



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document:	Federal Reserve Board (FRB) Division of Information Technology (IT) <u>Information Classification and Handling Standard</u> , 2019
Requested date:	14-October-2020
Release date:	10-November-2020
Posted date:	30-November-2020
Source of document:	Information Disclosure Section Board of Governors of the Federal Reserve System 20th & Constitution Avenue, NW, Washington, DC 20551 Fax: (202) 872-7565 <a href="#">Electronic Request Form</a>

The governmentattic.org web site ("the site") is a First Amendment free speech web site and 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.



BOARD OF GOVERNORS  
OF THE  
**FEDERAL RESERVE SYSTEM**  
WASHINGTON, D. C. 20551

ADDRESS OFFICIAL CORRESPONDENCE  
TO THE BOARD

November 10, 2020

*Re: Freedom of Information Act Request Nos. F-2021-00014 and  
F-2021-00015*

This is in response to your email messages dated and received by the Board's Information Disclosure Section on October 14, 2020. Pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, you request:

[FOIA F-2021-00014]

A copy of Federal Reserve Board document entitled:  
Information Classification and Handling Standard and  
appendices.

[FOIA F-2021-00015]

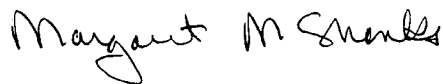
A copy of the document describing the taxonomy/categories of  
limited distribution information at Federal Reserve Board, such  
as Confidential, Strictly Confidential, etc.

Staff searched Board records and located the Board's Information Classification and Handling Standard and its appendices that you seek in your FOIA request numbered F-2021-00014. Because this document describes the Board's taxonomy of limited distribution information, it is also considered responsive to your FOIA request numbered F-2021-00015. I have determined, however, that certain portions of this document consist of information relating to the techniques or procedures of the information security operations of the Board that, if disclosed, could reasonably be expected to risk circumvention of the law. This information is exempt and will be withheld from you under authority of exemption 7(E) of the FOIA, 5 U.S.C. § 552(b)(7)(E). I have also determined that the information should be withheld because it is reasonably foreseeable that disclosure would harm an interest protected by an exemption described in subsection (b) of the FOIA, 5 U.S.C. § 552(b). The responsive document has been reviewed under

the requirements of subsection (b) and all reasonably segregable nonexempt information will be provided to you. The document being provided to you will indicate the amount of information that has been withheld and the applicable exemption.

Accordingly, your request is granted in part and denied in part for the reason stated above. The Board's Information Disclosure Section will provide you with a copy of the document being made available to you under separate cover. If you believe you have a legal right to any of the information that is being withheld, you may appeal this determination by writing to Office of the Secretary, Board of Governors of the Federal Reserve System, Attn: FOIA Appeals, 20th Street & Constitution Avenue NW, Washington, DC 20551; or sent by facsimile to Office of the Secretary, (202) 872-7565; or electronically to FOIA-Appeals@frb.gov. Your appeal must be postmarked or electronically transmitted within 90 days of the date of the response to your request.<sup>1</sup>

Very truly yours,



Margaret McCloskey Shanks  
Deputy Secretary of the Board

---

<sup>1</sup>As an alternative to an administrative appeal, you may contact the Board's FOIA Public Liaison, Ms. Candace Ambrose, at 202-452-3684 for further assistance. Additionally, you may 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, MD 20740-6001; email at ogis@nara.gov; telephone at 202-741-5770 or toll free at 1-877-684-6448; or facsimile at 202-741-5769.



# **Information Classification and Handling Standard**

Version 3.0 | January 7, 2019  
Prepared by the Information Security Officer

## TABLE OF CONTENTS

<b>1.0</b>	<b>Introduction .....</b>	<b>3</b>
<b>2.0</b>	<b>Scope .....</b>	<b>3</b>
<b>3.0</b>	<b>Definitions .....</b>	<b>4</b>
<b>4.0</b>	<b>General Controls .....</b>	<b>7</b>
<b>5.0</b>	<b>Classifications .....</b>	<b>7</b>
<b>6.0</b>	<b>Restricted-Controlled FR.....</b>	<b>12</b>
<b>7.0</b>	<b>Restricted FR.....</b>	<b>16</b>
<b>8.0</b>	<b>Sensitive Personally Identifiable Information (SPII FR) .....</b>	<b>19</b>
<b>9.0</b>	<b>Internal FR/Official Use .....</b>	<b>23</b>
<b>10.0</b>	<b>Nonconfidential .....</b>	<b>26</b>
<b>11.0</b>	<b>Public/Official Release.....</b>	<b>26</b>
<b>12.0</b>	<b>Personal/Non-work.....</b>	<b>27</b>
<b>13.0</b>	<b>Mobile Storage Devices .....</b>	<b>27</b>
<b>14.0</b>	<b>E-Mail and Calendar Security .....</b>	<b>29</b>
	<b>Attachment 1: Coversheets.....</b>	<b>32</b>
	<b>Attachment 2-A: Summary for Handling Printed Information .....</b>	<b>36</b>
	<b>Attachment 2-B: Summary for Handling Digital Information.....</b>	<b>37</b>

## 1.0 Introduction

The fundamental principle of handling requirements is to provide appropriate protection for assets of the Board of Governors of the Federal Reserve System (the Board) and to information relating to the Board's customers, business partners, and staff. The purpose of this Standard is to define specific handling requirements for printed and digital information of the Board (see section 2.0 below for scope).

The requirements in this standard are the minimum requirements for classifying and handling Board information. Thus, to the extent information within the Board is subject to additional special restrictions, such as through contractual arrangements, the standard applies to this information only to the extent they are consistent with the additional special restrictions. Examples of information that may be subject to greater or different requirements are the following:

- Information released by information owners to parties outside the Federal Reserve System (FRS), and for which continued controls are established on a contractual basis or by applicable law, for example, data sharing agreements with OCC and FDIC. Information subject to the attorney-client privilege.
- Information received or obtained by the Board but subject to confidentiality or other specific obligations under a contract or by applicable law (e.g., Privacy Act).
- Personally Identifiable Information which is subject not only to the requirements in this document but also to the Board's [Policy for Handling Personally Identifiable Information](#).

## 2.0 Scope

### Coverage

- Other than as set forth in this Section 2.0 and Section 1.0 (above), this standard applies to all information of the Board in any form, including printed or digital form.
- Fiscal agency (Treasury) information, including Sensitive But Unclassified (SBU) and Personally Identifiable Information (PII), subject to Treasury handling requirements
- This Standard does not apply to information that is classified for national security purposes as defined in [Executive Order 12958](#) (as amended).
- The Office of Board Members (BDM) has developed processes and procedures for the handling of Board classified information during the embargo process of officially releasing information to the press. These processes and procedures are documented in the Public Affairs Embargoed Information Handbook. During the embargo process, the Handbook is the governing handling document.

### 3.0 Definitions

<b>Digital Information</b>	Information that is electromagnetically stored on non-paper, computer readable media such as, but not limited to, computer hard drives, DVD, CD, Zip disks, floppy disks, USB flash drives.
<b>Fiscal Agent Information</b>	Information managed by a Reserve Bank acting as fiscal agent of the Treasury, such as the Treasury Web Application Infrastructure and other business lines operated on behalf of Treasury's Bureau of the Fiscal Service and the Office of the Fiscal Assistant Secretary.
<b>Fixed Media</b>	Media that is stationary and not easily moved, i.e. internal hard drive.
<b>Federal Reserve Board Staff</b>	Employees, contractors, or any other person who performs work for or provides service to the Board.
<b>Information Owner</b>	Persons within the Board's divisions or offices and/or the business sections within the division or office that are responsible for the information they use and for making decisions regarding the classification, protection and use of that information within the section, division, office, Board and, to the extent permitted by Board policy and consistent with law, outside the Board by third parties. The Information Owner ensures the Information System Owners of information systems which utilize the Information Owner's information have implemented the appropriate security controls.
<b>Media</b>	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

<b>Mobile Devices</b>	Computer devices that are easily moved, e.g., a laptop or a handheld device such as a smartphone or tablet.
<b>Mobile Storage Devices</b>	<p>A subset of Mobile Devices which are hardware-based, portable devices with internal storage that can be easily attached or removed from PCs. Examples include:</p> <ul style="list-style-type: none"> <li>• USB flash drives</li> <li>• Portable hard drives</li> <li>• Digital audio players (e.g., Mp3 players)</li> <li>• Flash memory cards (e.g., Secure Digital (SD))</li> <li>• Tablets</li> <li>• Smartphones</li> </ul>
<b>NIST SP</b>	National Institute of Standards and Technology Special Publication.
<b>Non-public Information</b>	Information, whether in printed, digital, or any other form, that individuals learn by reason of Board employment or work for the Board and that the Board has not yet disclosed to the general public or authorized to be disclosed.
<b>Non-Sensitive PII</b>	Personally identifiable information unlikely to lead to identity theft and whose loss the Board has determined will not have a serious or greater impact.
<b>Personally Identifiable Information (PII)</b>	Information in printed or digital form maintained by the Board (or a Reserve Bank or contractor on behalf of the Board to accomplish a Board function) about an individual, including a member of the public as well as a current, former, or prospective Board or Federal Reserve Bank employee or contractor. PII generally means any information that identifies or describes a particular individual and includes, but is not limited to, an individual's name combined with other personal information such as the



individual's social security number, driver's license number, birth date, place of birth, account numbers, passwords (including mother's maiden name) or security codes (including biometric records) as well as any other personal information that is linked to or can be linked to an individual. PII also includes information on an individual's education, financial transactions, medical history, and criminal or employment history that may lead to identity theft. Reference: Board's Policy for Handling Personally Identifiable Information.

**Printed Information**

Media that is in paper form.

**Removable Media**

Digital media that is removable from a device. For example, tape, CD-R, DVD+RW, or USB storage device, such as a flash drive.

**Sensitive PII**

Personally identifiable information that if lost or misused has the potential to cause serious harm to an individual or to the Board's mission or operations. A Social Security number (in combination with other information connected to an individual's name) is an example of Sensitive PII. Reference: Board's Policy for Handling Personally Identifiable Information.

**Trusted Third Party**

Trusted Third Parties are defined as third parties with whom the Board (itself or through a specific division/office) has a formal agreement regarding the handling, storage, and protection of information and computing assets. Examples of trusted third parties include: the Federal Reserve Banks, select FFIEC agencies, and select state banking regulators. Divisions maintain their own list of division-specific trusted third parties.

**User** Any individual who has authorized access to Board Information and Information Systems as those terms are defined in the Board Information Security Program document.

## 4.0 General Controls

### Overview

Information is created or obtained in printed or digital form and its handling and use must adhere to the controls identified for the specific format in which the information resides. As an example, a hand-written document would adhere to the controls identified for “Printed Information,” while information stored on a USB flash drive would adhere to the controls identified for “Digital Information.”

1. Using the seven levels of sensitivity (Board handling classifications), the Information Owner is required to assign a Board handling classification level (set out in section 5.0 below) when he or she creates the information or obtains non-public information from outside the Board.
2. When the Information Owner removes information from long-term storage, he or she must review the Board handling classification for the information and determine if a reclassification of the information is appropriate. The Information Owner may also reclassify the information whenever he or she believes a reclassification is warranted.
3. All information, other than information classified Public/Official Release, may not be distributed outside of the Board unless it is authorized by the Board’s regulations and policies and the distribution is consistent with applicable law (See section 5.4 for more information).

## 5.0 Classifications

### Board Handling Classifications

Other than as provided in this Standard, all Board information (whether printed or digital form) must be designated by the Information Owner using the seven Board handling classifications described below. Only the Information Owner may declassify or change the classification of information or a document that contains the information. For the classification levels where the classification name has changed or been replaced, the new classification must be used for all email classification purposes. Until the same requirement is put in place for documents and information systems (or other digital media), they may be labeled with either the old or the new classification name. In order from most sensitive to the least sensitive, the Board handling classification levels are:

1. *Restricted-Controlled FR* - applies to information that, if disclosed to or modified by unauthorized individuals, might result in the risk of serious monetary loss, serious productivity loss, or cause a serious negative impact to the Board's ability to perform its mission. This designation rather than the designation of Restricted FR is appropriate where the Information Owner determines the dissemination of the information must be limited to a specific group of individuals. This designation may potentially include PII about non-Board or Federal Reserve Bank individuals.
2. *Restricted FR* - applies to information that, if disclosed to or modified by unauthorized individuals, might result in the risk of significant monetary loss, significant productivity loss, or cause a significant negative impact to the Board's ability to perform its mission. This designation may potentially include PII or Sensitive PII about non-Board or FRS individuals.
3. *Sensitive Personally Identifiable Information (SPII FR)*<sup>1</sup> - applies to information about an individual, including a member of the public or a current, former, or prospective Board or Federal Reserve Bank employee or contractor that, if lost or misused, has the potential to cause serious harm to an individual or to the Board's missions or operations. Examples of SPII FR include, but are not limited to, the following information that is linked or linkable to an individual when combined with the individual's name or other identifier:
  1. Social Security number, driver's license number, passport number, or other government-issued identification number;
  2. A bank account number or credit or debit card number, in addition to any required security code, access code, or password that would permit access to a person's financial account;
  3. Medical records; and
  4. Investigative records, including law enforcement and background check.

---

<sup>1</sup> The term SPII FR is replacing Board Personnel for e-mail classification purposes. In the near future, SPII FR will also replace Board Personnel for all document and information system classification purposes. In the interim, either classification (SPII FR or Board Personnel) may be used for documents and information systems (or other digital media).

The SPII FR designation is also appropriate where other PII is used or combined in such a manner that it could lead to identity theft or other serious harm or serious invasion of personal privacy if lost, misused, or subject to unauthorized disclosure. To the extent PII or Sensitive PII about a member of the public is contained in supervisory materials, the Restricted FR designation should be utilized.

4. *Internal FR/Official Use* - applies to information that has not been officially declassified and that does not meet the risk criteria for higher information classifications and that, if disclosed to or modified by unauthorized individuals, might result in the risk of some monetary loss, some productivity loss, or some embarrassment to the Board.

INTERNAL FR/OFFICIAL USE also applies to:

- Non-sensitive Personally Identifiable Information (PII).
- Communications with vendors and other external parties that involves information that would be classified as Internal FR/Official Use if communicated inside the Board.

5. *Public/Official Release (only used for e-mail communications)* – Applies to information that an authorized official of the Board has released for publication including information that represents the official position of the Board.

6. *Non-confidential (only used for e-mail communications)* - Applies to information related to the business of the Board or is created as part of a FR staff's work for the Board which does not meet the criteria for INTERNAL FR/OFFICIAL USE or higher classifications, and that, if disclosed, would not result in any monetary loss, productivity loss, or embarrassment to the Board. This would include information cleared by authorized staff for unrestricted external dissemination but that does not represent the official position of the Board. Examples could include economic research papers that do not influence Federal Open Market Committee (FOMC) or Supervision policies.

7. *Personal/Non-work (only used for e-mail communications)* – applies to information that is not related to Board work including personal information

## Non-Board Handling Classifications

1. *Treasury SBU (only used for e-mail communications)* – applies to Treasury Fiscal Services information that is classified as sensitive but unclassified per [Treasury policy](#).
2. *Treasury Unclassified (only used for e-mail communications)* – applies to Treasury Fiscal Services information that is not sensitive or does not rise to the level of being labelled *Treasury SBU* per [Treasury policy](#).

## BISP Impact Levels (FIPS 199 classifications)

1. In addition to classifying information for handling purposes as described above, the Information Owner must also classify the information for information security purposes as required by the Board Information Security Program (BISP). The BISP security classification process requires all Board information to be classified into three levels—Low, Moderate, or High—based on the potential impact to the Board should events occur that jeopardize the Confidentiality, Availability or Integrity of the information.
2. To determine the BISP impact level, the Information Owner must assign risk impact levels to the information in the three security objectives—Confidentiality, Availability, and Integrity—along with an overall impact level for the information. (*For more information, see Board Information the [Security Categorization spreadsheet](#)*).
3. The impact levels the Information Owner assigns to the information are then used to determine the minimum set of BISP controls and requirements that apply to the information.

## Interplay between Board handling classification and BISP impact levels

1. While the Board handling classification level and BISP impact levels are separate and distinct types of classifications, the two classifications overlap to the extent they both concern the confidentiality of the information. Thus, BISP impact levels correspond to the Board handling classifications as follows:
  - Low for Confidentiality = Internal FR/Official Use
  - Moderate for Confidentiality = Restricted FR, SPII, or Restricted-Controlled FR
  - High for Confidentiality = Restricted-Controlled FR
2. The Information Owner must assign both a BISP impact level and a Board handling classification to the information.

3. The controls that apply for each Board classification (section 6.0) have been mapped to the NIST SP 800-53 (current version) Media Protection (MP) control family. If the Information Owner meets the requirements of this standard, the Information Owner also complies with the BISP requirements for protecting the confidentiality of the information.

## Disclosure of Information

Only Board information that is rated Public/Official Release or Non-confidential may be disclosed outside of the Board including by a Reserve Bank. All other information is non-public information and as such cannot be disclosed in any form (printed, digital, symbols, formulas, codes, etc.) regardless of the medium used to communicate the information without authorization. This means that non-public information may not be disclosed without approval through mechanisms such as e-mail, phone calls, texts, word of mouth, social media (including but not limited to, Facebook, LinkedIn, and Twitter).

Non-public information of the Board may be distributed outside of the Board or the Reserve Banks by authorized staff only to the extent permitted by the Board's regulations, policies, and applicable law. These regulations, policies, and laws include, but are not limited to:

- The Board's Rules Regarding Availability of Information (12 CFR part 261);
- The Board's Rules Regarding Access to Personal Information Under the Privacy Act of 1974 (12 CFR part 261a);
- The Right to Financial Privacy Act of 1978 (12 USC 3401 et seq.);
- The Privacy Act of 1974 (5 USC 552a);
- The Freedom of Information Act (FOIA) (5 USC 552); and
- Removal of Board Information by Departing Personnel policy.

Requests from members of the public for the release of non-public including unpublished information must be referred to the Board's Freedom of Information Office for response. All other requests for release of non-public including unpublished information, including requests by other agencies, must be referred to the Board's General Counsel for response.

When the Information Owner makes an authorized release of the information to the public, the information will automatically be reclassified as Public/Official Release.

## 6.0 Restricted-Controlled FR

### Restricted-Controlled FR Printed Information

(BISP impact level-- High or Moderate for Confidentiality)

#### *MP-2: Media Access*

1. A list of the specific FR Staff authorized to have access to the information for official business purposes must be prepared and the list must be either attached to the document(s) or be centrally maintained by an authorized authority.
2. Duplication of Restricted-Controlled FR documents is not recommended. If duplication is necessary, each copy must include a unique identifier.

#### *MP-3: Media Labeling*

3. Documents must be clearly stamped or labeled with "Restricted-Controlled FR" at the top of every page, including any cover memoranda or title pages. All pages must be numbered using the "x of y" (e.g., 2 of 20) numbering or be consecutively numbered with the final page labeled "last page." Upon the inclusion of Restricted-Controlled FR information into the document, whether the document is in draft or final form, the document must be labeled following "Restricted-Controlled FR" labeling guidelines.
4. All Restricted-Controlled FR documents must be accompanied with a Restricted-Controlled FR blue coversheet. The coversheet must be placed on top of the document(s) and attached by staple, paper clip or equivalent when printed, delivered, or stored in a physical location.

#### *MP-4: Media Storage*

5. Storage of Restricted-Controlled FR documents requires one of the following physical controls: locked in a desk drawer; locked in a file cabinet; or kept in a locked office.

#### *MP-5: Media Transport*

6. Restricted-Controlled FR documents to be delivered through internal mail or messenger must be either hand-delivered to an authorized recipient or placed within two sealed envelopes. The innermost envelope must be labeled as "Restricted-Controlled FR."
7. Restricted-Controlled FR documents to be delivered through an external delivery service must be placed within two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking and confirmation. The sender must maintain a list of specific items containing Restricted-Controlled FR that were shipped in order to assist in follow up activities if the shipment is lost or stolen.
8. Restricted-Controlled FR documents may only be sent via encrypted fax machine and confirm receipt.

#### *MP-6: Media Sanitization & Disposal*

9. Restricted-Controlled FR documents must be physically destroyed in a manner that precludes disclosure or reconstruction, for example, paper shredders or approved secure document receptacles.

## **Restricted-Controlled FR Digital Information<sup>2</sup>**

(BISP impact level-- High or Moderate for Confidentiality)

#### *MP-2: Media Access*

---



1. A list of the specific FR Staff authorized to have access to the information for official business purposes must be prepared and the list must be either directly attached to the media or be centrally maintained by an authorized authority.
2. Duplication of Restricted-Controlled FR information on digital media is not recommended. If necessary, each copy must include a unique identifier.

#### *MP-3: Media Labeling*

3. A label indicating that the data or digital information is Restricted-Controlled FR must be provided when the information is accessed or displayed. For example, this includes a label being within the header of a document or at the top of every page or screen of web content. Removable media containing Restricted-Controlled FR must be clearly labeled "Restricted-Controlled FR."

#### *MP-4: Media Storage*

4. Storage of Restricted-Controlled FR information on removable media or mobile device requires one of the following physical controls: locked in a desk drawer, locked in a file cabinet or kept in a locked office.
5. Restricted-Controlled FR information may only be stored on fixed media or mobile device which is owned by the Board or Trusted Third Party and which is encrypted using an encryption module that is FIPS-140-2 certified.

#### *MP-5: Media Transport*

6. Restricted-Controlled FR information may only be removed or transported on removable media or a mobile device that is encrypted using an encryption module that is FIPS-140-2 certified.
7. Restricted-Controlled FR information stored on encrypted removable media or mobile device that is to be delivered through internal mail or messenger must be either hand-delivered to an

authorized recipient or placed within two sealed envelopes. The innermost envelope must be labeled as "Restricted-Controlled FR."

8. Restricted-Controlled FR information stored on encrypted removable media or mobile device that is to be delivered through an external delivery service must be placed within two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking and confirmation. Sender must maintain a list of specific items containing Restricted-Controlled FR that were shipped in order to assist in follow up activities if the shipment is lost or stolen.
9. E-mail transmission of Restricted-Controlled FR information in digital form internal to the Federal Reserve System must be sent following the process identified in Section 11: E-mail Security. E-mails sent outside the Federal Reserve System must be encrypted using a Board-approved encrypted e-mail solution such as (b)(7)(E)
  - The message body of the e-mail must provide an indicator on the first line of the e-mail message body (**not the subject line**) indicating that information within the e-mail is Restricted-Controlled FR data. If the Restricted-Controlled FR data are contained in the attachment of the e-mail, add additional text on the second line indicating that the attachment contains Restricted-Controlled FR data.
10. E-mails containing Restricted-Controlled FR information must not be forwarded using automated mechanisms (e.g., e-mail forwarding rules) to non-FRS owned or leased resources.
11. Restricted-Controlled FR information must not be communicated using non-FRS owned social media tools (e.g., Twitter, Facebook, LinkedIn)

#### *MP-6: Media Sanitization & Disposal*

12. Restricted-Controlled FR information stored on removable or fixed media that is to be disposed of or reused must be handled according to the *Media Sanitation and Disposal Policy and Procedures*.

## 7.0 Restricted FR

### Restricted FR Printed Information

(BISP impact level-- Moderate for Confidentiality)

#### *MP-2: Media Access*

1. Restricted FR information may only be shared with other FR staff who are authorized and have a need to know the information for official business purposes. Access to the Restricted FR must be limited to as few people as possible.
2. Duplication is limited to a "need to know."

#### *MP-3: Media Labeling*

3. Documents must be clearly stamped or labeled with "Restricted FR" at the top of every page, including any cover memo. All pages must be numbered using the "x of y" (e.g., 2 of 20) numbering or be consecutively numbered with the final page labeled "last page." Upon the inclusion of Restricted FR information into the document, whether the document is in draft or final form, the document must be labeled following "Restricted FR" labeling guidelines."
4. All Restricted FR documents must be accompanied with a Restricted FR pink coversheet. The coversheet must be placed on top of the document(s) and attached by staple, paper clip, or equivalent when printed, delivered, or stored in a physical location.

#### *MP-4: Media Storage*

5. Storage of Restricted FR information requires one of the following physical controls: locked in a desk drawer; locked in a file cabinet; or kept in a locked office.

6. Restricted FR information may only be stored on fixed media or mobile device which is owned by the Board or Trusted Third Party and which is encrypted using an encryption module that is FIPS-140-2 certified.-

*MP-5: Media Transport*

7. Restricted FR documents to be delivered through internal mail or messenger must be either hand-delivered to an authorized recipient or placed within a sealed envelope.
8. Restricted FR documents to be delivered through external delivery service must be placed within two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking and confirmation.
9. Restricted FR documents may only be sent via encrypted fax machine and confirm receipt.

*MP-6: Media Sanitization & Disposal*

10. Restricted FR documents must be physically destroyed in a manner that precludes disclosure or reconstruction, for example, paper shredders or secure document receptacles.

## Restricted FR Digital Information<sup>3</sup>

(BISP impact level-- Moderate for Confidentiality)

*MP-2: Media Access*

1. Share Restricted FR with other FR staff who are authorized and have a need to know the information for official business purposes. Limit access to the Restricted FR to as few people as possible.

---

<sup>3</sup> This section applies to information stored on portable digital media such as CD, DVD, ZIP disks, floppy disks, USB flash drives, and portable hard drives.

2. Duplication is limited to a “need to know.”

*MP-3: Media Labeling*

3. A label indicating that the data or digital information is Restricted FR must be provided when the information is accessed or displayed. For example, this includes a label within the header of an electronic document or at the top of a screen or page of web content. Removable media containing Restricted FR information must be clearly labeled “Restricted FR.”

*MP-4: Media Storage*

4. Storage of Restricted FR information on removable media or a mobile device requires one of the following physical controls: locked in a desk drawer, locked in a file cabinet or kept in a locked office.
5. Restricted FR information may only be stored on fixed media or mobile device which is owned by the Board or Trusted Third Party.

*MP-5: Media Transport*

6. Restricted FR information may only be removed or transported on removable media or a mobile device that is encrypted using an encryption module that is FIPS-140-2 certified..
7. Restricted FR information on encrypted removable media or mobile device that is to be delivered through internal mail or messenger must be either hand-delivered to an authorized recipient or placed within a sealed envelope.
8. Restricted FR information on encrypted removable media or mobile device that is to be delivered through external mail must be placed within two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking and confirmation.

9. E-mail transmission of Restricted FR information in digital form internal to the Federal Reserve System must be sent following the process identified in Section 11: E-mail Security. E-mails sent outside the Federal Reserve System must be encrypted using a Board-approved encrypted e-mail solution such as (b)(7)(E)
  - The message body of the e-mail (**not the subject line**) must provide an indicator that the message or attachment(s) contains Restricted FR data.

*MP-6: Media Sanitization & Disposal*

10. Restricted FR information stored on removable or fixed media that is to be disposed of or reused must be handled according to the *Media Sanitation and Disposal Policy and Procedures*.
11. E-mails containing Restricted FR information must not be forwarded using automated mechanisms (e.g., e-mail forwarding rules) to non-FRS owned or leased resources.

## 8.0 Sensitive Personally Identifiable Information (SPII FR)

### Sensitive Personally Identifiable Printed Information

(BISP impact level-- Moderate for Confidentiality)

*MP-2: Media Access*

1. SPII may be shared with FR staff or a Board contractor only as provided in the Board's Policy for Handling Personally Identifiable Information policy. Access to Sensitive Personally Identifiable Information must be limited to as few people as possible.
2. Duplication is limited to a "need to know."

*MP-3: Media Labeling*

3. Documents must be conspicuously stamped or labeled as "Sensitive Personally Identifiable Information" at the top of every page. All pages must be consecutively numbered. Upon the inclusion of Sensitive Personally Identifiable Information into the document, whether the document is in draft or final form, the document must be labeled following "Sensitive Personally Identifiable Information" labeling guidelines.
4. All SPII FR documents must be accompanied with a Sensitive Personally Identifiable Information green coversheet. The coversheet must be placed on top of the document(s) and attached by staple, paper clip or equivalent when delivered or stored in a physical location.

*MP-4: Media Storage*

5. Storage of SPII FR information requires one of the following physical controls: locked in a desk drawer; locked in a file cabinet; or kept in a locked office.

*MP-5: Media Transport*

6. SPII FR documents to be delivered through internal mail or messenger must be either hand-delivered to an authorized recipient or placed within a sealed envelope.
7. SPII FR documents to be delivered through external delivery service must be placed within two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking and confirmation. The sender must maintain a list of specific items containing Sensitive Personally Identifiable Information that were shipped in order to assist in follow up activities if the shipment is lost or stolen. If the sender determines that tracking the shipment and maintaining a list of the specific items is not possible or would prevent the execution of an essential Board function, the sender may choose another appropriate method for shipping so long as he or she uses compensating controls to the extent possible.

8. SPII FR Information may only be sent via a secure fax unless the person the information concerns specifically authorizes the non-secure fax communication or unless doing so is not possible and would prevent the execution of an essential Board function or activity. When using secure fax is not possible, the transmitter must use compensating controls (for example, sending the fax only if the recipient is present and confirming receipt) to the extent possible.

*MP-6: Media Sanitization & Disposal*

9. SPII FR documents must be physically destroyed in a manner that precludes disclosure or reconstruction, for example, paper shredders or secure document receptacles.

## **Sensitive Personally Identifiable FR Digital Information<sup>4</sup>**

(BISP impact level-- Moderate for Confidentiality)

*MP-2: Media Access*

1. SPII FR may be shared with FR staff or a Board contractor only as provided in the Board's Policy for Handling Personally Identifiable Information policy. Access to Sensitive Personally Identifiable Information must be limited to as few people as possible.
2. Duplication is limited to a "need to know."

*MP-3: Media Labeling*

---

<sup>4</sup> This section applies to information stored on portable digital media such as CD, DVD, ZIP disks, floppy disks, USB flash drives, and portable hard drives. .



3. A label indicating that the data or digital information is SPII FR must be provided when the information is accessed or displayed. For example, this includes a label within the header of an electronic document or at the top of a screen or page of web content. Removable media containing Sensitive Personally Identifiable Information must be clearly labeled "Sensitive Personally Identifiable Information."

#### *MP-4: Media Storage*

4. Storage of SPII FR on removable media or mobile devices requires one of the following physical controls: locked in a desk drawer, locked in a file cabinet or kept in a locked office.
5. SPII FR may only be stored fixed media or mobile device which is owned by the Board or Trusted Third Party.

#### *MP-5: Media Transport*

6. SPII FR Information may only be removed or transported on removable media or mobile device that is encrypted using an encryption module that is FIPS-140-2 certified.
7. SPII FR Information on encrypted removable media or mobile device that is to be delivered through internal mail or messenger must be either hand-delivered to an authorized recipient or placed within a sealed envelope.
8. SPII FR Information on encrypted removable media or mobile device that is to be delivered through external mail must be placed within two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking and confirmation. The sender must maintain a list of specific items containing Sensitive Personally Identifiable Information that were shipped in order to assist in follow up activities if the shipment is lost or stolen. If the sender determines that tracking the shipment and maintaining a list of the specific items is not possible or would prevent the execution of an essential Board function, the sender may choose another appropriate method for shipping so long as he or she uses compensating controls to the extent possible.
9. E-mail transmission of SPII FR Information in digital form internal to the Federal Reserve System must be sent following the process identified in Section 14: E-mail Security. E-mails sent outside the Federal Reserve System must be encrypted using a Board-approved encrypted e-mail

solution such as (b)(7)(E) unless the person the information concerns specifically authorizes the unencrypted e-mail communication or unless doing so is not possible and would prevent the execution of an essential Board function or activity. When using encrypted e-mail is not possible, the transmitter must use compensating controls (for example, sending the e-mail only if the recipient is available and confirming receipt) to the extent possible.

- The message body of the e-mail (**not the subject line**) must provide an indicator that the message or attachment(s) contains Sensitive Personally Identifiable Information data.

10. E-mails containing SPII FR Information must not be forwarded using automated mechanisms (e.g., e-mail forwarding rules) to non-FRS owned or leased resources.

#### *MP-6: Media Sanitization & Disposal*

11. SPII FR Information stored on removable or fixed media that is to be disposed of, or reused, must be deleted according to the *Media Sanitation and Disposal Policy and Procedures*.

## 9.0 Internal FR/Official Use

### Internal FR/Official Use Printed Information

(BISP impact level—Low for Confidentiality)

#### *MP-2: Media Access*

1. Internal FR/Official Use may be shared with other FR staff who are authorized and who have a need to know the information for official business purposes.
2. Internal FR may be shared with a Reserve Bank employee or a Board contractor if you have authority to do so as a result of the position you hold or if you have been granted specific authority by your supervisor to share the information.

3. Duplication is limited to a “need to know.”

*MP-3: Media Labeling*

4. A label indicating that the data or digital information is Internal FR/Official Use must be provided when the information is accessed or displayed. For example, this includes a label within the header of an electronic document or at the top of a screen or page of web content. Removable media containing Internal FR/Official Use information must be clearly labeled “Internal FR/Official Use.”

*MP-4: Media Storage*

5. Storage of Internal FR/Official Use information on printed media must be stored in a secure location.

*MP-5: Media Transport*

6. Internal FR/Official Use documents to be delivered through external mail must be placed within a sealed envelope.

*MP-6: Media Sanitization & Disposal*

7. Internal FR/Official Use information on printed media must be physically destroyed in a manner that precludes disclosure or reconstruction, for example, paper shredders or secure document receptacles.

## Internal FR/Official Use Digital Information<sup>5</sup>

(BISP impact level-- Low for Confidentiality)

### *MP-2: Media Access*

1. Internal FR/Official Use information may be shared with other FR staff who are authorized and who have a need to know the information for official business purposes.
2. Internal FR/Official Use Information may be shared with a Reserve Bank employee or a Board contractor if you have authority to do so as a result of the position you hold or have been granted specific authority by your supervisor to share the information.
3. Duplication is limited to a "need to know."

### *MP-3: Media Labeling*

4. Removable media containing Internal FR/Official Use information must be clearly labeled as "Internal FR/Official Use". For example, this includes a label within the header of an electronic document.

### *MP-4: Media Storage*

5. Storage of Internal FR/Official Use information on removable media or mobile device requires one of the following physical controls: locked in a desk drawer, locked in a file cabinet or kept in a locked office.
6. Internal FR/Official Use information may only be stored on fixed media or mobile device which is owned by the Board or Trusted Third Party.

---

<sup>5</sup> This section applies to information stored on portable digital media such as CD, DVD, ZIP disks, floppy disks, USB flash drives, and portable hard drives.

#### *MP-5: Media Transport*

7. Internal FR/Official Use information on digital media that is to be delivered through external mail must be placed within a sealed envelope.
8. Internal FR/Official Use information may only be removed or transported on Board or Federal Reserve System-owned media.
9. E-mail transmission of Internal FR/Official Use information in digital form internal to the Federal Reserve System must be sent following the process identified in Section 14: E-mail Security.
10. E-mails containing Internal FR/Official Use information must not be forwarded using automated mechanisms (e.g., e-mail forwarding rules) to non-FRS owned or leased resources.

#### *MP-6: Media Sanitization & Disposal*

11. Internal FR/Official Use information stored on removable and fixed media that is to be disposed of, or reused, must be deleted according to the *Media Sanitation and Disposal Policy and Procedures*.

## **10.0 Nonconfidential**

See Section 14: E-mail and Calendar Security

## **11.0 Public/Official Release**

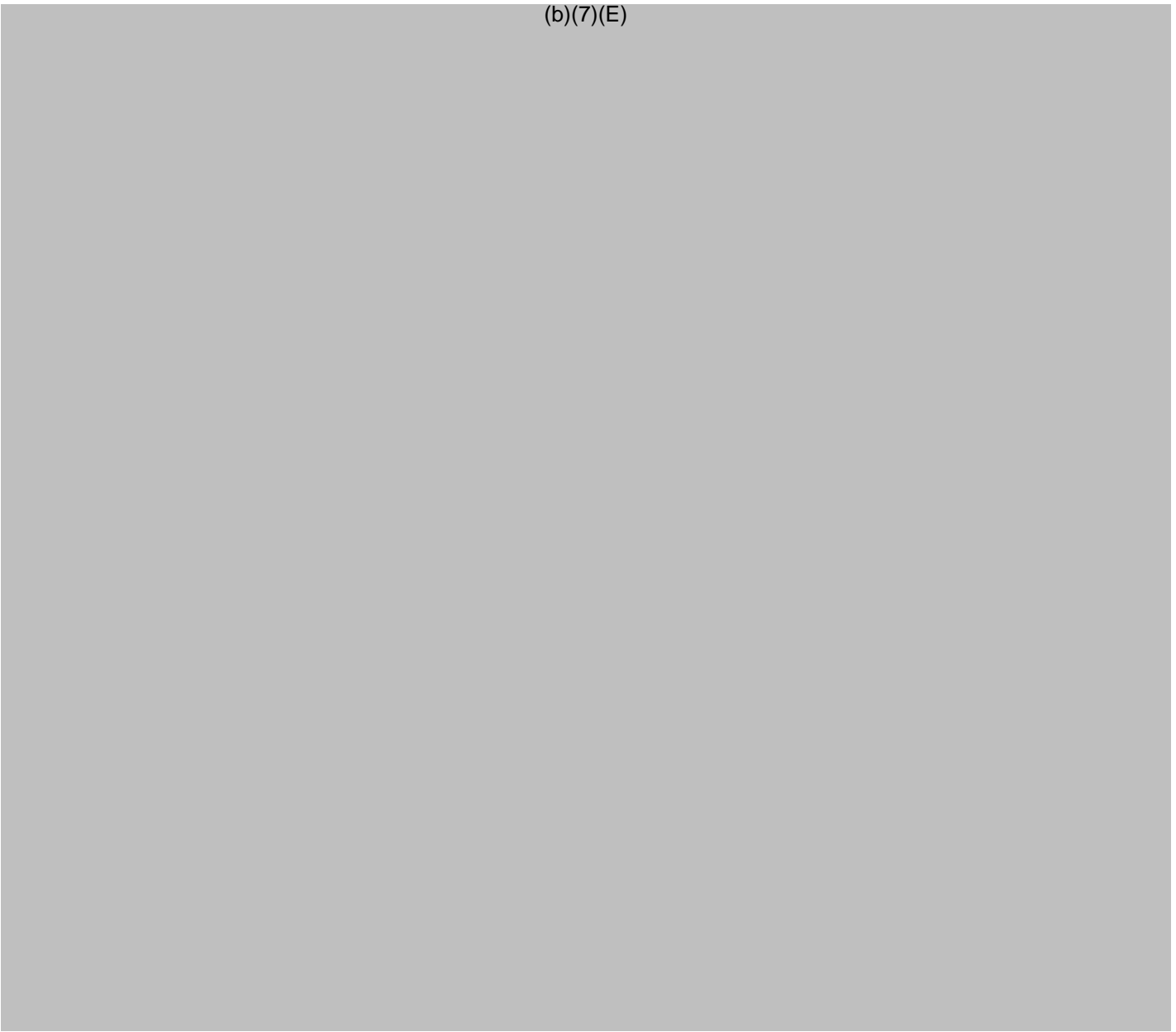
See Section 14: E-mail and Calendar Security

## **12.0 Personal/Non-work**


See Section 14: E-mail and Calendar Security

## **13.0 Mobile Storage Devices**

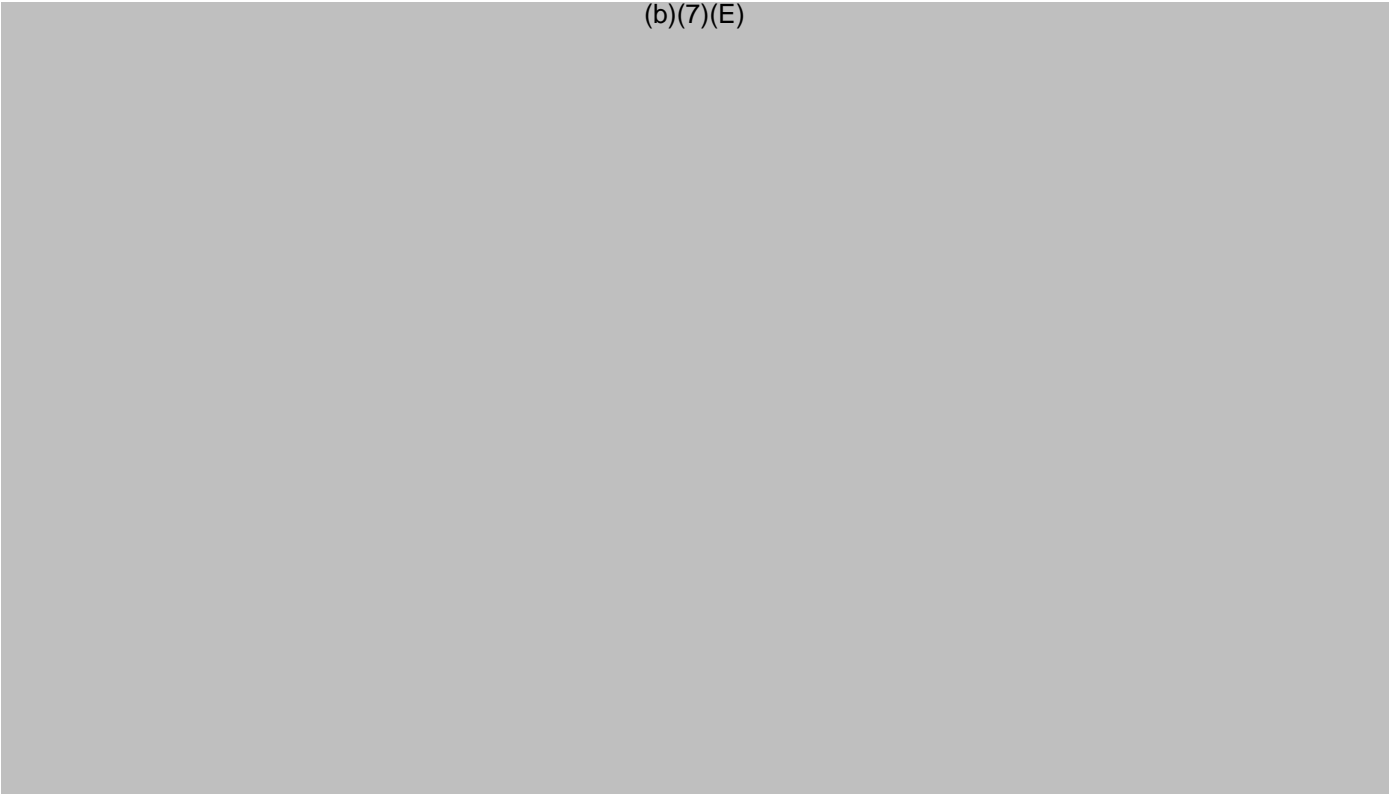
(b)(7)(E)



(b)(7)(E)

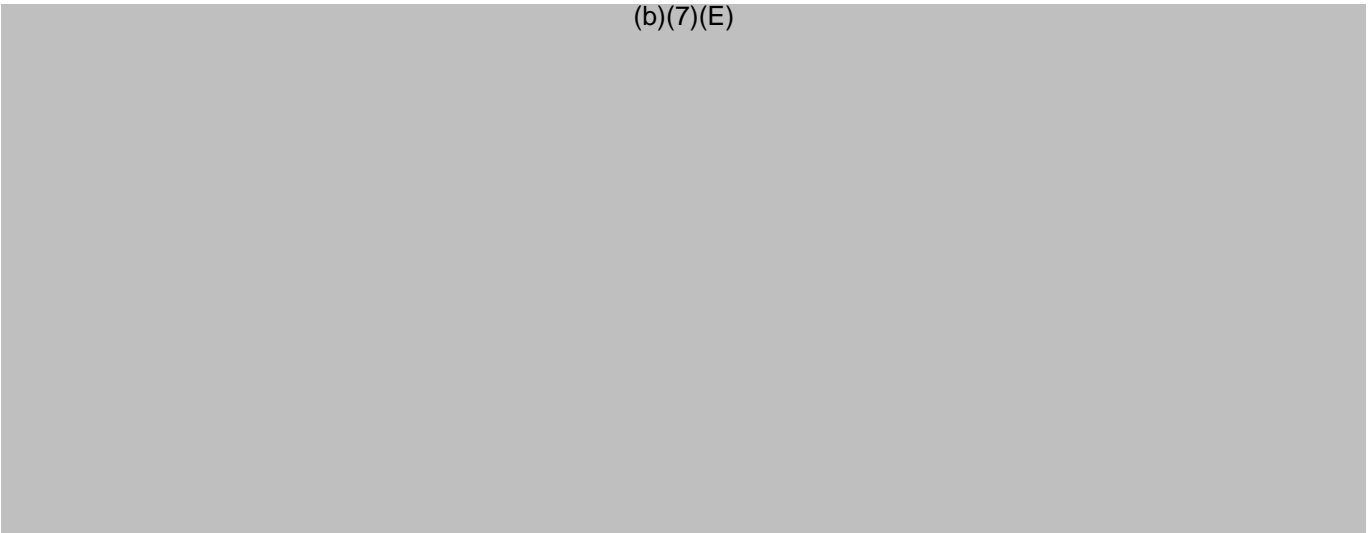


(b)(7)(E)




## **14.0 E-Mail and Calendar Security**

(b)(7)(E)

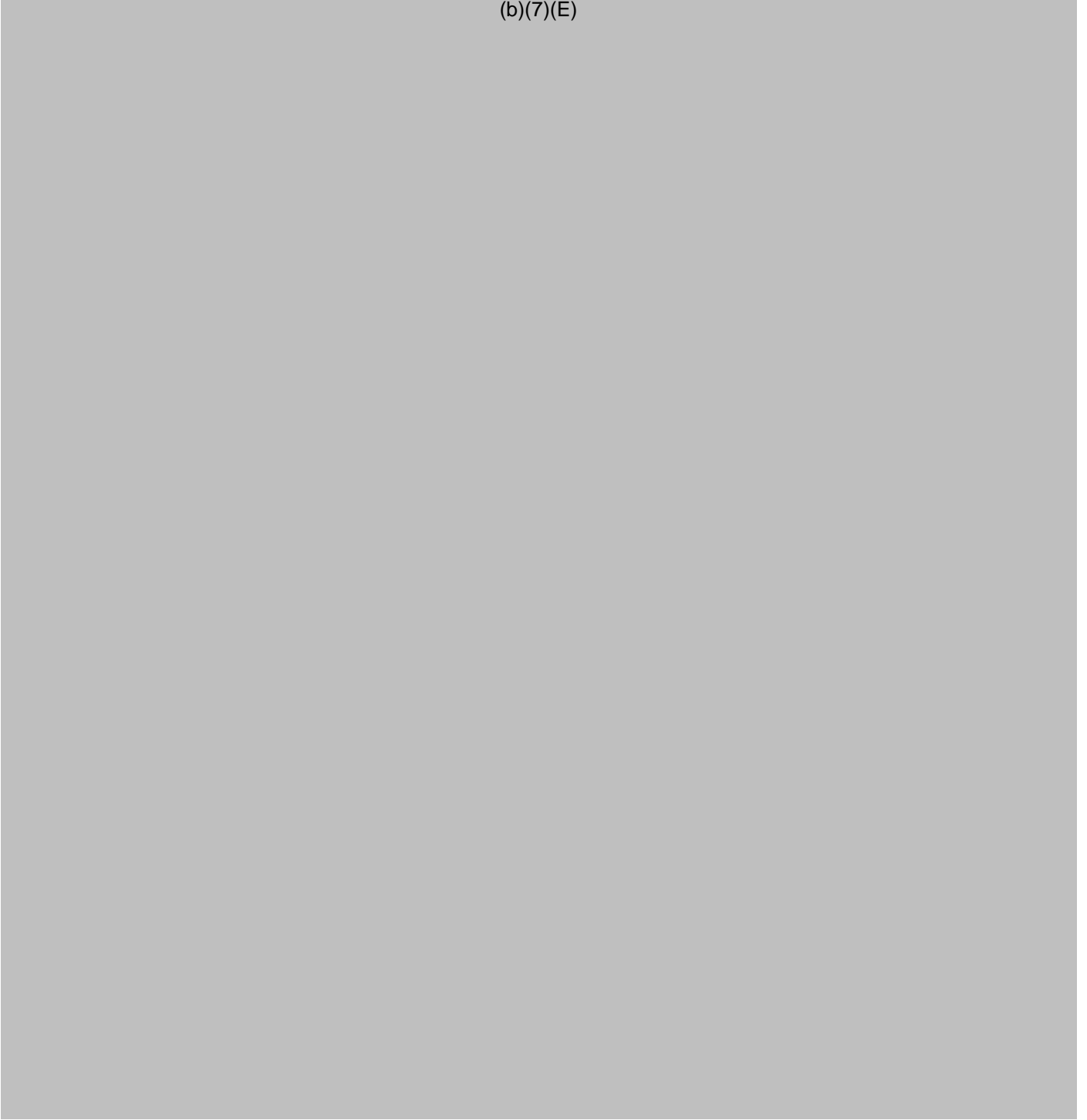




(b)(7)(E)



(b)(7)(E)



### **Attachment 1: Coversheets**

These coversheets must be placed on top of the document(s) and attached by staple, paper clip, or equivalent when printed, delivered, or stored in a physical location.

# RESTRICTED-CONTROLLED FR

HANDLE THE ATTACHED DOCUMENT IN ACCORDANCE  
 WITH THE FRB INFORMATION SECURITY PROGRAM.

## Use/Distribution

A list of the specific FR Staff authorized to have access to the information for official business purposes must be prepared and either attached to the document(s) or centrally maintained by an authorized authority.

## Labeling – “Restricted-Controlled FR”

Stamped or labeled at the top of each page.

## Page Numbering

“x of y” (e.g. 2 of 20) on each page **or** consecutively number each page with final page labeled “last page”.

## Duplication

Duplication is not recommended. If duplication is necessary, each copy must include a unique identifier.

## Packaging/Delivery/Transmission

Internal Mail or Messenger/FRB Pouch: Either hand deliver to an authorized recipient or place document within two sealed envelopes with innermost envelope labeled “Restricted-Controlled FR”

External Delivery Service: Place within two sealed envelopes and send via Registered Mail (or equivalent service) providing delivery tracking and confirmation. Maintain a list of shipped items in order to assist with follow-up activities if the shipment is lost or stolen.

Fax: Document must be sent via encrypted fax machine with confirmed receipt.

## Storage

Documents must be stored in a locked cabinet or desk.

## Destruction

Documents must be shredded or destroyed via incineration.

# RESTRICTED-CONTROLLED FR

Version 2.0, January 10, 2008

# RESTRICTED FR

**HANDLE THE ATTACHED DOCUMENT IN ACCORDANCE  
 WITH THE FRB INFORMATION SECURITY PROGRAM.**

## **Use/Distribution**

Share only with FR Staff who are authorized and have a need to know the attached information for official business purposes.

## **Labeling – “Restricted FR”**

Stamped or labeled at the top of each page.

## **Page Numbering**

“x of y” (e.g. 2 of 20) on each page or consecutively number each page with final page labeled “last page”.

## **Duplication**

Limited to need to know.

## **Packaging/Delivery/Transmission**

Internal Mail or Messenger/FRB Pouch: Either hand deliver to an authorized recipient or place document within a sealed envelope.  
External Delivery Service: Placed within two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking and confirmation.  
Fax: Document must be sent via encrypted fax machine with confirmed receipt.

## **Storage**

Documents must be stored in a locked office, cabinet, or desk.

## **Destruction**

Documents must be shredded or destroyed via incineration.

# RESTRICTED FR

Version 2.0, January 10, 2008



# BOARD PERSONNEL

HANDLE THE ATTACHED DOCUMENT IN ACCORDANCE  
 WITH THE FRB INFORMATION SECURITY PROGRAM.

## Use/Distribution

PII may be shared with FR staff or Board contractors only as provided in the Board's Policy for Handling Personally Identifiable Information. Access to Board Personnel must be limited to as few people as possible.

## Labeling – "Board Personnel"

Stamped or labeled at the top of each page.

## Page Numbering

Number each page consecutively.

## Duplication

Limited to need to know.

## Packaging/Delivery/Transmission

Internal Mail or Messenger/FRB Pouch: Either hand deliver to an authorized recipient or place document within a sealed envelope.  
External Delivery Service: Placed within two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking and confirmation.

Fax: If machine is in a secure location, such as a locked room, confirm receipt when sending. If the machine is not in a secure location, send and receive only when a recipient is present and confirm receipt when sending.

## Storage

Documents must be stored in a locked office, cabinet, or desk.

## Destruction

Documents must be shredded or destroyed via incineration.

# BOARD PERSONNEL

Version 3.0, January 10, 2008

## Attachment 2-A: Summary for Handling Printed Information

PRINTED	Restricted-Controlled FR <sup>6</sup>	Restricted FR <sup>7</sup>	Sensitive Personally Identifiable Information (Sensitive PII)	Internal FR/Official Use <sup>8</sup> (including Non-Sensitive PII)
<b>MP-2 Access</b>	A list of the specific FR Staff authorized to access the information must be prepared & attached to the document(s) or centrally maintained by an authorized authority	Authorized and need to know for official business purposes and limited to as few people as possible.	Share only as provided in the Board's Policy for Handling Personally Identifiable Information policy and limited to as few people as possible	Authorized & need to know for official business purposes. PII may be shared with a FRS employee or Board contractor if authorized by the Board employee's supervisor or the employee's position
<b>MP-2 Duplication</b>	Not recommended. If necessary, each copy must have a unique identifier	Limited to need to know	Limited to need to know	Limited to need to know
<b>MP-3 Labeling</b>	"Restricted-Controlled FR" at the top of every page. Numbered using the "x of y" numbering or consecutively numbered w/ the final page labeled "last page"	"Restricted FR" at the top of every page. Numbered using the "x of y" numbering or consecutively numbered w/ the final page labeled "last page"	"Sensitive Personally Identifiable Information" at the top of every page. All pages must be consecutively numbered	"Internal FR/Official Use" at the top of the first page. All pages must be consecutively numbered
<b>MP-3 Coversheet</b>	Restricted-Controlled FR blue coversheet	Restricted FR pink coversheet	Sensitive Personally Identifiable Information green coversheet	No coversheet
<b>MP-4 Storage</b>	1 of the following physical controls: locked desk drawer, file cabinet or office	1 of the following physical controls: locked desk drawer, file cabinet or office	1 of the following physical controls: locked desk drawer, file cabinet or office	Stored in a secure location
<b>MP-5 Transport: Internal</b>	Hand-delivered or placed within two sealed envelopes. The innermost envelope labeled as "Restricted-Controlled FR."	Hand-delivered or placed within a sealed envelope	Hand-delivered or placed within a sealed envelope	No special requirements
<b>MP-5 Transport: External</b>	Two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking & confirmation. Sender must maintain a list of specific items containing Restricted-Controlled FR that were shipped	Two sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking & confirmation.	2 sealed envelopes & sent via Registered Mail providing delivery tracking & confirmation. Sender must maintain a list of specific items containing Sensitive PII that were shipped. When tracking is not used, the transmitter must use compensating controls to the extent possible.	Placed within a sealed envelope
<b>MP-5 Transport: Fax</b>	Sent via encrypted fax machine and confirm receipt	Sent via encrypted fax machine and confirm receipt	Sent via encrypted fax machine & confirm receipt. When using non-secure fax, the transmitter must use compensating controls to the extent possible.	No special requirements

<sup>6</sup> FOMC Documents are labeled *Class I FOMC- Restricted Controlled (FR)*

<sup>7</sup> FOMC Documents are labeled *Class II FOMC – Restricted (FR)*

<sup>8</sup> FOMC Documents are labeled *Class III FOMC – Internal FR/Official Use*

<b>MP-6 Sanitization &amp; Disposal</b>	Physically destroyed (e.g., paper shredders or approved secure document receptacles)	Physically destroyed (e.g., paper shredders or approved secure document receptacles)	Physically destroyed (e.g., paper shredders or approved secure document receptacles)	Physically destroyed (e.g., paper shredders)
---	--	--	--	--

## Attachment 2-B: Summary for Handling Digital Information

<b>DIGITAL</b>	<b>Restricted-Controlled FR<sup>9</sup></b>	<b>Restricted FR<sup>10</sup></b>	<b>Sensitive Personally Identifiable Information (Sensitive PII)</b>	<b>Internal FR/Official Use<sup>11</sup> (including Non-sensitive PII)</b>
<b>MP-2 Access</b>	A list of the specific FR Staff authorized to access the information must be prepared & attached to the media or centrally maintained by an authorized authority.	Authorized and need to know for official business purposes and limited to as few people as possible.	Share only as provided in the Board's Policy for Handling Personally Identifiable Information policy and limited to as few people as possible	Authorized & need to know for official business purposes. PII may be shared with a FRS employee or Board contractor if authorized by the Board employee's supervisor or the employee's position
<b>MP-2 Duplication</b>	Not recommended. If necessary, each copy must have a unique identifier	Limited to need to know	Limited to need to know	Limited to need to know
<b>MP-3 Labeling</b>	Restricted-Controlled FR label must be provided when the information is accessed or displayed. Label Removable media "Restricted-Controlled FR"	Restricted FR label must be provided when the information is accessed or displayed. Label Removable media "Restricted FR"	Sensitive Personally Identifiable Information label must be provided when the information is accessed or displayed. Label Removable media "Sensitive Personally Identifiable Information"	Removable media labeled as "Internal FR/Official Use"
<b>MP-4 Storage</b>	1 of the following physical controls: locked desk drawer, file cabinet or office. Store only on Board or Trusted Third Party owned media that is encrypted using an encryption module that is FIPS-140-2 certified.	1 of the following physical controls: locked desk drawer, file cabinet or office. Store only on Board or Trusted Third Party owned media that is encrypted using an encryption module that is FIPS-140-2 certified.	1 of the following physical controls: locked desk drawer, file cabinet or office. Sensitive PII stored on portable media must be encrypted. Store only on Board or Trusted Third Party owned media that is encrypted using an encryption module that is FIPS-140-2 certified.	Store in a secure location. Store only on Board or FRS owned media.

<sup>9</sup> FOMC Digital Information, including E-mail is labeled *Class I FOMC - Restricted Controlled (FR)*

<sup>10</sup> FOMC Digital Information, including E-mail is labeled *Class II FOMC – Restricted (FR)*

<sup>11</sup> FOMC Digital Information, including E-mail is labeled *Class III FOMC – Internal FR/Official Use*



<b>DIGITAL</b>	<b>Restricted-Controlled FR<sup>9</sup></b>	<b>Restricted FR<sup>10</sup></b>	<b>Sensitive Personally Identifiable Information (Sensitive PII)</b>	<b>Internal FR/Official Use<sup>11</sup> (including Non-sensitive PII)</b>
<b>MP-5 Transport: Internal</b>	Transport on Board or Trusted Third Party owned encrypted portable media that is encrypted using an encryption module that is FIPS-140-2 certified and hand-deliver or place in 2 sealed envelopes. Innermost envelope labeled Restricted-Controlled FR	Transport on Board or Trusted Third Party owned encrypted portable media that is encrypted using an encryption module that is FIPS-140-2 certified and hand-deliver or place in a sealed envelope	Transport on Board or Third Party owned encrypted portable media that is encrypted using an encryption module that is FIPS-140-2 certified and hand-deliver or place in a sealed envelope	Transport only on Board or FRS owned media
<b>MP-5 Transport: External</b>	Transport on Board or Trusted Third Party owned encrypted removable media that is encrypted using an encryption module that is FIPS-140-2 certified in 2 sealed envelopes and sent via Registered Mail providing delivery tracking & confirmation. Sender must maintain a list of specific items containing Restricted-Controlled FR that were shipped	Transport on Board or Trusted Third Party owned encrypted removable media that is encrypted using an encryption module that is FIPS-140-2 certified in 2 sealed envelopes and sent via Registered Mail (or equivalent service) providing delivery tracking & confirmation.	Transport on Board or FRS owned encrypted removable media that is encrypted using an encryption module that is FIPS-140-2 certified in 2 sealed envelopes and sent via Registered Mail providing delivery tracking & confirmation. Sender must maintain a list of specific items that were shipped. When tracking is not used, the transmitter must use compensating controls to the extent possible.	Placed within a sealed envelope. Transport only on Board or FRS owned media.
<b>MP-5 Transport: E-mail</b>	Internal Recipients: Use "FRS Only" category (Reserve Bank users sending Class I FOMC information use the FOMC Classification)  External Recipients: Encrypt using Board approved encryption technologies. Use "Secure External" category. Class I FOMC must not be sent outside the FRS.	Internal Recipients: Use "FRS Only" category. (Reserve Bank users sending Class II FOMC information use the FOMC Classification)  External Recipients: Encrypt using Board approved encryption technologies Use "Secure External" category. Class II FOMC must not be sent outside the FRS.	Internal Recipients: Use "FRS Only" category  External Recipients: Encrypt using Board approved encryption technologies unless the person the information concerns specifically authorizes the unencrypted e-mail communication. Using unencrypted e-mail requires the transmitter to use compensating controls. Use "Secure External" category	Internal Recipients: Use "FRS Only" category  External: Use "Unsecured External" category
<b>MP-6 Sanitization &amp; Disposal</b>	Follow the Media Sanitation and Disposal Policy & Procedures	Follow the Media Sanitation and Disposal Policy & Procedures	Follow the Media Sanitation and Disposal Policy & Procedures	Follow the Media Sanitation and Disposal Policy & Procedures