Bank Management System (BMS) 1.0
Federal Reserve Bank of St. Louis/ Bureau of the Fiscal Service
User Authorization Form

The User listed is designated to perform the Role and Organization(s) responsibilities in the Bank Management System (BMS), in accordance with the BMS Security Matrix.
Note: Forms should be completed electronically with the exception of the Authorized Signature.

Section 1 – General Information	
Select User Type	Select User Type
Select Primary User Role	Select User Role
Select Secondary User Role (if applicable)	Select User Role
Select Division/Program	Select Division/Program

Section 2 – User Profile Information					
ITIM Single Sign-on ID (if applicable)					
First Name					
Last Name					
E-mail Address					
Phone Number					
Organization Name					
Street Address					
Street Address Line 2					
City		State		Zip	

Section 3 – Authorized Signature

By signing below, the individual certifies that he/she is duly authorized by the organization to designate individuals who can serve as a Bank Management Service (BMS) user. The authorized individual will be contacted and must confirm signature before request can be completed. **The authorized individual signing this form cannot be designated as the user on this form**.

Name (print)		Signature			
Title		Phone		Date	
Email Address					

Please submit completed forms via e-mail to the BMS Enrollment Team:
STLS.BMS.Enrollment@stls.frb.org

Internal Use Only	
BMS Team Approver:	Date:
BMS Management:	Date:

General Notices

To access BMS, 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 BMS services. We may act upon on 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 Depositary's duly authorized officers. A Depositary 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 BMS services. These terms and conditions can be found on the Website(s) of the application(s) providing BMS 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 BMS 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 BMS 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 Depositary will not have access to BMS services, unless the information is furnished.

From systems including those used to provide BMS 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.