Privacy Impact Assessment
of
Secure External Team Space

Program or application name:

Secure External Team Space

Contact information:

System Owner:	Peter Purcell
Organization:	Division of Banking Supervision and Regulation
Address:	20th Street and Constitution Avenue, N.W. Washington, D.C. 20551
Telephone:	202-452-2298

IT System Owner:	Patrick Turner
Organization:	Federal Reserve Bank of Philadelphia
Address:	10 Independence Mall Philadelphia, PA. 19106
Telephone:	(215) 574-6000

Description of the IT system:

Secure External Team Space is an externally hosted web service provided by an authorized private contractor to the Federal Reserve that permits authorized Board of Governors of the Federal Reserve System (Federal Reserve) employees the ability to securely exchange electronic information with the financial institutions that are supervised and regulated by the Federal Reserve during the supervisory process as well as with state banking regulators with respect to their regulated financial institutions. The information exchanged in Secure External Team Space will include virtually all of the information that may be exchanged in the ordinary course as part of the supervisory process including, but not limited to, bank examination information requests sent to a financial institution and the institution's responses to those requests.

Additionally, Secure External Team Space provides Federal Reserve Banking Supervision & Regulation ("BS&R") staff with the ability to quickly and effectively exchange critical supervisory information in the event of an emergency or crisis situation with both supervised and regulated financial institutions, other government agencies and State or Federal Law Enforcement.

1. The information concerning individuals that is being collected and/or maintained:

Secure External Team Space is not designed to capture personally identifiable information; however, certain financial institution records that are exchanged as part of the supervisory process may include the following:

a. loan customer name;
b. home address;
c. social security number;
d. tax payer identification number;
e. driver's license number;
f. birth date;
g. place of birth;
h. account numbers;
i. loan account number;
j. loan or account officer name;
k. loan officer number;
l. loan balances, interest rates and payment information;
m. non-public confidential bank loan classifications;
n. financial transaction data;
o. non-public Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Asset Control documentation that main pertain to a particular loan or customer;
p. non-public Suspicious Activity Reports (SARS) that may pertain to a particular loan or customer; and
q. subpoenas and related legal documentation.

2. Source(s) of each category of information listed in item 1.

The information collected in Secure External Team Space is provided by financial institutions that are supervised and regulated by the Federal Reserve during the course of the supervisory process. Information collected in Secure External Team

Space during an emergency or crisis may be provided by the supervised financial institutions as well as by other State and Federal government agencies.

3. Purposes for which the information is being collected.

The Federal Reserve uses the information exchanged in Secure External Team Space to evaluate financial institutions' safety and soundness and compliance with consumer and community affairs laws and regulations. Personally identifiable information obtained during the supervisory process is generally not specifically referenced by examiners, but may be used to support analyses and findings. For example, individual data may be used to support aggregate analysis of issues raised during the course of the examination or supervision process.

4. Who will have access to the information.

Access to personally identifiable information in Secure External Team Space is generally limited to authorized Federal Reserve employees and contractors who have a need for the information for official purposes, which is generally limited to Federal Reserve supervisory staff who are directly involved with on-going supervisory related activities.

The information may also be shared as needed for conducting joint supervisory initiatives with the Federal Financial Institution Examination Council staff or other bank regulatory agencies, including the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, state banking regulators, and foreign banking regulators consistent with the Board's regulations as well as explicit information sharing agreements that require the implementation of access restrictions and security safeguards.

In addition, the information may also be disclosed for enforcement, statutory and regulatory purposes; to another agency or a Federal Reserve Bank, to a member of Congress; to the Department of Justice, a court, an adjudicative body or administrative tribunal, or a party in litigation; to contractors, agents, and others; and persons who are reasonably necessary to assist in connection with the Board's efforts to respond to the suspected or confirmed compromise of security or confidentiality and prevent, minimize, or remedy such harm.

5. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses).

Individuals do not have an opportunity to decline to provide the information or consent to particular uses of the information because the information is not collected from the individual. The information is collected directly from the financial institution during the bank examination or supervision process pursuant to the institution's statutory obligation to provide any and all financial records to its federal regulator. The information is acquired by the financial institution from its customers as a routine business activity.

6. Procedure(s) for ensuring that the information maintained is accurate, complete, and up-to-date.

The financial institution submitting the required supervisory information to the Federal Reserve is responsible for the accuracy, completeness and timeliness of the information submitted during the supervisory process.

7. The length of time the data will be retained, and how will it be purged.

The data in the application is retained for a minimum of three years. If data from this application is printed and stored in examination work papers, the information is retained for the normal examination work paper retention period of a minimum of three years. If data from this application is printed and retained in banking applications work papers, it is retained for no less than 15 years.

8. The administrative and technological procedures used to secure the information against unauthorized access.

A third-party vendor, whose internal controls have been reviewed and affirmed by an independent Auditor as operating with sufficient effectiveness, provides hosting and management oversight of the Secure External Team Space service. Federal Reserve employees requiring access to Secure External Team Space must first complete an approval process to have an "exchange" created and their access granted by the central Secure External Team Space Administrator based on a documented business need. Once authorized for access to Secure External Team Space, an employee has to be "invited" to a Secure External Team Space exchange before he/she can gain access to any information. Once access is granted, the particular Federal Reserve employee is responsible for administering access to

his/her exchange in accordance with the requirements of the particular supervisory activity or crisis event. Care is taken to ensure that only those employees who are authorized and have a need for the information for official business purposes have access to that information. Any exchanges that may process personal or highly sensitive information will require dual factor authentication.

9. Whether a new system of records under the Privacy Act will be created. (If the data is retrieved by name, unique number, or other identifier assigned to an individual, then a Privacy Act system of records may be created).

No new system of records is required because any personally identifiable information maintained in connection with Secure External Team Space is not retrieved by reference to an individual's name or other personal identifier.

Reviewed:

/signed/	07/09/2013
_____	_____
Ray Romero Chief Privacy Officer	Date
/signed/	07/10/2013
_____	_____
Sharon Mowry Chief Information Officer	Date