Pension Benefit Guaranty Corporation

Order

Subject: Protecting Sensitive Information

Directive Number: IM 10-3

Effective Date: 4/23/08 **Originator: OGC**

Stephen E. Barber
Chief Management Officer

---

1. **PURPOSE:** This Order establishes the policies and procedures for protecting sensitive information.

2. **CANCELLATION:** This Order supersedes PBGC Directive IM 10-3 dated 6/10/93.

3. **SCOPE:** This Order applies to all PBGC employees and contractors.

4. **AUTHORITIES:**

   a. Freedom of Information Act (FOIA); 5 U.S.C. § 552.
   b. Privacy Act of 1974; 5 U.S.C. §552a.
   c. Trade Secrets Act; 18 U.S.C. §1905.
   d. Internal Revenue Code (I.R.C.) §6103.
   e. Paperwork Reduction Act; 44 U.S.C. §§3501-3520.
   f. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C.§§ 3541-3549.
   g. OMB Memorandum M-06-16 (June 23, 2006), Protection of Sensitive Agency Information.
   h. OMB Memorandum M-07-16 (May 22, 2007), Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

5. **BACKGROUND:** This Order implements guidance issued by the Office of Management & Budget (OMB) to strengthen policies and procedures to protect sensitive information in the possession of the federal government from loss or unauthorized disclosure through a data breach.

   AN EMPLOYEE THAT FAILS TO FOLLOW THE POLICIES OR PROCEDURES ESTABLISHED UNDER THIS DIRECTIVE IS SUBJECT TO DISCIPLINE BY THE PBGC, UP TO AND INCLUDING TERMINATION OF

EMPLOYMENT. *SEE* PBGC DIRECTIVE PM 30-1. A CONTRACTOR MAY BE REMOVED FROM FURTHER WORK UNDER A PBGC CONTRACT. PBGC EMPLOYEES AND CONTRACTORS ARE ALSO SUBJECT TO CIVIL AND CRIMINAL FINES AND PENALTIES FOR UNAUTHORIZED ACCESS OR DISCLOSURE OF SENSITIVE PBGC INFORMATION.

6. **DEFINITIONS:**

a. **Contracting Officer's Technical Representative (COTR).** The PBGC official that has been designated to provide technical direction to a PBGC contractor and contractor employees and to monitor the progress of the contractor's work.

b. **Data breach**. Any situation where an unauthorized person for an unauthorized purpose has accessed or acquired (or potentially accessed or acquired) sensitive PBGC information in electronic or hard copy format.

c. **Data extract**. For purposes of this directive, the term data extract refers to any sensitive PBGC information that has been temporarily downloaded or copied from a PBGC information system such as PRISM, CHAMPS, or CFS, and maintained in electronic format outside the originating system.

A data extract does **not** include sensitive information in electronic form that is transmitted or disclosed to a PBGC contractor or other authorized person or entity under a Memorandum of Understanding and Interconnection Security Agreement established under policies and procedures outlined in Volume 4 of PBGC's Information Assurance Handbook.

d. **Electronic Format**. PBGC information as it is maintained or viewed from a server, hard drive, random access memory (RAM), read-only memory (ROM) or from another type of portable electronic storage device.

e. **Hard Copy Format**. The physical representation of PBGC information when it is printed on paper.

f. **Information System**. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, creation, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Examples include desktop and laptop computers assigned to staff.

g. **Information System Owner**. A PBGC Department Director or other PBGC Official who has been designated as responsible for the procurement, development, integration, modification, or operation and maintenance of an information system.

h. **Need-to-know**. The phrase describes information that a PBGC employee or contractor must use to perform the official duties of their position.

i. **Network**. Two or more PBGC information systems that are linked to share resources, exchange files, or allow electronic communications.

j. **Portable Storage Device.** A laptop computer, personal digital assistant, CD, DVD, diskette, flash drive or other electronic storage device that can be transported outside the PBGC.

k. **Sensitive PBGC information** may include, among others, agency records in electronic or hard copy format that refer to:

(1) Personally identifiable information (PII) about individuals that is subject to the Privacy Act of 1974, 5 U.S.C. §552a, such as information relating to individual participants and beneficiaries in covered pension plans, or individual PBGC employees or contractors. PII also includes nonpublic information about an individual that, when combined with the individual's name, can be used to distinguish or trace an individual's identity, such as the individual's social security number, date or place of birth, and mother's maiden name, *etc*.

(2) Confidential business information submitted to the PBGC by a plan sponsor or controlled group member or information required to be submitted under ERISA §§ 4010 or 4043, 29 U.S.C. §1310 or 1343. Such information is exempt from disclosure in response to a request under the Freedom of Information Act, 5 U.S.C. 552(b)(4), and protected from unauthorized disclosure under the Trade Secrets Act, 18 U.S.C. §1905.

(3) Confidential cost or proprietary information submitted in response to a PBGC request for proposals (RFP) or PBGC source selection information protected from disclosure under the Procurement Integrity Act, 41 U.S.C. §423(a).

(4) Tax returns or return information obtained from the Internal Revenue Service under I.R.C. §6103.

(5) Any other nonpublic information that a PBGC employee or contractor knows, or reasonably should know, is considered confidential by the PBGC or the person or entity that submitted the information to the PBGC such as tax returns submitted to PBGC by a tax payer.

IF AN EMPLOYEE OR CONTRACTOR HAS A QUESTION ABOUT WHETHER INFORMATION OBTAINED IN THE COURSE OF

PERFORMING OFFICIAL DUTIES FOR THE PBGC IS SENSITIVE AND SUBJECT TO THE POLICIES AND PROCEDURES OUTLINED IN THIS DIRECTIVE, THE EMPLOYEE OR CONTRACTOR SHOULD CONSULT THEIR SUPERVISOR OR COTR, AS APPROPRIATE, FOR GUIDANCE.

l. **Third Party Request:** a request for access to or copies of sensitive PBGC information made by a person or entity outside the PBGC who has not been authorized to access the information requested.

7. **POLICIES AND PROCEDURES.** PBGC employees and contractors are responsible for all sensitive information obtained by them in the course of performing official duties, whether in electronic or hard copy format, and must treat such information in a manner that will prevent it from being accessed by or disclosed to a person or entity who is not authorized to receive it.

a. **Access.** Access to sensitive PBGC information is limited to PBGC employees or contractors with a need-to-know that information to perform official duties.

(1) PBGC employees and contractors must refer any third-party request for access to or copies of sensitive information through supervisory channels to the PBGC's Disclosure Officer for processing under the Freedom of Information Act and the Privacy Act.

(2) PBGC employees and contractors must refer all inquiries from the media to the Communications and Public Affairs Department.

(3) Sensitive PBGC information in electronic format must be stored or maintained in a PBGC Information System that is subject to the information security policies and procedures outlined in PBGC's Information Assurance Handbook. *See* http://intranet/dirpoldel/iah.cfm.

(a) The Information System Owner determines which PBGC employees and contractors are authorized to access the Information System under the procedures outlined in Volume 1 of the PBGC's Information Assurance Handbook.

(b) PBGC employees and contractors who have been authorized to access a PBGC Information System must abide by the terms of PBGC Directive IM 05-04, Use of Information Technology (http://intranet/DirPolDel/Directives/IM_05_4.pdf.) and all policies and procedures outlined in PBGC's Information Assurance Handbook. *See* http://intranet/dirpoldel/iah.cfm.

(4) To protect sensitive information in hard copy format, PBGC employees or

contractors must:

(a) Promptly retrieve print outs from copiers, printers, or fax machines so that sensitive information is not accessed by individuals who do not have a need to know;

(b) Store sensitive information in a locked drawer or file cabinet when it is not being used;

(c) Cover sensitive information on one's desk when leaving for a brief period of time;

(d) When necessary, label or mark documents as "Sensitive Information" or attach a sensitive information cover sheet, Form PBGC 263 (Attachment 1), to the materials to prevent inadvertent access or disclosure.

(e) Shred non-record copies of sensitive information in hard copy format when the information is no longer needed for the assignment or task. *See* PBGC Directive IM 15-1, PBGC Records Management Program.

(5) PBGC employees and contractors must follow the safeguarding policies and procedures established under PBGC Directive IM 10-2 to access and use tax returns and return information obtained by the PBGC under I.R.C.§ 6103. (Tax returns or return information submitted to the PBGC by a taxpayer are considered sensitive PBGC information and subject to the policies and procedure outlined in this directive.)

b. **Removal or transmittal**. To the maximum extent practicable, sensitive PBGC information should not be removed from the PBGC's offices (including the offices of a Field Benefit Administrator) or downloaded from a PBGC Information System for transmission outside a PBGC network.

(1) Unless authorized under ¶ 7. d., PBGC employees and contractors are prohibited from downloading sensitive information in electronic format to a portable storage device (*e.g.*, lap top computer, CD, DVD, diskette, flash drive or a personal digital assistant).

(2) Unless authorized under ¶ 7. d., PBGC employees and contractors are prohibited from transmitting sensitive information in electronic format over the internet to a recipient who is not connected to a PBGC network.

(a) Sensitive PBGC information may be transmitted by electronic mail between PBGC employees and contractors who have been

assigned accounts on PBGC's electronic mail system and who have a need-to-know the sensitive information to perform official duties.

(b) If an electronic mail message between PBGC employees or contractors must include personally identifiable information (PII) about an individual, the sender must not include the individual's Social Security number in the subject line of the message, but only in the body of the message so that the Social Security number does not appear readily in the recipient's inbox.

(3) When necessary for an authorized business purpose, a PBGC employee or contractor may seek authorization under written procedures developed by the PBGC Information System Owner to remove from PBGC's offices sensitive information in hard copy format from the information system.

(a) To the maximum extent practicable, only copies of sensitive PBGC information in hard copy format should be removed from PBGC's offices, not original documents or records.

(b) Employees and contractors should only remove from PBGC the minimum amount of sensitive information necessary to perform a particular assignment or task.

(c) PBGC employees or contractors that remove sensitive information in hard copy format from the PBGC's offices are responsible for taking reasonable precautions to prevent the loss or unauthorized disclosure of the information. Reasonable precautions include, but are not limited to:

1) Transporting sensitive information in a locked briefcase, backpack, portfolio, or other container. The container should be identifiable by a tag, label, or decal that lists the owner, his or her mailing address, and other contact information so that the container can be returned if it is lost or misdirected.

2) Locking sensitive information that is being transported by car out of sight in the car's trunk.

3) Storing sensitive information in a drawer or cupboard when it must be left unattended at home or while on travel in a hotel room.

4) Shredding non-record copies of sensitive information in

hard copy format when the information is no longer needed for an assignment or task. Information or documents that qualify as a PBGC "record" under the Federal Records Act, 41 U.S.C. §4401, must be retained until eligible for destruction under a records disposition schedule that has been approved by the National Archives and Records Administration. *See* PBGC Directive IM 15-1, PBGC Records Management Program.

c. **Remote Access.** Authorized PBGC employees and contractors may access sensitive PBGC information maintained in electronic format in a PBGC information system from a remote location via PBGC Atwork (atwork.pbgc.gov) or PBGC Outlook Web Access (owa.pbgc.gov) by using a PBGC-issued security token.

HOWEVER, PBGC EMPLOYEES AND CONTRACTORS ARE PROHIBITED FROM DOWNLOADING SENSITIVE INFORMATION ACCESSED VIA PBGC ATWORK OR PBGC OWA TO THE USER'S HOME COMPUTER OR ANY PORTABLE STORAGE DEVICE THAT WAS NOT PROVIDED BY THE PBGC.

For example, an employee working from home may log into PBGC's network through PBGC Atwork and access a Microsoft Word document saved on the employee's h:\ drive that includes sensitive information. The employee may edit the document and save it back to the h:\ drive on PBGC's network. The employee is not permitted to save the document to a local drive on the employee's home computer, log out of the PBGC's network, and edit the document using the version of Microsoft Word installed on the employee's home computer.

d. **Creating Data Extracts**. If remote access and use of sensitive information outside the PBGC via PBGC Atwork or OWA is not practicable, a PBGC employee or contractor may seek authorization under written procedures developed by the PBGC Information System Owner to create a temporary data extract of the information in electronic format that can be transmitted or removed outside the PBGC for an authorized business purpose.

(1) Data extracts must be password protected and encrypted using Winzip's 256-bit AES encryption, before the sensitive information can be removed or transmitted outside PBGC.

(2) If an employee elects to use a flash drive to store a data extract, the flash drive must support encryption. If you have questions about whether a flash drive supports encryption, please contact the PBGC Service Desk (extension 3999).

(3) The password to an encrypted data extract must be transmitted or carried separately so that the sensitive information is protected if the data extract is misdirected or lost.

(4) The PBGC employee or contractor who creates a data extract is responsible for deleting or destroying it when it is no longer needed for official business.

(a) Information from a data extract that qualifies as a PBGC "record" under the Federal Records Act, 41 U.S.C. §4401, must be transferred to a PBGC information system where it can be maintained by PBGC until eligible for destruction under a records disposition schedule approved by the National Archives and Records Administration. *See* PBGC Directive IM 15-1, PBGC Records Management Program.

(b) Non-record information in electronic format must be deleted or erased when no longer needed in accordance with the policies and procedures established under Volume 10 of PBGC's Information Assurance Handbook.

(5) Examples:

(a) An employee of the Benefit Payments and Administration Department (BAPD) is assigned to attend an informational meeting for participants and beneficiaries of a newly trusteed plan. To be able to answer questions raised by any of the participants or beneficiaries who attend about their own benefits, the BAPD employee requests approval to download participant data to a PBGC lap top computer that can be carried to the meeting. If downloading the data to take to the meeting is authorized, the BAPD employee must encrypt the data when it is saved to the lap top computer. After the meeting, the BAPD employee is responsible for deleting the data from the lap top.

(b) An attorney in the Office of Chief Counsel (OCC) is preparing a pleading to file in the bankruptcy of a plan sponsor. Because the pleading refers only to publicly available information that is available to all the parties in the litigation, the OCC attorney can attach the pleading to an e-mail message sent to her personal e-mail address so that she can work from home to meet a filing deadline.

(c) If the pleading in the above example referred to sensitive PBGC information such as the amount of benefits owed by PBGC under

title IV of ERISA to specific individuals, or information about the plan sponsor submitted to the PBGC under ERISA § 4010, the OCC attorney would be required to access and edit the pleading from home via PBGC Atwork. Alternatively, the OCC attorney could seek approval under OCC procedures to download and encrypt the pleading to a portable flash drive that supports encryption that she could carry home to edit the document from her home computer. The employee could not save the pleading to a drive on her home computer when editing the document.

(d) An employee in the Legislation and Regulations Department (LRD) is drafting a regulation to implement recent legislative changes to ERISA. Because proposed policies, regulations, or legislation do not typically include sensitive information, the LRD employee may save the file to a CD that he can take from the office to work from home. However, if the proposed regulation addresses a controversial issue that is the focus of media or Congressional attention, the LRD employee should consult with his supervisor to determine whether the draft regulation should be treated as sensitive PBGC information under this Directive.

e. **Logging Data Extracts**. To maintain accountability of all sensitive information transmitted or carried outside the PBGC in a data extract, PBGC information system owners must develop written procedures to maintain a log of all data extracts that have been authorized to be created and removed or transmitted outside the PBGC.

(1) The log must include:

(a) The name of the PBGC employee or contractor who created the data extract;

(b) A description of type and amount of sensitive information included in the data extract;

(c) The date the data extract was created;

(d) The portable storage device to which the sensitive information was downloaded or saved (*e.g.*, an encrypted file saved to a laptop computer, CD, DVD, diskette, flash drive or other electronic storage device); and

(e) The date the data extract was deleted.

(2) The procedures developed by the PBGC Information System owner must

designate an employee or contractor who is responsible for maintaining data extract logs. The responsible employees must:

(a) Contact each employee or contractor who created a data extract at least once every 90 days, to determine whether it is still in use, or has been deleted or destroyed (after record information has been transferred to a PBGC information system where it can be maintained by PBGC until eligible for destruction).

(b) Submit a report to the PBGC's Senior Agency Information Security Officer each quarter that includes:

1) The identity of the PBGC employees or contractors who were authorized to create a data extract;

2) the date the data extract was created;

3) A description of type and amount of sensitive information included in the data extract; and

4) Whether the data extract is still in use, or the date it was deleted.

(c) The PBGC Information System Owner must submit to the PBGC Senior Agency Information Security Officer for approval the written procedures developed to authorize users to create data extracts, log data extracts, and report on whether data extracts are still needed by the user or have been erased or deleted. The procedures must be submitted for approval within 45 days of the effective date of Directive or when business processes require modification of previously approved procedures.

f. **Reporting Requirement**. PBGC employees or contractors who become aware that sensitive PBGC information may have been lost, improperly accessed or disclosed must immediately report their concern to their supervisor or COTR, as appropriate, and to the PBGC's Senior Agency Information Security Officer, the Information Systems Security Officer, or the Office of Inspector General. Prompt reporting is necessary for PBGC to take appropriate action to mitigate any harm caused by the loss or unauthorized disclosure. *See* PBGC Information Assurance Handbook, Volume 8, Incident Response.

g. **Corrective Action.** PBGC may take corrective action against a PBGC employee or contractor that fails to follow the policies or procedures established by the PBGC to protect sensitive information.

(1) A PBGC employee is subject to discipline under the procedures outlined in PBGC Directive PM 30-1. Penalties may include reprimand, suspension, or removal.

(2) A contractor may be removed or disqualified from further work under a PBGC contract.

(3) PBGC will also consider prompt removal of an individual's authority to access PBGC information systems if the individual demonstrates egregious disregard or a pattern of error in protecting sensitive PBGC information.

(4) The behaviors for which PBGC may initiate corrective or disciplinary action include, but are not limited to:

(a) Failure to follow the policies or procedures established by PBGC to protect sensitive information, regardless of whether that failure resulted in the loss or unauthorized disclosure of sensitive information;

(b) Exceeding authorized access to, or disclosure to unauthorized persons or entities, of sensitive PBGC information;

(c) Failure to report any known or suspected loss of control or unauthorized disclosure of sensitive PBGC information; and

(d) For supervisors and managers, failure to adequately instruct, train, or supervise employees in their responsibilities to protect sensitive information.

(5) PBGC employees and contractors are also subject to civil and criminal fines and penalties for unauthorized access or disclosure of sensitive PBGC information.

(a) The Privacy Act applies to information about an individual that is retrievable from a system or records by reference to the individual's name or other unique identifier assigned to the individual. PBGC and its employees and contractors are subject to civil and criminal fines and penalties for unauthorized disclosure of information subject to the Privacy Act.

(b) The Trade Secrets Act makes it a crime for a PBGC employee to disclose information that is exempt from disclosure under the Freedom of Information Act because it refers to trade secrets or confidential commercial or financial information that has been

submitted to the PBGC, unless the disclosure is authorized by law or regulation.

(c) PBGC and its employees and contractors are subject to civil and criminal fines and penalties for unauthorized access, disclosure, or inspection of tax returns or return information obtained by the PBGC under I.R.C.§ 6103.

(d) Unauthorized access or exceeding authorized access to a computer system may constitute a crime under 18 U.S.C. §1030.

8. **Responsibilities:**

a. **The Chief Information Officer** is responsible for:

(1) establishing the policies and procedure for protecting sensitive PBGC information;

(2) providing annual computer security training for PBGC employees and contractors to make them aware of the applicable policies and procedures for protecting sensitive information; and

b. **The General Counsel** is responsible for rendering legal advice with respect to:

.

(1) the policies and procedures established to protect sensitive PBGC information; and

(2) initiating and taking corrective or disciplinary action against a PBGC employee or contractor for failing to follow the policies and procedures established to protect sensitive PBGC information.

c. **The Deputy General Counsel** has been designated as the Senior Agency Official for Privacy and has agency-wide responsibility for information privacy issues.

d. **PBGC Information System Owners** are responsible for developing written procedures to authorize users to create data extracts, log data extracts, and report on whether data extracts have been erased or deleted in accordance with ¶ 7 d. and e.

e. **PBGC's Senior Agency Information Security Officer** is responsible for:

(1) approving procedures developed by PBGC Information System Owners to authorize users to create data extracts, log data extracts, and report on whether data extracts are still needed by the user or have been erased or deleted in accordance with ¶ 7 d. and e.

(2) reviewing quarterly reports required under ¶ 7 e. on whether data extracts from a PBGC Information System are still needed by the user or have been erased or deleted.

f. **PBGC's Information Systems Security Officer** is responsible for responding to reports that sensitive PBGC information may have been lost or improperly accessed or disclosed in a data breach under the policies and procedures outlined in Volume 8 of PBGC's Information Assurance Handbook - Incident Response.

g. **PBGC's Disclosure Officer** is responsible for:

(1) responding to third party requests for information under the Freedom of Information Act and the Privacy Act; and

(2) providing training for PBGC employees and contractors on the Freedom of Information Act and the Privacy Act.

h. **The Procurement Department** is responsible for:

(1) insuring that all contract actions include provisions that require contractors to follow PBGC's policies and procedures for protecting sensitive information; and

(2) initiating appropriate corrective action against a contractor for failure to follow PBGC's policies and procedures for protecting sensitive information.

i. **Supervisors and managers** are responsible for:

(1) instructing employees in their responsibilities to protect sensitive information; and,

(2) after consulting with appropriate officials from the Human Resources Department, initiating corrective or disciplinary action when an employee fails to follow PBGC's policies and procedures for protecting sensitive information.

j. **Employees and contractors** are responsible for:

(1) following the policies and procedures established by the PBGC to protect sensitive information;

(2) seeking guidance from their supervisor or COTR, as appropriate, if they have any questions on how to protect sensitive PBGC information; and

(3) reporting any known or suspected loss of control or unauthorized disclosure of sensitive PBGC information to their supervisor or COTR, as appropriate, and to the PBGC's Senior Agency Information Security Officer, the Information Systems Security Officer, or the Office of Inspector General.

Attachment

ATTACHMENT
IM 10-3

NOTICE

DOCUMENT RESTRICTED
TO OFFICIAL USE
WITHIN PBGC ONLY

RECIPIENTS OF THIS DOCUMENT MUST NOT SHOW OR RELEASE ITS CONTENTS FOR OTHER THAN OFFICIAL PURPOSES WITHIN PBGC UNDER ANY CIRCUMSTANCES.

AT ALL TIMES IT MUST BE SAFEGUARDED TO PREVENT IMPROPER DISCLOSURE OF THE INFORMATION CONTAINED THEREIN.

DIRECTED BY:

_____
SIGNATURE

_____ _____
ORGANIZATION **PHONE EXT.**

_____
DATE