G-INVOICING AGENCY ACCOUNT ENROLLMENT FORM

G-Invoicing is a Fiscal Service-owned application used to originate and approve Intragovernmental Buy/ Sell transactions including the establishment of General Terms and Conditions (GT&Cs) and Orders between trading partners.

To establish an agency account, you must first identify a primary and secondary **Master Administrator** to be created in the G-Invoicing system. The **G-Invoicing Master Administrators** are assigned the *Master Administrator* role and delegated authority to create, modify, and deactivate additional agency **User Administrators** and **Group Administrators** and manage the Organization Model for the agency account. All **Master Administrators** are created by **Central Administrators.**

G-Invoicing Primary Master Administrator Acknowledgment

"Primary" Master Administrator agrees:

- Retain the signed copy of the G-Invoicing System Account Enrollment Form for a period of seven (7) years and make it available for examination by request.
- Ensure two (2) Master Administrators are assigned AND active in the agency account at all times.
- Ensure all G-Invoicing users are informed of the requirements listed below:
    1. Users must certify that Intragovernmental transactions (IGT) are in compliance with the requirements and responsibilities set forth in applicable laws and regulations, including Vol. 1 Treasury Financial Manual 2-4700, App. 8, IGT Guide and related guidance on https://www.fiscal.treasury.gov/index.html and Chapter 4000 Intragovernmental transaction applications: Intra-governmental payment and collections (IPAC) and Government Invoicing (G-Invoicing);
    2. Users shall not decompile, disassemble or reverse engineer any aspect of G-Invoicing;
    3. Use of G-Invoicing is only for processing transactions for any aspect of the United States government;
    4. Users shall not reproduce, duplicate, copy, sell, resell, or exploit for any commercial purpose, any portion of G-Invoicing;
    5. Users must agree that G-Invoicing may contain proprietary information of a third party for which the Federal Reserve Bank has obtained a license for use and disclosure;
    6. Access to G-Invoicing is granted based on least privilege access model and individual credentials assigned to each individual user of the system:
        a. User must not divulge credentials used to access the system to anyone.
        b. User must not share credentials with any other users.
        c. Unauthorized use may result in prosecution or criminal penalties. If I suspect that the confidentiality of my credentials has been compromised, I will immediately notify the Treasury Support Center at (877) 440- 9476.

Additionally, the G-Invoicing "**Primary" Master Administrator** acknowledges the following terms and will ensure **User Administrators** are informed and aware of the following requirements.

"Primary Master Administrator" "Master Administrator" certifies:

- Create and maintain users who are authorized to conduct G-Invoicing transactions for the agency;
- Apply least privilege access requiring users be granted the most restrictive set of privileges required to perform the duties of their role and responsibilities thereby limiting the potential damage that can result from accident, error, or unauthorized use.
    - *NOTE:* ALL **Primary Master Administrators** and **Master Administrators** should reference the *"G-Invoicing Administrator" and "G-Invoicing User Guide"* for a list of application roles and permissions. The guides are available on the G-Invoicing Home Page menu.
- Ensure user accounts are disabled **within two (2) business days** of voluntarily leaving service.

- Ensure user accounts are disabled **immediately (same day)** when a user is involuntarily terminated from service.
- Participate in G-Invoicing "Annual User Recertification" to review and approve user access of the G-Invoicing agency account and confirm access is appropriate for their role and responsibilities within the agency.

The following information must be entered exactly as it should be entered into G-Invoicing, including any spaces, capitalizations, and abbreviations.

Agency Profile Information	
* Agency Name:	
*Address Line 1:	
Address Line 2:	
*City:	
* State/Province:	
*ZIP Code:	
*Country:	United States of America
* Phone Number: *xxx-xxx-xxxx*	

Shared Service Provider (where applicable)	
* Provider Name:	
* Primary Contact Name:	
* Address Line 1:	
Address Line 2:	
* Email address:	
* City/ State:	
* ZIP Code:	
* Country:	United States of America
*Phone Number: *xxx-xxx-xxxx*	

** Required field must be completed*

Appendix A: Agency Locator Code (ALC) Treasury Account Symbol (TAS)

ALC and TAS Information			
*Agency Location Code(s)			
Treasury Account Symbol (TAS) Account Filters: Using an * in the table will include all data for that field, if more granular access is needed, please specify in the fields column. Each row is a separate TAS filter. For TAS filters, use the additional rows provided.			
ATA	*AID	MAIN	SUB

** Required field must be completed*

If additional ALC & TASs are needed, please provide a separate document

Appendix B: Agency Master Administrators & Agency Approver

G-Invoicing "Primary" Master Administrator	
☐ SailPoint IIQ "Agency Approver" **	
*First Name:	
Middle Initial:	
*Last Name:	
Title/Position:	
*Work Email:	
*Work Phone Number:	
*Date:	
*Signature: *(Digital signature-PIV,PIV-I,CAC)*	

G-Invoicing "Secondary" Master Administrator	
☐ SailPoint IIQ "Agency Approver" **	
*First Name:	
Middle Initial:	
*Last Name:	
Title/Position:	
*Work Email:	
*Work Phone Number:	
*Date:	
*Signature: *(Digital signature-PIV,PIV-I,CAC)*	

User Information (if adding additional Master Admins or SailPoint "Agency Approvers")			**Master Administrator***		**SailPoint "Agency Approvers" ****		***SailPoint Agency Approver Digital Signature
			ADD		ADD		
*Name	*Title	*Email Address	QA	Prod	QA	Prod	

* *Required information*

If additional "Master Administrators" are needed, please provide a separate document. The "Primary Master Administrator" will be added as the "User Administrator" for all "Master Administrator" user accounts in G-Invoicing by default. The "User Administrator" can be updated once the account has been established.

* No signature required for Master Administrators not added as SailPoint Approver.

** The SailPoint IIQ "**Agency Approver**" will receive an email for all end user access requests submitted via SailPoint IdentityIQ. The user must complete the "Manager" field in SailPoint IIQ to ensure the first level approval email is routed properly. Once the "Manager" approves the access request, the request is routed to the members of the "**Agency Approver**" group. The SailPoint IIQ "Agency Approver" group is populated with ALL prior agency "Primary Master Administrators", "Master Administrators" and "User Administrators". The SailPoint IIQ "**Agency Approver"** has the sole responsibility for approving access requests for end users within their agency. The "Agency Approver" is responsible to confirm the identity of the end user submitting the access request and whether he/she is authorized to access the functions in the application being requested. When the "Manager" and "Agency Approver" receives the email of a pending access request for their agency, he/she must log into the SailPoint IdentityIQ and approve/reject the request as appropriate.

*** Read the below "Agency Approver" Responsibility Agreement before signing

Responsibilities:

I am aware that the Bureau of the Fiscal Service's policy is to treat all information as an asset, whether it is computer programs, software, data or other information collected, stored, and generated in the conduct of its business. To the best of my ability, I will protect information from unauthorized use, modification, destruction, or disclosure, whether accidental or intentional.
o I am aware of the policies and requirements of the Bureau of the Fiscal Service and agree to abide by them.
o I will NOT attempt to circumvent any of the security mechanisms within SailPoint IdentityIQ and IPAC system.
o I will ensure that proper authorizations on requests are checked.
o I will ensure that all fields on the requests are complete and correct.
o I will ensure proper record keeping of all information processed.
o I will comply with all security-related polices, standards, procedures and practices.
o I will notify the Treasury Support Center at 877-440-9476 of any known or suspected violation of information security policy, procedures, or threat to IPAC resources.

I have read and understand the "Agency Approver" Responsibility Agreement and agree to abide by it.

*OFFICIAL AGENCY AUTHORIZED APPROVER TO SETUP AGENCY ACCOUNT	
*Name:	
*Title:	
*Email Address:	
*Phone Number: *xxx-xxx-xxxx*	
*Address: (Street, City, State, Zip)	
*Date:	
*Approver's Signature: *Digital signature (PIV,PIV-I,CAC)*	

* *Required information*

** By signing as an **Agency Approver**, the officer (Chief Financial Officer, Deputy Financial Officer, Director of the Office of Finance, Office of Accounting or other comparable title) certifies that he/she is duly authorized by the agency/organization to designate who may serve as "Primary Master Administrator" for the above named agency.*

The following sections will be completed by the Federal Reserve Bank of St. Louis

Agency Organizational Unit (OU) Information	
*Organization Unit:	

Agency entered in G-Invoicing by:		
*Environment:		
* Analyst Name:		
* Date:		
* Signature: *Digital signature (PIV,PIV-I,CAC)*		

* *Required information*

11.5.5.1 Write and Maintain a Privacy Act Statement

Pursuant to 5 U.S.C. §552a (e) (3) agencies are required to provide what is commonly referred to as a Privacy Act Statement to all persons asked to provide personal information about themselves, which will go into a system of records (i.e., the information will be stored and retrieved using the individual's name or other personal identifier such as a Social Security Number). Department of the Treasury (Treasury) policy is to provide a Privacy Act Statement regardless of whether the collection is part of a system of records or not. All Privacy Act statements must be reviewed by the Chief Privacy Officer or Privacy Act Officer.