Program for Security of FOMC Information

As amended effective January 26, 2016

I. INTRODUCTION.

The Program for Security of FOMC Information ("the Program") describes what confidential FOMC information is, how it is classified, who has access to it, how it should be handled, and who is responsible for ensuring that it is protected. Everyone with access to confidential FOMC information is required to review and abide by the rules described below.

These security procedures are not intended to preclude discussions within the Federal Reserve of important FOMC-related issues, including the general reasons for the Federal Open Market Committee's (the "Committee") decisions. Such discussions may be conducted for research purposes or for preparing briefings and other information for Committee members, but care should be taken that all discussion participants have the appropriate level of authorization if confidential information is being shared.

II. DEFINITION OF CONFIDENTIAL FOMC INFORMATION.

Confidential FOMC information includes all privileged information that comes into the possession of the Board members, Federal Reserve Bank presidents, or Federal Reserve System staff in the performance of their duties for, or pursuant to the direction of, the Committee. Such information covers, but is not limited to, expressions of policy views at Committee meetings, reasons for those views, votes of the Committee, and staff forecasts. The information that must be kept confidential may be in any form. It includes not only paper documents, but also electronic messages and files, recordings, notes, oral briefings, and discussions relating to confidential FOMC matters.

III. CLASSIFICATION OF CONFIDENTIAL FOMC INFORMATION.

There are three security classifications for confidential FOMC information. The first two classifications—"Class I FOMC – Restricted Controlled (FR)" and "Class II FOMC – Restricted (FR)"—apply to very sensitive FOMC information. Class I FOMC information must be handled at least as securely as material classified by the Federal Reserve Board as "Restricted Controlled (FR)." Access to Class II information is somewhat less restrictive than access to Class I. It must be treated at least as securely as material classified by the Federal Reserve Board as "Restricted (FR)." The classification "Class III FOMC – Internal (FR)" applies to less sensitive information that still requires confidential treatment. It must be handled at least as securely as material classified by the Federal Reserve Board as "Internal (FR)." (See Section VI below for handling requirements.)

Information in these classifications must be kept confidential until it is released to the public by the Chairman or by the Committee secretary pursuant to Committee instructions. All questions related to the classification, distribution, or handling of documents should be directed to the FOMC Secretariat.

A. "Class I FOMC – Restricted Controlled (FR)."

This classification is generally applied to information that includes policymaker input, e.g., information related to monetary policy decisions at meetings, nonpublic views expressed by policymakers on likely future policy, and identification of meeting participants who express particular views. Class I information includes, but is not limited to:

1. *Monetary Policy: Strategies and Alternatives* ("Tealbook B").
2. Minutes of Committee meetings, including drafts.
3. Committee meeting recordings and transcripts.
4. Portions of Committee meeting participants' prepared remarks that include material from Class I documents such as Tealbook B and other monetary policy alternatives under consideration.

5. Submissions by, or on behalf of, policymakers in the Summary of Economic Projections process.

6. Special memoranda or reports deemed particularly sensitive, including materials that might otherwise carry a Class II designation (e.g., a report from the manager containing information on sensitive foreign exchange operations).

B. "Class II FOMC – Restricted (FR)."

This classification is generally applied to Board staff forecasts prepared for the Committee and to information about open market operations. Class II information includes, but is not limited to:

1. *Economic and Financial Conditions: Current Situation and Outlook* ("Tealbook A"), and Board staff projections or assumptions relating to interest rates.

2. Reports of the manager on domestic and foreign open market operations.

3. Information on Desk operations posted on confidential portions of the "MarketSource" website of the Federal Reserve Bank of New York.

4. Other materials on economic and financial developments (including foreign), special memoranda, tables, and charts less sensitive than those in Class I, including briefing materials containing Class II information that are produced and circulated within the Board or individual Federal Reserve Banks.

C. "Class III FOMC – Internal (FR)."

This classification is generally applied to less-sensitive background information prepared by Board staff to support policy discussions. Class III information includes, but is not limited to:

1. Tealbook Data Sheets.

2. Committee meeting agendas.

D. Security Classification Downgrading of FOMC Information.

FOMC information loses its security classification when the Committee releases it to the public. Class II information is downgraded to Class III six months after the relevant Committee meeting. Additionally, Tealbook B and monetary policy alternatives documents are downgraded from Class I to Class II six months after the relevant Committee meeting, and from Class II to Class III one year after the relevant meeting.

IV. ACCESS TO CONFIDENTIAL FOMC INFORMATION WITHIN THE FEDERAL RESERVE SYSTEM.

Staff access to confidential FOMC information, which includes Class I, Class II, and Class III information, requires prior authorization. Before gaining access and annually thereafter, all Federal Reserve System persons, including office support staff, must receive, review, and agree to abide by the rules for handling confidential information that are referred to in this document.

At each Federal Reserve Bank, the president, or the research director on the president's behalf, is responsible for designating those persons to be given access to each class of information. At the Federal Reserve Bank selected by the Committee to execute open market transactions (the "Selected Bank"), the manager of the System Open Market Account ("SOMA") may also designate staff on behalf of the president. At the Board, that responsibility is assumed by the Chairman or the Chairman's designees and by Board members for their assistants. Access at the Selected Bank and the Board of Governors is limited on a strict "need-to-know" basis. Access at the other Federal Reserve Banks is also limited on a strict "need-to-know" basis and is subject to the numerical limits noted below. In complying with these limits, Federal Reserve Banks may designate different persons to have access to different documents. For example, one slot could be filled by designating an international economist as having access to all special memoranda relating to foreign currency operations, and a domestic economist as having access to other Class I and Class II memoranda. At each institution, access to Class I, Class II, and Class III information should be reviewed carefully at least once every year.

A. Access to "Class I FOMC – Restricted Controlled (FR)" materials at Federal Reserve Banks other than the Selected Bank (and the Federal Reserve Bank that serves as the backup site for open market operations) is restricted to the president and first vice president and to seven other Federal Reserve Bank personnel as well as a limited number of office support staff.

B. Access to "Class II FOMC – Restricted (FR)" materials at Federal Reserve Banks other than the Selected Bank (and the Federal Reserve Bank that serves as the backup site for open market operations) is restricted to the president and first vice president and to eleven other Federal Reserve Bank personnel as well as a limited number of office support staff.

C. Access to "Class III FOMC – Internal (FR)" information is limited on a "need-to-know" basis, but no specific limit is set on the number of persons who may have access to such information at each location.

D. The lists of all persons, including office support staff, who are authorized to have access to Class I, Class II, or Class III information are to be generated and transmitted to the FOMC Secretariat annually, after the first regularly scheduled Committee meeting of the year (at which any changes to the Program would typically be considered). Over the course of the year, changes resulting from new staff assignments should also be transmitted. Records of individuals' agreements to abide by the rules described in the Program should be maintained at each institution. Such records would include individuals' signatures or electronic equivalent.

E. To facilitate the preparation of special analyses and briefings within the System, eligible staff may be granted ad-hoc access to Class I and Class II information on a strict "need-to-know" basis for a specific and limited period of time. Such ad-hoc access may be granted by the president of a Federal Reserve Bank or a research director on his/her behalf or by the secretary for Board staff. Staff granted ad-hoc access must review and agree to abide by the rules described in the Program before receiving access. The FOMC Secretariat should be advised that such access has been given, and records of the access and related agreement should be maintained at each Federal Reserve Bank.

F. The Chairman may make ad-hoc exceptions to this section that are either more or less restrictive for particular documents being circulated or for other confidential information.

G. In order to provide secure and rapid document delivery, access to selected confidential FOMC information is given electronically through the Secure Document System ("SDS"). SDS access is restricted at each Federal Reserve Bank to the president and first vice president and up to seven other Federal Reserve Bank personnel. The Desk at the Selected Bank has access for four additional users at that Federal Reserve Bank. The president of each Federal Reserve Bank may delegate to the research director the responsibility for selecting users, monitoring compliance with SDS guidelines, and communicating with the FOMC Secretariat when changes in usage or other issues occur. Access to SDS for Board staff is authorized by a designee of the Chairman and monitored by the FOMC Secretariat.

H. Eligibility for access to confidential FOMC information for non-US citizens is, in all cases (including under IV.E), governed by 12 CFR 268.205 and by this Program. (A summary of this rule, as it pertains to FOMC information, is appended to this document as "Attachment 1.") Eligibility is determined based on a number of factors (including, but not limited to, country of origin, immigration status, length of residency, and employment history) and in many cases may require a background check.

I. Persons who are not employees may not be given confidential FOMC information unless all the requirements of this section IV, including citizenship require-

ments, are met and a designee of the Chairman gives prior approval.

V. ACCESS TO CONFIDENTIAL FOMC INFORMATION OUTSIDE THE FEDERAL RESERVE SYSTEM.

Access to classified FOMC information outside the Federal Reserve System is limited as follows:

A. Confidential FOMC documents generally are made available to the public after a lag of about five years. Such availability is subject to staff review (including consultation with the Chairman or the Committee where appropriate) for the purpose of redacting any materials that are still deemed to be sensitive after five years. For example, confidential information obtained from or about particular persons or businesses, foreign governments and central banks, and international institutions that is deemed sensitive after the five-year lag will be protected. In addition, national security classified information that may be contained in FOMC documents remains confidential until it is declassified. The principal objectives of the Committee's policy of withholding sensitive information after the five-year lag are to preserve the Committee's ability to collect needed information, to allow its representatives to participate in sensitive discussions and report on them to the Committee, to avoid disclosures that would adversely affect U.S. international relations, and to comply with the applicable laws governing the disclosure of confidential information.

B. Staff officers of the Committee, and those designated by the Chairman, are authorized to transmit pertinent information on System foreign currency operations to appropriate officials of the Treasury Department.

C. The Chairman may make ad-hoc exceptions to this section that are either more or less restrictive for particular documents or for other confidential information.

VI. HANDLING OF CONFIDENTIAL FOMC MATERIALS.

To assure the necessary confidentiality, it is important that special care be exercised in handling FOMC materials. The minimum requirements for handling confidential FOMC and Federal Reserve information are described in the Federal Reserve Board's "Information Classification and Handling Guide" document (copies of summary appendices of this document, labeled "Attachment 2-A" and "Attachment 2-B," are attached for convenience and are also available as pages 34–36 at: (spweb.frb.gov/sites/IT/Content/Pages/FISMA/documents/Information%20Classification%20and%20Handling%20Standard.pdf). As noted in Section III above, confidential FOMC information must be treated at least as securely as information in the corresponding Federal Reserve Board category. The following requirements are highlighted here:

A. In addition to ensuring that the materials themselves are made available only to staff members who have been given access to them, the information they contain should be discussed with such persons only.

B. Persons who no longer have access to confidential FOMC information, whether because of a job change within the Federal Reserve, employment outside the Federal Reserve, or retirement, must release custody of all confidential materials in their possession and remain subject to all the prohibitions relating to the disclosure of FOMC information that is still confidential.

C. The distribution to the Committee of all documents, other than the manager's reports, should be handled through the FOMC Secretariat.

D. In addition, to facilitate the identification of Class I and Class II FOMC information, the appropriate coversheet should be placed on all such documents that are to be circulated. (The Tealbook is distinctive in appearance and meets this requirement without an additional cover page.) The most up-to-date coversheets are available on

the FOMC Secretariat's web site: (fweb.rsma.frb.gov/dma/fomc/).

VII. ONGOING RESPONSIBILITY FOR MAINTAINING CONFIDENTIALITY.

A. The president of each Federal Reserve Bank is responsible for ensuring the confidentiality of FOMC information at that Federal Reserve Bank and for the conduct and discretion of that Federal Reserve Bank's staff with regard to the use of the information. The Chairman fulfills this role at the Board. No confidential FOMC information may be released except pursuant to Committee instructions or with written authorization from the Chairman and prompt notification to the Committee.

B. At each institution (Board or Federal Reserve Bank), the basic principles and rules of confidentiality shall be reviewed at least once a year with every person who has access to confidential FOMC information. In addition to annual circulation of the Program for Security of FOMC Information, institutions may implement further procedures in support of information security.

C. If any Committee participant or Federal Reserve System staff person becomes aware of an incident in which FOMC information security rules may have been breached, that person should promptly alert the FOMC Secretariat. The secretary or the Committee's general counsel will, with appropriate consultation with the Chairman, promptly refer all material potential breaches to the Board's inspector general and request an investigation of the incident. The Chairman will inform the Committee about these matters and investigations, as appropriate.

D. If a staff person at the Federal Reserve Board has been found to be responsible for a breach of FOMC information security, the Chairman will determine the consequences for that person. If a staff person at a Federal Reserve Bank has been found to be responsible for a breach of FOMC information security, the president of that Federal Reserve Bank will determine the consequences for that person and will inform the Chairman of that determination. If a Committee participant has been found to be responsible for a breach of FOMC information security, the Committee will determine the consequences for that participant. The Inspector General will contact law enforcement agencies whenever an investigation indicates that criminal statutes may have been violated.

VIII. COMMITTEE MEETING ATTENDANCE.

A. Except by approval of the Committee, attendance at Committee meetings, including conference calls, is limited to:

1. Board members and Federal Reserve Bank presidents and any other alternate members. In the absence of a president, a substitute Federal Reserve Bank officer designated by the president or the Federal Reserve Bank's board of directors.
2. Committee officers. In the absence of an associate economist from a Federal Reserve Bank, one substitute designated in advance by the president, with notice to the FOMC Secretariat.
3. The manager of the SOMA. In the manager's absence, a substitute designated by the manager or the president of the Selected Bank, with notice to the FOMC Secretariat.
4. One adviser or one substitute designated in advance, with notice to the FOMC Secretariat, by each president who is not currently a member of the Committee.
5. One first vice president of a Federal Reserve Bank. This designee would be in addition to those listed above. The FOMC Secretariat maintains a rotational schedule based on nominations from Federal Reserve Banks.
6. One assistant to the manager (such as the deputy manager), FOMC Secretariat assistance, and a limited number of additional

members of System staff designated by the Chairman.

B. Attendance may be limited further by the Chairman if a meeting, or portion of a meeting, gives rise to unusual sensitivity problems.

Attachment 1
NON-CITIZEN ELIGIBILITY FOR ACCESS TO FOMC INFORMATION
Summary of 12 C.F.R. 268.205

Access to all FOMC information is governed under the Program for the Security of FOMC Information. Under these rules, U.S. citizens are eligible for access to all levels of FOMC information (Class I, II, and III).[1] As explained below, eligibility for access to FOMC information for non-citizens depends on the person's job, citizenship status, residency and other requirements. The Committee applies the same requirements for access to its information that the Board applies when granting access to sensitive information of the Board.[2]

As a general matter, a non-citizen is eligible for access to FOMC information in only one of two ways—as a *Protected Individual* or as an *Eligible Employee*. Protected Individuals, defined below, are treated similarly to citizens, and are eligible for all levels of FOMC information. Eligible Employees, defined below, are initially eligible for access based on their country of origin, but may subsequently be eligible for a higher level of access if they meet certain criteria. Non-citizens who are neither Protected Individuals nor Eligible Employees may not be granted access to FOMC information.

1. Protected Individuals[3]

A "Protected Individual" is a person who is a lawful permanent resident (that is, holds a "green card") and who has taken certain steps toward becoming a U.S. citizen. Those steps require that the person *either*:

A. Sign a declaration of intent to become a U.S. citizen and file for U.S. citizenship within six months of becoming eligible to do so,

or

A. Be an employee of the Federal Reserve System (FRS) since January 1, 2006;
B. File for citizenship before requesting access to FOMC information; and
C. Pass a background check acceptable to the Board.

A green card holder who does not qualify under one of these criteria is not a Protected Individual, and therefore is eligible for access only if he or she is an Eligible Employee (see below).

2. Eligible Employees

To be an Eligible Employee, the non-citizen must be employed in a position at the Board or Federal Reserve Bank that requires a Ph.D. in economics or finance. If the non-citizen is employed in such a position, his or her eligibility for access is granted in two stages.

A. *Initial Eligibility*: Eligibility in the initial stage depends on whether the non-

[1] In all cases, whether a person is a citizen or not, access to information of the FOMC is contingent on both the eligibility discussed here **and a "need to know,"** which involves a determination by the FOMC Secretariat or the Committee Chairman that the person must be permitted access at the proposed level in order to perform his or her job. Persons who are granted access to FOMC information must abide by all rules that apply to the handling of that information.

[2] The Board's rule for access to sensitive information by non-citizens is set forth in 12 C.F.R. 268.205.

[3] Under the Board's rule, the term "Protected Individual" also includes U.S. citizens and U.S. nationals (persons who are born in American Samoa, certain former citizens of the former Trust Territory of the Pacific Islands, and certain children of non-citizen nationals born abroad). The term "Protected Individuals" also covers three additional categories of persons (those admitted for temporary residence under certain immigration provisions and those granted asylum or refugee status). However, requests for access by persons in these later categories are unlikely to arise and are thus not described here.

citizen's country of origin is on the current "country list," which is a list of countries whose citizens may be hired by appropriated federal agencies under federal legislation (see the current country list below).[4]

i. If the non-citizen is from a country on the country list, he or she is eligible initially for Class II access.

ii. If the non-citizen is not from a country on the country list, he or she is eligible initially only for Class III access.

B. *Higher Eligibility*: In the second stage of eligibility, a non-citizen can become eligible for access to information **one** level higher (i.e., a non-citizen from a country list country can become eligible for Class I access and a non-citizen who is not from a country list country can become eligible for Class II access). A non-citizen is eligible for this next level of access if he or she has:

i. Resided in the United States for six years;

ii. Been employed with the FRS for two years;

iii. Been recommended for a higher level of access by his or her division director; and

iv. Passed a background check acceptable to the Board.

COUNTRY LIST

Albania
Argentina
Australia
Bahamas
Belgium
Bolivia
Brazil
Bulgaria
Canada
Chile
Colombia
Costa Rica
Croatia
Cuba
Czech Republic
Denmark
Dominican Republic
Ecuador
El Salvador
Estonia
France
Germany
Greece
Guatemala
Haiti
Honduras
Hungary
Iceland
Ireland
Israel
Italy
Japan
Latvia
Lithuania
Luxembourg
Netherlands
New Zealand
Nicaragua
Norway
Panama
Paraguay
Peru
Philippines
Poland
Portugal
Romania
Slovakia
Slovak Republic
Slovenia
Spain
South Korea
Thailand
Trinidad & Tobago
Turkey
United Kingdom
Uruguay
Venezuela

[4] The list of eligible countries and persons is subject to legislative and other changes. The last change to the list was in 2004.

Attachment 2-A: Summary for Handling Printed Information

PRINTED	Restricted-Controlled FR[5]	Restricted FR[6]	Board Personnel (Sensitive PII)	Internal FR[7] (including Non-Sensitive PII)
MP-2 Access	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
MP-2 Duplication	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
MP-3 Labeling	"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"	"Board Personnel" at the top of every page. All pages must be consecutively numbered	"Internal FR" at the top of the first page. All pages must be consecutively numbered
MP-3 Coversheet	Restricted-Controlled FR blue coversheet	Restricted FR pink coversheet	Board Personnel green coversheet	No coversheet
MP-4 Storage	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
MP-5 Transport: Internal	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
MP-5 Transport: External	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
MP-5 Transport: Fax	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
MP-6 Sanitization & Disposal	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)

[5] FOMC Documents are labeled *Class I FOMC- Restricted Controlled (FR)*
[6] FOMC Documents are labeled *Class II FOMC – Restricted (FR)*
[7] FOMC Documents are labeled *Class III FOMC – Internal FR*

Attachment 2-B: Summary for Handling Digital Information

DIGITAL	Restricted-Controlled FR[8]	Restricted FR[9]	Board Personnel (Sensitive PII)	Internal FR[10] (including Non-sensitive PII)
MP-2 Access	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
MP-2 Duplication	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
MP-3 Labeling	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"	Board Personnel label must be provided when the information is accessed or displayed. Label Removable media "Board Personnel"	Removable media labeled as "Internal FR"
MP-4 Storage	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.
MP-5 Transport: Internal	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

[8] FOMC Digital Information, including E-mail is labeled *Class I FOMC - Restricted Controlled (FR)*

[9] FOMC Digital Information, including E-mail is labeled *Class II FOMC – Restricted (FR)*

[10] FOMC Digital Information, including E-mail is labeled *Class III FOMC – Internal FR*

DIGITAL	Restricted-Controlled FR[8]	Restricted FR[9]	Board Personnel (Sensitive PII)	Internal FR[10] (including Non-sensitive PII)
MP-5 Transport: External	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.
MP-5 Transport: Email	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 email 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
MP-6 Sanitization & Disposal	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