounts Administration of Users and Groups (e.g. Root Account) • Password Management • Directory/File System Access and Security • Audit & Monitoring

UNIX SECURITY STANDARDS

Tab I

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
The existence of UNIX Security Standards which provides <i>technical controls</i> over <i>Basic UNIX Security Procedures</i>	Source: There is currently no UNIX Standards The closest document that speaks to UNIX standards is contained within the <i>Network Security Enhancement Technical Report</i> , within the <i>UNIX Security Configuration Best Practices Checklist</i>	There are no <i>Basic UNIX Security Standards</i>	The UNIX Security Standards should address, for example: <ul style="list-style-type: none"> • The process for ensuring that security upgrades are applied • The criteria for determining what UNIX services are essential and the process for disabling and/or removing them from the server
The existence of UNIX Security Standards which provides <i>technical controls</i> over <i>Accounts Administration of Users and Groups (e.g. Root Account)</i>	Same	There are no policy guidelines for <i>Accounts Administration of Users and Groups</i>	The standards for <i>Accounts Administration of Users and Groups</i> should address, for example: <ul style="list-style-type: none"> • Specific guidelines over user accounts (e.g. Each user must have a personal account with a unique login name, user identification UID code and password) • Specific guidelines over Account Administration (e.g. Guest Account, reuse of UID's, etc.) • Generic User account Removal & the recertification process for the existence and appropriateness of those user accounts • Controls over the root account • User Home directories • User Environment files • Group membership • Admin Groups • Non-system Group ID (GID) segregation
The existence of UNIX Security Standards which provides <i>technical controls</i> over <i>Password Management</i>	Same	There are no specific policy guidelines for <i>Password Management</i>	Specific <i>Password Management Standards</i> should address, for example: <ul style="list-style-type: none"> • Minimum length • Composition • Aging • Vendor supplied default passwords change requirements • Prohibition on the storage of Passwords in command files or shell scripts • Controls over Brute Force attacks

UNIX SECURITY STANDARDS

Tab. I

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of UNIX Security Standards which provides <i>technical controls over Directory/File System Access and Security</i></p>	<p>Same</p>	<p>There are no specific policy guidelines for <i>Directory/File System Access and Security</i></p>	<ul style="list-style-type: none"> • The Shadow Password File Protection <p>Specific Directory/File System Access and Security standards, should address, for example:</p> <ul style="list-style-type: none"> • System directories and files (e.g. criteria used for restrictions) • Controls over start-up & Kernel files • Controls over File Structure and permissions • Controls over Network Files
<p>The existence of UNIX Security Standards which provides <i>technical controls over Audit & Monitoring</i></p>	<p>Same</p>	<p>There are no specific policy guidelines for <i>Audit & Monitoring</i></p>	<p>Specific Audit & Monitoring standards, should address, for example:</p> <ul style="list-style-type: none"> • Random checks on: <ul style="list-style-type: none"> > Unexpected users logged on to the system > Users from unexpected hosts logged on > Users logged on at expected times > Normal system processes that are not running > Unexpected system processes that are running • Daily Activities <ul style="list-style-type: none"> > Login failures > Logins from unknown hosts > Failed access to system files > Inappropriate access permissions to system files > Heavy system activity by a user after hours > Unexpected mounted files systems > Unexpected hosts and netrc files > Unexpected SUID/SGID orphan or disguised files > Successful and unsuccessful su to root > Unexpected changes in permissions or ownerships

ORACLE SECURITY PLAN

Tab J

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of a Standard Oracle Security Plan which provides <i>high-level</i> guidance on this <i>General Support System</i>, which addresses NIST SP 800-18 & OMB requirements, which cover:</p>	<p>Source: There is currently no Standardized Oracle Security Plan</p> <p>Documents within PBGC which address Oracle include:</p> <ul style="list-style-type: none"> • PRISM DB Security Requirements – (PBGC Oracle Role Standards, Oracle Server Auditability/Security & Querying Oracle for Security Data) • Genesis Production Instance Security Document – (Oracle Database Schema Owner and Contents & Password protected roles) • Consolidated Maintenance Team – (Standards for Application Security) – (Application/Oracle Password Policies & Application specific Oracle Roles) • Network Security Enhancement Technical Report – (Oracle database security configuration white paper) • Security Test and Evaluation (ST&E) Report of Premium Accounting System (PAS) – (Oracle Violations, Audit Trail, View_Audit_Trail_Threshold_Lock_Out, Password_Min_Length & Sec_Change_Audit) 	<p>The lack of a entity-wide Windows NT security plan, which addresses System Identification, Management, Operational & Technical Controls.*</p> <p>The content of the discussion on Oracle Security Standards is not discussed with consistency and is fragmented amongst several documents, as detailed within the current PBGC column of this matrix</p> <p>* For details, refer to the "Major Application/General Support System Security Plan – (NIST 800-18/OMB A-130 Compliance Review)" contained within this document</p>	<p>The security plan should address the same key components previously identified during the review of NIST 800-18 compliance for <i>General Support Systems</i> (e.g. Windows NT)</p> <p style="text-align: center;">Additional Oracle Security Plan Enhancements</p> <p>The <i>Management Controls</i> section of this plan should include a high-level discussion on the following topics:</p> <ul style="list-style-type: none"> • General Oracle Database Standards, which identifies the roles & responsibilities of: <ul style="list-style-type: none"> ➢ The Primary Database Administrator(s) – (DBA) ➢ Backup DBA(s) ➢ Primary System Administrator(s) ➢ Backup System Administrator(s) • Level of authority for: <ul style="list-style-type: none"> ➢ Approving accounts ➢ Approval for creating, deleting and managing accounts ➢ Process for determining how account approval will be performed: email, web site, hard-copy form, etc. ➢ Determination of what constitutes a security breach and the appropriate penalty for each breach ➢ Approval for establishing views and roles

ORACLE SECURITY STANDARDS

Tab K

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
<p>The existence of ORACLE Security Standards which provides basic <i>technical controls</i> over this database</p>	<p>Documents within PBGC which address Oracle are noted within the Oracle Security Plan section of this document</p>	<p>There are no uniform standards that govern <i>Basic ORACLE Security</i>. The ORACLE Security Standards are fragmented amongst several technical documents (PRISM DB Security Requirements, Genesis Production Instance Security Document, Consolidated Maintenance Team - (Standards for Application Security), Network Security Enhancement Technical Report & Security Test and Evaluation (ST&E) Report of Premium Accounting System (PAS))</p>	<p>Additional Oracle Security Plan Enhancements</p> <p>The <i>technical controls</i> section of the Oracle Security Standards should include a discussion on the risks and controls, for example:</p> <ul style="list-style-type: none"> • User Identification & Integrity • Profiles • Roles • System Privileges • Object-Level Privileges • System & Object Auditing responsibilities <p>User Identification & Integrity</p> <ul style="list-style-type: none"> • Controls over unauthorized server environment access • The potential need for supplemental password administration software and/or procedures. • Required change of the initial password for new Oracle database installations <p>A process in place which verifies that all accounts have passwords assigned</p> <p>A process in place which verifies that user accounts do not use easily guessed passwords (e.g. Test, PBGC & Oracle)</p> <p>A process in place to ensure that passwords are not the same as the user account name</p> <p>A process in place, which identifies all users defined in the database. Security standards should require the verification that each account has a documented access request on file, and that each account is currently active. Additionally, security standards should also verify the adequacy of controls in place to ensure</p>

ORACLE SECURITY STANDARDS

Tab K

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<p>that inactive or terminated employee accounts are removed from the database</p> <p>Profiles</p> <ul style="list-style-type: none"> • A process in place to investigate and resolve any parameter settings that appear questionable <p>Roles</p> <ul style="list-style-type: none"> • Requirement for DBA's to periodically review the roles granted to each user account and evaluate the appropriateness of Critical Oracle Privileges (See below for details) • A process in place to ensure the key roles such as (EXP_FULL_DATABASE & others) are restricted to the <i>database administrator's account</i> <p>System Privileges</p> <ul style="list-style-type: none"> • Requirement for DBA's to periodically review the reasonableness of system privileges against the typical profiles listed below: <ul style="list-style-type: none"> > End User – (e.g. Create session) > Auditor – (e.g. create session & select any table) > Security Officer – (e.g. Alter, Audit, Create, Drop & Grant capabilities) > Assessing the reasonableness of privileges for critical tables <p>Object-Level Privileges</p> <ul style="list-style-type: none"> • Requirement for DBA's to review Object-Level Access security, which can augment security privileges at the role level • Requirement for DBA's to review the table level access privileges for reasonableness. Ensure that the GRANTABLE parameter is NO to

ORACLE SECURITY STANDARDS

Tab K

Industry Practices	Current PBGC Policy	Gaps	Suggested Corrective Action
			<p>prohibit users from passing their access privileges to others</p> <p>System & Object Auditing responsibilities</p> <ul style="list-style-type: none"> • Ensuring the Oracle security standards assign the responsibility for System & Object Auditing that is consistent with the business environment • The level of <i>System auditing</i> should also be evaluated for appropriateness through the Data Dictionary view • The level of <i>object auditing</i> in place should be evaluated for appropriateness through the Data Dictionary view • The Oracle Security standards should assign responsibility for ensuring the reviewing the DBA_AUDIT_TRAIL is reviewed on a regular basis