governmentattic.org
"Rummaging in the government's attic"

Description of document:	Pension Benefit Guaranty Corporation's (PBGC) Directive on Use of Information Technology, 2016 and Volume 19 of the PBGC Information Assurance Handbook, 2008
Requested date:	23-January-2017
Released date:	09-February-2017
Posted date:	22-May-2017
Source of document:	Disclosure Officer Pension Benefit Guaranty Corporation 1200 K Street, N.W., Suite 11101 Washington, D.C. 20005 Fax: (202) 326-4042 Email: disclosure@pbgc.gov

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

PBGC
Protecting America's Pensions
Pension Benefit Guaranty Corporation
1200 K Street, N.W., Washington, D.C. 20005-4026

PBGC 2017-000491

February 9, 2017

Re: Request for Information under the Freedom of Information Act

I am responding to your request received by the Disclosure Division on January 23, 2017. Your request stated that you are requesting "a digital/electronic copy of PBGC Directive IM 05-04, Use of Information Technology. [You] also request a digital/electronic copy of Section 19 of the Information Assurance Handbook." You authorized $25.00 for the production of this request. We processed your request in accordance with the Freedom of Information Act (FOIA) and the Pension Benefit Guaranty Corporation's (PBGC) implementing regulation.

In response to your request, we conducted a search of agency records and located 23 pages of responsive records. The documents are being provided to you electronically to the e-mail address provided in your request. The Disclosure Officer has determined that these documents are fully releasable:

- PBGC Directive IM 05-04, Use of Information Technology (12 pages)
- Section 19, Information Assurance Handbook (11 pages).

Although this is not a denial of your records request, I am providing you with your administrative appeal rights in the event you wish to avail yourself to this process. The FOIA provides at 5 U.S.C. § 552(a)(6)(A)(i) (2014) amended by FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 that if a disclosure request is denied in whole or in part by the Disclosure Officer, the requester may file a written appeal within 90 days from the date of the denial or, if later (in the case of a partial denial), 90 days from the date the requester receives the disclosed material. The PBGC's FOIA regulation provides at 29 C.F.R. § 4901.15 (2015) that the appeal shall state the grounds for appeal and any supporting statements or arguments, and shall be addressed to the General Counsel, Pension Benefit Guaranty Corporation, 1200 K Street, N.W., Washington, D.C. 20005. To expedite processing, the words "FOIA Appeal" should appear on the letter and prominently on the envelope.

In the alternative, you may contact the Disclosure Division's Public Liaison at 202-326-4040 for further assistance and to discuss any aspect of your request. You also have the option to contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

This completes the processing of your request and there were no fees assessed for its processing. You may submit future requests for PBGC records by accessing FOIAonline, our electronic FOIA processing system, at https://foiaonline.regulations.gov, or by email to Disclosure@pbgc.gov.

Sincerely,

Sandra L. Lewandowski
Government Information Specialist

Enclosures

Pension Benefit Guaranty Corporation

PBGC

Protecting America's Pensions

Directive

Subject: Use of Information Technology Resources

Directive Number: IM 05-04

Effective Date: 11-03-2016 **Originator: OIT**

Alice C. Maroni
Chief Management Officer

11/3/2016

1. **PURPOSE:** This Directive establishes the use of PBGC information technology (IT) resources for official business and limited personal use. The personal use privilege is intended to be limited and should not be abused.

2. **EFFECTIVE DATE:** This Directive updates IM 05-04 dated 4/26/2006 and is effective on the date shown above.

3. **SCOPE:** This Directive applies to all PBGC federal employees, contractor employees, visitors, and volunteers conducting business related to or on behalf of PBGC, irrespective of how the federal employees and contractor employees accesses IT resources, whether locally or remotely. Notwithstanding this Directive, PBGC may take emergency action as necessary to protect these resources. Note: If deemed appropriate by PBGC management, any exceptions for union officers and stewards will be set forth in the applicable collective bargaining agreement (CBA) or in a specific agreement between PBGC and the union.

4. **AUTHORITIES:**
   a. 5 U.S. Code § 301, Departmental Regulations
   b. Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2899 (codified as amended in 44 U.S.C. §§ 3541-3549).
   c. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (amending 44 U.S.C. Chapter 35).
   d. Federal Records Act, 44 U.S.C. §§ 2911, 3301
   e. Presidential and Federal Records Act Amendments of 2014, Pub. L. No. 113-187.
   f. Freedom of Information Act, 5 U.S.C. § 522
   g. Privacy Act of 1974, 5 U.S.C. § 552a (2000)
   h. Hatch Act, 5 U.S.C. §§7321-7326

i. Clinger-Cohen Act of 1996, Pub. L. No. 104-106 (Div. D and E)
j. Executive Order 13556 of November 4, 2010; Controlled Unclassified Information
k. Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. Part 2635
l. Office of Management and Budget (OMB) Circular No. A-130, Appendix III, Security of Federal Automated Information Resource
m. OMB Circular A-130, Management of Federal Information Resources, November 28, 2000
n. OMB Memorandum M-04-26, Personal Use Policies and "File Sharing" Technology (2004)
o. PBGC Directive IM 05-2, PBGC Information Security Policy
p. PBGC Directive IM 05-09, Privacy Program
q. PBGC Directive IM 10-03 Protecting Sensitive Information
r. PBGC Directive PM 30-1, Disciplinary and Adverse Actions
s. PBGC Directive PM 30-2, Professional Courtesy and Civility
t. PBGC Directive Records Management Program
u. PBGC Order PM 10-5 Telework Program
v. PM 05-17, Personnel Security and Suitability Program
w. PBGC Order FM 15-3, Suspension and Debarment Program

5. **BACKGROUND:** PBGC Directive is needed to ensure IT resources are available for official business necessity by limiting personal (non-official) use, and by taking actions necessary to protect resources, including responding to threats, and ensuring computer and telephone networks are stable. All federal employees/contractor employees have an obligation to protect and conserve U.S. Government property as well as put forth an honest effort in the performance of their duties, both of which preclude excessive use of IT resources for other than official purposes, or in a manner that creates an appearance that PBGC endorses their personal communications.

6. **DEFINITIONS:**

a. **Contracting Officer.** A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

b. **Contracting Officer's Representative (COR).** The official designated to provide technical direction to contractors and to monitor the progress of the contractor's work.

c. **Contractor Employee.** Any individual providing services to PBGC under contract or purchase order or any individual who is an employee of a firm or entity that provides services to the PBGC under a contract or purchase order.

d. **Electronic Messages.** Electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals.

e. **Electronic Messaging Account.** Any account that sends electronic messages.

f. **Federal Employee.** A current federal employee is a person who officially occupies a position in the federal government. For the purposes of this Directive, the term "federal employee" could also refer to an applicant or appointee during differing stages of the hiring process.

g. **Government Property.** Any form of real or personal property in which the government has an ownership, leasehold, or other property interest as well as any right or other intangible interest that is purchased with Government funds, including the services of contractor personnel. The term includes office supplies, telephone and other telecommunications equipment and services, the Government's mail, automated data processing capabilities, printing and reproduction facilities.

h. **Information Technology Resources (IT Resources).** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information. Examples include desktop and laptop computers assigned to federal employees/contractor employees accessing PBGC resources via remote technology (e.g. for Telework) and mobile devices.

i. **Mobile Devices.** Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory). Also, portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

j. **Official Business.** Any activity carried out by federal employees/contractor employees in the performance of job assignments, duties, and responsibilities.

k. **Office Equipment.** Equipment that includes, but is not limited to, laptop and desktop computers, mobile phones, peripheral equipment and software, telephones, copiers, handheld devices, facsimile machines, Internet connectivity and access to Internet services and electronic mail.

l. **Personal Use.** Any activity that does not accomplish official PBGC business.

m. **Personally identifiable information (PII).** Any information about an identifiable individual maintained by PBGC including, but not limited to, information about an individual's employment, financial history, medical history, education, family, and other

information that can be used to distinguish or trace an individual's identity, such as an individual's name, social security number, date and place of birth, mother's maiden name, and biometric records.

n. **Full Disk Encryption (FDE).** The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product.

o. **Records.** All information created or received by PBGC federal employees/contractor employees that is evidence of PBGC's business activities and preserved, or appropriate for preservation, by PBGC. A record can be in any media format (e.g. paper, digital or photo) and should document business activities or decisions. Also, records are defined as either temporary (at some point in time they can be destroyed) or permanent (a record that should be permanently stored at NARA).

p. **Removable Media Encryption (RME).** Software technology which monitors and encrypts data on removable devices such as Compact Disk (CDs) and thumb drives or any other device connected to a PBGC desktop or laptop.

q. **Sensitive Information.** Information that has a degree of confidentiality such that loss, misuse, unauthorized access, or modification of it could compromise the element of confidentiality and thereby adversely affect PBGC's business operations, plans or participants of pension plans insured or trusteed by PBGC, or the privacy of individuals covered under the Privacy Act. Refer to PBGC Directive IM10-03 for complete definition of Sensitive Information.

r. **Social Media.** Online environment where content is created, consumed, promoted, distributed, discovered, or shared for purposes that are primarily related to communities and social activities rather than functional, task-oriented objectives. "Media" in this context is an environment characterized by storage and transmission, while "social" describes the distinct way that these messages propagate in a 'one-to-many' or 'many-to-many' fashion.

s. **Unauthorized Software.** Computer applications not licensed, tested, and installed by PBGC, including shareware and freeware (for example, applications downloaded from the Internet).

t. **Unauthorized Files.** Files that have no official business or purpose on PBGC's computers and include, but are not limited to, files and software for which federal employees/contractor employees do not have authority to use because (a) materials for which federal employees/contractor employees do not have copyrighted permission; (b) material that is proprietary, trademarked, or subject to intellectual property rights (beyond fair use); or, (c) material covered by the Privacy Act.

u. **Unauthorized Hardware.** Office equipment not purchased, tested, distributed, and installed by PBGC, including desktop computers, laptops, flash drives, peripheral equipment, telephones, copiers, scanners, handheld devices, and facsimile machines.

7. **POLICY:** It is PBGC policy to permit limited personal use of Government office equipment and IT resources provided that such use complies with the provision prescribed herein. Limited personal use shall not interfere with official business or interfere with the mission or operations of PBGC.

a. **IT Resource Limits**. In general and for all federal employees/contractor employees, limits are imposed for the resources as indicated in the IT Resource Limits document.

(1) Periodically, federal employees/contractor employees will be provided with information concerning the amount of storage being used for electronic mailboxes, network file storage, and OneDrive for Business. Should federal employees/contractor employees find that they are approaching or have exceeded the above limits, they should contact the IT Service Desk to arrange for assistance in reducing the amount of resources.

(2) Should a federal employee/contractor employee have a business need to transmit or receive an electronic mail message in excess of the size limit specified in the IT Resource Limits document, that person should contact the IT Service Desk to use alternative transmission modes (e.g. file transfer protocol). Email messages exceeding the allowed size limit will be returned to sender.

(3) **Encrypted Message Attachments**. Federal employees/contractor employees shall ensure that all electronic mail attachments to external recipients containing PII are encrypted and secured with a password. The password shall be sent to the recipient in a separate communication mode (i.e. electronic mail, telephonically).

b. **Limited Personal Use of Office Equipment and IT Resources.** To create a more accommodating work environment, PBGC allows federal employees/contractor employees limited personal use of office equipment and IT resources. This policy does not create a right to use office equipment or IT resources for personal use, nor does it permit the use of any PBGC resources, including office equipment or IT resources, in any manner for the operation of a private business. Rather, this Directive grants federal employees/contractor employees the privilege to use office equipment and IT resources for limited personal use under the following general conditions. Personal use may be further restricted based on business need or in instances where use violates this Directive. Personal use is authorized when such use:

(1) Involves little or no additional expense to the Government.

(2) Is performed during the federal employee/contractor employee's non-work time.

(3) Does not reduce productivity or interfere with the orderly, efficient operation of PBGC.

(4) Does not violate the Privacy Act of 1974, the Standards of Ethical Conduct for Employees of the Executive Branch, or any other law, regulation, or PBGC

Directive.

(5) Adheres to PBGC Media Relations Directive.

(6) Does not compromise information security or result in a breach of PII.

c. **Guidelines and Examples of Personal Use.** The following guidelines are provided to further delineate and clarify the meaning and intent of limited personal use. The guidelines are not exhaustive, but serve to help federal employees/contractor employees determine the bounds of limited personal use in commonly occurring situations.

(1) The personal use incurs little or no additional cost to PBGC (such as electricity, ink, small amounts of paper, and ordinary wear and tear).

(2) The personal use of occasional short duration telephone or fax calls.

(3) Infrequent sending and receiving of personal electronic mail messages, limited personal use of the Internet for viewing web sites and social media sites.

(4) The use of a federal employee/contractor employee desktop computer to play music or view video files for which the federal employee/contractor employee has a license and which are contained on compact disks (CDs) or other computer-readable, removable original distribution media. Sound volume shall be controlled to not disrupt or interfere with the work activities of other federal employees/contractor employees.

d. **IT Authorization Procedures.** The Technical Review Board (TRB) is the formal mechanism for approving technical standards, technology, and products (software/hardware).

(1) **Request for new IT acquisition.** In the event that a federal employee/contractor employee or supervisor believes that a particular software, hardware, or other IT is needed to achieve PBGC business objectives, it is the responsibility of the federal employee/contractor employee and supervisor to seek approval from the TRB.

(2) **Change Approval.** Changes to PBGC IT environment must be submitted to the Change Advisory Board (CAB) in accordance with the IT Infrastructure Operations Department (ITIOD) Change Management Process and the ITIOD Change Management Standard Operating Procedures.

e. **General Prohibitions.**

(1) Prohibitions Subject to Disciplinary Action. The following use of office equipment and IT resources are prohibited, and any violations may subject the federal employee/contractor employee to immediate disciplinary action as described in *Directive PM 30-1, Disciplinary and Adverse Actions*.

a. Engaging in illegal, unethical, or inappropriate activities, including activities which could be offensive to federal employees/contractor employees or the public. Such activities include, but are not limited to, electronic mail forgery, hate speech, and materials that ridicule others on

the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

b. Conducting a private business or other commercial activities (e.g. federal employee/contractor employee dealing with customers or clients associated with outside employment or other activities related to outside employment). Federal employees/contractor employees are prohibited from using work time, office equipment, or IT resources to maintain or support commercial activities. For example, a federal employee/contractor employee may not use office equipment or IT resources (even during non-work hours) to run a travel business or accounting service, or conduct any activities, such as Internet research, in support of that personal enterprise. This absolute prohibition on using office equipment or IT resources to support commercial activities also prohibits federal employees/contractor employees from using office equipment or information technology resources to assist relatives, friends, or other persons in such activities. However, this does not prohibit limited personal use of office equipment or IT resources for a non-profit, volunteer, or pro bono activity, provided such use is done on the federal employee/contractor employee's non-work time and adheres to the limited personal use guidance of this Directive.

c. Using office equipment or IT resources as a staging ground or platform to gain unauthorized access to other systems.

d. Engaging in vulgar or obscene activity, such as sending electronic mail or visiting an Internet site that has graphically violent or sexually explicit material. In addition, federal employees/contractor employees shall not create, download, view, copy, store, or transmit sexually explicit or sexually oriented materials.

e. Engaging in or obtaining information to engage in gambling, illegal weapons possession, terrorism, or other illegal or prohibited activities.

f. Damaging, disrupting, or attempting to damage or disrupt PBGC's office equipment or IT resources. This includes intentionally or knowingly releasing a computer virus or other malicious software.

g. Participating in lobbying or prohibited partisan political activity, such as expressing opinions about candidates, distributing campaign literature, and donating or soliciting funds. This includes advocating or soliciting funds for partisan political groups and charitable organizations, except for PBGC approved purposes such as the annual U.S. Savings Bonds drive, the Combined federal Campaign, and certain Thomson School events.

h. Sharing information stored on PBGC Connect in a manner that allows it to be accessed by or disclosed to a person or entity who is not authorized to receive it.

i. Use of personally owned mobile devices and media to store sensitive information.

j. Unauthorized use of non-PBGC contracted cloud services to store PBGC information.

k. Access to any network or system for which the person has not been authorized or in a manner that knowingly violates PBGC policies.

l. Unauthorized use of a system (e.g. accessing information not needed to conduct one's official duties or unauthorized use of privileged commands). For example, no user may access the root account on a Unix system or attempt to access the most privileged accounts on the system unless he or she is authorized and has a reason to do so.

m. Unauthorized remote access services or mechanisms designed to bypass authorized remote access services.

n. Unauthorized forwarding or synchronization of email or other internal PBGC information or records to personally owned devices or resources.

o. Except under extenuating circumstances, using personal email account or personal electronic messaging account to conduct PBGC business to include sending or forwarding[1] official records from a PBGC email account to a personal email account.

(2) **Prohibitions Subject to Warning before Disciplinary Action.** The following actions are generally prohibited and will, if taken, result in a warning and advice as to how to avoid taking them in the future. Failure to heed the warning and follow the advice may result in future disciplinary action.

a. Modifying office equipment and IT resources, including, but not limited to, loading unauthorized software, unauthorized hardware, or unauthorized files as defined in this Directive, making computer system configuration changes, or attaching any equipment or device to office equipment or IT resources unless a part of their official duties, except by authorized Office of Information Technology (OIT) federal employee in performance of assigned duties.

b. Any personal use that could cause security exposure, congestion, delay, or disruption of service to any IT resources. For example, federal employees/contractor employees may not:

(i) Send electronic greeting cards or announcements in excess of 1MB in size through electronic mail or other means.

(ii) Send video or sound files other than for PBGC business

(iii) Use push or peer-to-peer technology or other continuous data streams which can degrade the performance of the network.

(iv) Negligently damage or disrupt PBGC's office equipment or IT resources. (This includes negligently releasing a computer virus,

[1]Employees using personal email accounts in violation of this Directive must forward a complete copy of the record to an official PBGC electronic messaging account no later than 20 days after the original creation or transmission of the record.

sending a chain letter electronic mail, or other act that could harm a computer or network.)

(v) Attempt to copy, delete, modify or read another's electronic mail without permission.

(vi) Enter PBGC email addresses in websites for unofficial business when posting to websites and social media websites.

c. Unauthorized physical or wireless connection of unapproved IT devices to PBGC IT resources (e.g. the connection of personal Smartphones or cameras for purposes of charging the battery source or for accessing information, or the connection and use of personal flash drives or personal removable hard drives).

d. Sharing individual authentication credentials (e.g. Personal Identity Verification (PIV), token, authenticator, PINs, passwords, etc.) with users for whom access to those credentials is not explicitly authorized.

f. **Messages to Large Groups.** In addition to observing resource limits, federal employees/contractor employees are required to obtain approval before sending electronic mail, announcements, files, or messages of a personal or unofficial nature to groups of recipients. The approval levels for the following groups of recipients are shown below:

Group	Approving Official or Designee
20 or more users	Department Director
Affinity Groups (e.g. Blacks in Government, Federally Employed Women, Federal Managers Association, Recreation Association, PBGC Toastmasters, etc.)	EMC Sponsor (or Group President if Group has no EMC Sponsor)
Fitness Center Members	Fitness Center Manager

Note: Birth and death announcements within the affected person's department require no approval but are subject to resource limits.

g. **Full Disk Encryption (FDE) and Removable Media Encryption (RME).** Federal employees/contractor employees shall ensure that removable media is encrypted using FDE or RME prior to being disconnected from the PBGC system.

h. **Proper Representation.** It is the responsibility of every federal employee/contractor employee to ensure they are not giving the false impression that they are acting in an official capacity when they are using office equipment or IT resources for personal purposes. Federal employees/contractor employees must also ensure that they do not give the false impression that PBGC endorses or sanctions personal activities. This

could include posting materials to external newsgroups, bulletin boards, social media, or other public forums. If there is a possibility that such a personal use could be interpreted to represent PBGC, an adequate disclaimer must be given. For example, an acceptable disclaimer would be: *The contents of this message are mine personally and do not reflect any position of the U.S. Government or the Pension Benefit Guaranty Corporation.*

i. **Security Reviews.** Federal employees/contractor employees have no right of privacy nor an expectation of privacy in their use of IT resources, including during periods of limited personal use. Any use of IT resources is made with the understanding that such use is generally not secure, not private, and not anonymous. PBGC conducts announced and unannounced security inspections of PBGC's office equipment and IT resources, including electronic mail messages and files showing web sites visited. By using office equipment and IT resources, federal employees/contractor employees consent to audits, interception, monitoring, recording, copying, and inspection of its use. Content and information may be subject to disclosure under the Freedom of Information Act (FOIA). If federal employees/contractor employees wish their private activities to remain private, then they should not engage in those activities using PBGC IT resources and other office equipment.

j. **Remote Access.** Use only PBGC approved methods to access, view, or transmit data when working at home or on travel. PBGC reserves the right to require the usage of PBGC issued equipment for the purposes of remote authentication. The IT Service Desk issues approved software programs and remote access equipment. The Remote Access User Guide posted on the Intranet provides instructions and approved methods for accessing electronic mail, files, applications, and other PBGC IT resources remotely.

k. **Mobile Devices**. Federal employees/contractor employees are expected to abide by the Mobile Device Rules of Behavior. All PBGC laptop and mobile users must show activity and use of the assigned asset within a 30 day time period. PBGC users showing no use of the assigned mobile asset will be considered "inactive" and notified to return the device. Federal employee/contractor employees shall not attempt to circumvent built in device security ("hack", "reimage", "jailbreak", or "root") as this compromises the security posture of the device. Device integrity will be enforced through the use of PBGC enterprise monitoring and compliance tools and solutions. In addition, monthly audits of device usage will be assessed for all PBGC laptop and mobile device users to include metrics on text message usage, cellular voice usage, email usage, and virtual private network usage.

l. **Electronic Records Management.** Routinely saving all electronic mail messages and attachments slows the mail server and poses unnecessary administrative burdens to PBGC. If an electronic mail message or attachment is an official federal record, then save it as required by PBGC Records Management Program. Delete non-record material when no longer needed, then complete the delete by emptying electronic waste baskets, both on desktops and within electronic mail accounts.

m. **Incident Reporting and Handling**. Federal employees/contractor employees shall promptly report all security incidents, actual or suspected, to the IT Service Desk at (202)326-4000 x3999. Example of incidents may include suspected or confirmed presence of malware, policy violations, misuse, loss or theft of a PIV, Smartphone, laptop, tablet, etc. Additional information regarding incident reporting is contained in the OIT Security Incident Response Management Plan. Federal employees/contractor employees shall also promptly report actual or potential breaches of sensitive information, including the disclosure or misuse of PII, to the Privacy Office at Privacy_Breach@pbgc.gov.

8. RESPONSIBILITIES:

a. **Department Directors and Supervisors**

(1) Ensure PBGC federal employees/contractor employees adhere to the requirements outlined in this Directive.

(2) Initiate appropriate action when federal employees/contractor employees disregard requirements in this Directive and document non-compliance issues.

(3) Provides authorization for visitors and volunteers conducting official business related to or on behalf of PBGC to use Government office equipment and IT resources.

(4) Ensure visitors and volunteers are knowledgeable of federal and agency policy before authorizing use of Government office equipment or IT resources.

b. **PBGC Federal Employees/Contractor Employees**

(1) Read, acknowledge, and comply with the requirements of this Directive.

(2) Complete IT Security Awareness training as appropriate to this Directive.

c. **IT Service Desk**

(1) Provide IT and related customer support for PBGC staff via phone, GetIT, email, and walk-in.

d. **Contracting Officer and Contracting Officer's Representative**

(1) Ensure this Directive is incorporated into contracts directly or by reference.

(2) Initiate appropriate action when contractors do not comply with this Directive.

e. **Visitors and Volunteers Conducting Business Related To or On Behalf of PBGC**

(1) Require written authorization to use Government office equipment and IT resources.

(2) Those providing authorization shall ensure visitors and volunteers are knowledgeable of federal and agency policy before use of Government office equipment or IT resources.

9. **Rules of Behavior for Information Technology Users:** The Rules of Behavior for Information Technology Users provide additional guidance to further highlight the due care and diligence required to protect PBGC information technology resources as described in this Directive. Individuals requiring access to organizational information and information systems must read and accept by signature (hand-written or electronic), the Rules of Behavior prior to being granted logical access, and re-sign the Rules of Behavior annually and within 30 days of an update to the Rules of Behavior in order to have continued access.

10. **Processes, Procedures, and Related Documents:** All documents containing processes and procedures referenced throughout this Directive are available below or on PBGC's Intranet page.

- Office of Information Technology, Security Incident Management Plan
- Information Technology Infrastructure Operations Department (ITIOD), Change Management Standard Operating Procedures
- Information Technology Infrastructure Operations Department (ITIOD), Change Management Process
- Removable Media Instructions
- Office of Information Technology, Technical Review Board Processes and Procedures

Pension Benefit Guaranty Corporation

INFORMATION ASSURANCE HANDBOOK
VOLUME 19

PBGC RELEVANT INFORMATION TECHNOLOGY RESOURCES

VERSION 2.0

JUNE 2008

Prepared by:

PBGC Office of Information Technology
Enterprise Information Security Office
1200 K Street NW
Washington, DC 20005

TABLE OF CONTENTS

RELEVANT INFORMATION TECHNOLOGY SECURITY RESOURCES 1
1 INTRODUCTION 1

Change/Review Record

Document Title: IAH Volume 19, Relevant Information Technology Resources

Date of Initial Release:

Version No.	Date Revised	Description of Revisions	
Draft v 1.0		Initial draft of Relevant Information Technology Resources	
Completed by: TechGuard Security			Date: March 2007
Approved by:			Date:
Version No.	**Date Revised**	**Description of Revisions**	
Completed by:			Date:
Approved by:			Date:
Version No.	**Date Revised**	**Description of Revisions**	
Completed by:			Date:
Approved by:			Date:
Version No.	**Date Revised**	**Description of Revisions**	
Completed by:			Date:
Approved by:			Date:
Version No.	**Date Revised**	**Description of Revisions**	
Completed by:			Date:
Approved by:			Date:

RELEVANT INFORMATION TECHNOLOGY SECURITY RESOURCES

1 INTRODUCTION

This document contains a easy reference table for relevant IT security laws, regulations and guidance that are commonly encountered in information assurance and security. It also contains links to those sources for easy reference. Due to constant changes in relevant laws, regulations, and guidance departments should always make sure that they consult with the Chief Privacy Officer to ensure that they are using the most recent amendments to any laws contained in this guideline.

Pension Benefit Guaranty Corporation (PBGC) Information Assurance Handbooks (IAH) are intended to provide information, procedures, and processes to assist departments to implement effective security programs that achieve compliance with relevant laws, regulations and policies governing the security of federal information systems. It is expected that fundamental laws, guidelines, or standards upon which the PBGC IAH is based will change consequently requiring updates to table.

Table 1: Law and Regulations

Name, Citation and Link	Regulations or Guidance Covering the Act or Law
Clinger-Cohen Act (formerly known as the Information Technology Management Reform Act of 2002) Public Law 104-106	
Computer Fraud and Abuse Act of 1986 (as amended in 1994 and 1996) 18 U.S.C. § 1030, P.L. 99-474 (the link below does not include changes that may arise as a result of the Homeland Security Act, P.L. 107-296). http://www.usdoj.gov/criminal/cybercrime/1029NEW.htm	
Economic Espionage Act of 1996 (Trade Secret Theft) 18 U.S.C. Section 90 http://www.ncix.gov/publications/booklets brochures/booklet_EconomicEsp/eea_brochure_00.pdf (PDF)	

E-Government Act of 2002 Public Law 107-347 http://www.cio.noaa.gov/itmanagement/egovact.pdf (PDF)	
Electronic Communications Privacy Act 18 U.S.C. Section 2701 http://www4.law.cornell.edu/uscode/18/2701.html	
The Federal Managers' Financial Integrity Act 31 U.S.C. Section 1105, P.L. 97-255 http://www.whitehouse.gov/omb/financial/fmfia1982.html	
Freedom of Information Act (as amended 2002) 5 U.S.C. Section 552 http://www.usdoj.gov/04foia/foiastat.htm	DOJ Freedom of Information Act Guide, May 2002 (Guide to FOIA exemptions) (http://www.usdoj.gov/oip/foi-act.htm)
Government Paperwork Elimination Act 44 U.S.C. Section 3504, Public Law No. 106-277 http://www.cio.noaa.gov/itmanagement/pea.pdf (PDF)	
Paperwork Reduction Act 44 U.S.C. Section 3501, Public Law 104-13 http://www.cio.noaa.gov/itmanagement/pralaw.pdf (PDF)	
Privacy Act of 1974 5 U.S.C. § 552A http://www.usdoj.gov/foia/privstat.htm	Overview of the Privacy Act of 1974 http://www.usdoj.gov/04foia/04_7_1.html Overview of the Privacy Act of 1974:Role of the Office of Management and Budget Office of Management and Budget Memorandum

	99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" (http://www.whitehouse.gov/omb/memoranda/m99-05.html) OMB Memorandum 99-18, "Privacy Policies On Federal Web Sites" (http://www.whitehouse.gov/omb/memoranda/m99-18.html) OMB Memorandum 00-13, "Privacy Policies and Data Collection on Federal Web Sites" http://www.whitehouse.gov/omb/memoranda/m00-13.html
Right to Financial Privacy Act 12 U.S.C. 3401 http://www4.law.cornell.edu/uscode/12/ch35.html	
Federal Financial Management Improvement Act of 1996 FFMIA www.whitehouse.gov/omb/financial/ffs_**ffmia**.html	
Trade Secrets Protection Under Federal Law http://www.fbi.gov/publications/leb/1997/july976.htm (see Trade Secret Offenses links) (the link below does not include changes that may arise as a result of the Homeland Security Act, P.L. 107-296).	
Federal Information Security Management Act (FISMA from E-Gov Act) http://csrc.nist.gov/policies/FISMA-final.pdf (PDF)	
National Technology Transfer and Advancement Act of 1995 http://www.nal.usda.gov/ttic/faq/pl104113.htm	
National Archives and Records Administration Schedule 12	

http://www.archives.gov/records-mgmt/ardor/grs14.html	

Table 2: OMB Circulars

Circular Name and Number	Link to Circular
Office of Management and Budget Circular A-130, "Management of Federal Information Resources"	http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
OMB Circular A-123, Management Accountability and Control	http://www.whitehouse.gov/omb/circulars/a123/a123.html
OMB Circular A-127, Financial Management Systems	http://www.whitehouse.gov/omb/circulars/a127/a127.html
OMB Circular A-11, Preparation, Submission and Execution of the Budget	http://www.whitehouse.gov/omb/circulars/a11/03toc.html
OMB Circulars Index	http://www.whitehouse.gov/omb/circulars/index.html
OMB Circular M-97-02, Funding Information Systems Investments	http://www.whitehouse.gov/omb/memoranda/m97-02.html
OMB Circular	http://www.whitehouse.gov/omb/circulars/a11/02toc.html
OMB Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs	http://www.whitehouse.gov/omb/circulars/a094/a094.html
OMB Circular M-02-01Guidance for Preparing and Submitting Security Plans of	http://www.whitehouse.gov/omb/memoranda/m02-01.html

Action and Milestones	
OMB Office of Management and Budget Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 2003	www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf
Office of Management and Budget M-06-15, Safeguarding Personally Identifiable Information	www.whitehouse.gov/omb/memoranda/fy2006/**m-06-15**.pdf
Office of Management and Budget M-06-16, Protection of Sensitive Agency Information	www.whitehouse.gov/omb/memoranda/fy2006/m-06-19.pdf
Office of Management and Budget Memorandum 01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy	www.whitehouse.gov/omb/memoranda/m**01-05**.html
OMB Memorandum 03-22 Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002	http://www.whitehouse.gov/omb/memoranda/m03-22.html

Table 3: Directives

Directive Name and Number	Link to Directive
Presidential Decision Directive 67	http://www.fas.org/irp/offdocs/pdd/pdd-67.htm
Homeland Security Presidential Directive/Hspd-7	http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
Homeland Security Presidential Directive/Hspd-8	http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html

Table 4: National Institute of Standards and Technology Special Publications

NIST SP guidance	Directive/Guide
Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf (PDF)
Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme	http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf (PDF)
Wireless Network Security: 802.11, Bluetooth, and Handheld Devices	http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf (PDF)
Security Guide for Interconnecting Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf (PDF)
Guidelines on Firewalls and Firewall Policy	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf (PDF)
Procedures for Handling Security Patches	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf (PDF)
Contingency Planning Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf (PDF)

Underlying Technical Models for Information Technology Security	http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf (PDF)
Risk Management Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (PDF)
Engineering Principles for Information Technology Security (A Baseline for Achieving Security)	http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf (PDF)
Security Self-Assessment Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf (PDF)
Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products	http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf
Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172)	http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (PDF)
Guide for the Security Certification and Accreditation of Federal Information Systems (Final as of May 2004)	http://www.csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf (PDF)
Establishing a Computer Security Incident Response Capability (Superseded by NIST 800-61)	http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf (PDF)
Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers	http://checklists.nist.gov/docs/SP_800-70_20050526.pdf
Guide to Selecting Information Technology Security Products	http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf
Guidelines for Media Sanitization	http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Security for Telecommuting and Broadband Communications	http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf
Guide for Developing Security Plans for Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
Guide to Information Technology Security Services	http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf
Interfaces for Personal Identity Verification	http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf
Biometric Data Specification for Personal Identity Verification	http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf
Security Considerations in the Information System Development Life Cycle	http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf
Guidelines on Active Content and Mobile Code	http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf
Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf
Recommendation on Key Management	http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
Security Considerations for Voice Over IP Systems	http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
Electronic Authentication Guideline	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf