

**Treasury Collateral Management and Monitoring (TCMM)  
Local Security Administrator (LSA) Authorization Form**

The officer (Officer) of the Financial Institution (FI) identified below designates the following to serve as local security administrators (LSAs) for TCMM services. Each LSA may designate other individuals as users or LSAs. **At least two LSAs must be named for each FI location that requires access.**

**Section 1 – General Information**

- Create New LSA(s)**
- Modify LSA Information** (only applies to last name, e-mail address, phone number and/or address)
- Delete LSA(s)**

Financial Institution Name:

ABA Number: \_ \_ \_ \_ \_

**Section 2 – LSA Profile(s)**

**Local Security Administrator**

Single Sign-on User ID (If applicable)

LSA's Name (first, last)

LSA's E-mail Address (not shared)

Phone Number (direct number to LSA)

Branch Name (LSA location)

Street Address (LSA location)

Street Address Line 2 (LSA location)

City / State / Zip (LSA location)

LSA Activation Date

Effective Immediately

Future Effective Date \_\_\_ / \_\_\_ / \_\_\_

**Section 3 – Officer Authorization**

By signing below the Officer certifies that he/she is duly authorized by the Financial Institution to designate individuals who can serve as LSAs. The Officer also agrees to be responsible on behalf of the Institution for all security management related to TCMM access. **The officer signing this form cannot be designated as an LSA on this form.**

Name (print)		Signature	
Title		Phone	( ) - Date / /
Email Address			

**Please submit completed forms via e-mail or fax to the TCMM Treasury Support Center:**

TCMM\_TSC@stls.frb.org or 866-707-6574

**Internal Use Only**

Date/Time Confirmed with Authorizer:	Initials:	Date/Time Verified Authority and Title:	Initials:
Date Entered:	Initials:	Date Entry Verified:	Initials:

## General Notices

To access TCMM, Users may be issued authentication credentials such as a username and password. We (the United States Department of the Treasury and its designated agents) may rely upon the authentication credentials alone to provide access to TCMM services. We may act upon any electronic message that we establish to be associated with a known set of authentication credentials as if the message consisted of a written instruction bearing the ink signature of one of the Depository's duly authorized officers. A Depository accepts sole responsibility for and the entire risk arising from the use of authentication credentials by its Users.

All Users must agree to terms and conditions governing access to TCMM services. These terms and conditions can be found on the Web site(s) of the application(s) providing TCMM services. These terms and conditions include provisions requiring Users to maintain the confidentiality of their authentication credentials, to report the possible theft or compromise of their authentication credentials, and to take action whenever they no longer require access or require access to a lesser extent than is currently the case. The terms and conditions also include provisions that require LSAs to enforce the principle of least privilege, ensure that LSAs delete Users when appropriate, and require LSAs to periodically recertify their compliance with their responsibilities. These terms and conditions are subject to change from time to time. We may have Users "click-thru" these terms and conditions before first use, on a periodic basis, or whenever they change, to reflect their continued agreement to these terms and conditions.

We will not be liable for any loss or damage resulting from a problem beyond our reasonable control. This includes, but is not limited to, loss or damage resulting from any delay, error or omission in the transmission of any electronic information, alteration of any electronic information, any third party's interception or use of any electronic information, a failure of services provided by an Internet service provider, and malicious activity received from or introduced by a third party. Additionally, we are not liable for loss or damage resulting from acts of war, acts of terrorism, acts of God or acts of nature.

Except as otherwise required by law, in no event will we be liable for any damages other than actual damages arising in connection with TCMM services, including without limitation indirect, special, incidental or consequential damages.

Except as otherwise required by law, WE DO NOT MAKE ANY WARRANTIES, EXPRESS OR IMPLIED (INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE), WITH RESPECT TO ANY SOFTWARE, INFORMATION, SERVICE, OR OTHER ITEM PROVIDED BY, LOCATED ON, DERIVED FROM, ASSOCIATED WITH, REFERRED TO BY, OR LINKED TO BY THE TCMM SERVICES. EVERYTHING IS PROVIDED "AS IS."

## Privacy Act Statement

We are authorized to request the information on this form by 31 U.S.C. §§ 321, 323, and 3301, 3302, 3303, and 3304. We need this personal information to help authenticate and determine who is responsible for viewing potentially sensitive information or engaging in a transaction. Furnishing this information is voluntary, but an LSA cannot be designated, and Depository will not have access to TCMM services, unless the information is furnished.

From systems including those used to provide TCMM services, the parties to whom we disclose information may include:

- Appropriate Federal, state, local or foreign agencies responsible for investigating or prosecuting the violation of, or for enforcing or implementing, a statute, rule, regulation, order, or license, but only if the investigation, prosecution, enforcement or implementation concerns a transaction(s) or other event(s) that involved (or contemplates involvement of), in whole or part, an electronic method of collecting revenues for the Federal government. The records and information may also be disclosed to commercial database vendors to the extent necessary to obtain information pertinent to such an investigation, prosecution, enforcement or implementation.
- Commercial database vendors for the purposes of authenticating the identity of individuals who electronically authorize payments to the Federal Government, to obtain information on such individuals' payment or check writing history, and for administrative purposes, such as resolving a question about a transaction.
- A court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel or witnesses, for the purpose of civil discovery, litigation, or settlement negotiations or in response to a subpoena, where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings
- A congressional office in response to an inquiry made at the request of the individual to whom the record pertains.
- Fiscal agents, financial agents, financial institutions, and contractors for the purpose of performing financial management services, including, but not limited to, processing payments, investigating and rectifying possible erroneous reporting information, creating and reviewing statistics to improve the quality of services provided, or conducting debt collection services.
- Federal agencies, their agents and contractors for the purposes of facilitating the collection of revenues, the accounting of such revenues, and the implementation of programs related to the revenues being collected
- Federal agencies, their agents and contractors, to credit bureaus, and to employers of individuals who owe delinquent debt only when the debt arises from the unauthorized use of electronic payment methods. The information will be used for the purpose of collecting such debt through offset, administrative wage garnishment, referral to private collection agencies, litigation, reporting the debt to credit bureaus, or for any other authorized debt collection purpose.
- Financial institutions, including banks and credit unions, and credit card companies for the purpose of revenue collections and/or investigating the accuracy of information required to complete transactions using electronic methods and for administrative purposes, such as resolving questions about a transaction.
- Appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.