

## IPAC SailPoint Identity IIQ “AppApprover” Form

The CAIA-SailPoint “AppApprover” ALC group members are the final authorized approvers for all agency user role requests for the agency ALC. The first access approver is the user’s “Manager” assigned in SailPoint.

The “AppApprover” groups replaced the former “Master Administrator” and “Agency Administrator” roles in ISIM.

After a user submits their access requests in SailPoint IIQ, the user’s “Manager” (1<sup>st</sup> approver) will receive an email to approve the access request. Once approved, a second email is sent to the “AppApprover” (2<sup>nd</sup> approval) group members to approve the access request. User’s Manager (1st Approver) and SailPoint AppApprover (2nd Approver) cannot be the same person. Once both approvals are complete, the user will be able to access the application and role-based functions requested for the specific ALC/PON(s).

This form is completed for the following requests.

1. User to be added to the agency “AppApprover” group for the ALC/PON listed below and signed by an active agency SailPoint “AppApprover” group member.
2. User to be removed from the “AppApprover” group. No “AppApprover” signature is required.

### IPAC SailPoint IIQ “AppApprover” Responsibility Agreement

The information you provide on this form will be used principally to aid in the completion of your access request to the Bureau of the Fiscal Service systems. All or part of this information may be furnished by the Federal, State, local and public agencies in the event a violation of the law is disclosed. More information on Privacy Policy and Legal Notices is available at [www.fiscal.treasury.gov/privacy.html](http://www.fiscal.treasury.gov/privacy.html).

Completion of this form is voluntary; however, failure to complete the form requested will result in no consideration for access to the Bureau of the Fiscal Service systems. Although no penalties are authorized if you do not provide the requested information, failure to supply information will result in your not receiving access to the Bureau of the Fiscal Service systems.

#### SailPoint “AppApprover” 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.

- I am aware of the policies and requirements of the Bureau of the Fiscal Service and agree to abide by them.
- I will NOT attempt to circumvent any of the security mechanisms within SailPoint IdentityIQ and IPAC/RITS system.
- I will ensure that proper authorization on requests is checked.
- I will ensure that all fields on requests are complete and correct.
- I will ensure proper record keeping of all information processed.
- I will comply with all security-related policies, standards, procedures, and practices.
- I will notify the Treasury Support Center at 877-440-9476

I have read and understand the “AppApprover” Responsibility Agreement and agree to abide by it.

### SailPoint "AppApprovers"

The SailPoint "AppApprover" group provides approval for users to access ALL IPAC environments - Production, STG-Current and STG-Future.

By signing this form, I acknowledge I have read and understand the "AppApprover" Responsibility Agreement and agree to abide by it.

Name	Email Address	ADD	Remove*	ALC/PON(s)**	***Digital Signature of user being added (PIV, PIV-I, CAC)

\*No signature required to remove user.

\*\*Each unique Agency Location Codes (ALCs) and/or RITS Payroll Office Numbers (PONs) must be listed to establish access as the SailPoint "AppApprover".

\*\*\*All new "AppApprovers" must digitally sign the form to indicate they have read and agree to the "AppApprover" Responsibility Agreement above. **DO NOT LOCK THE FORM AFTER EACH SIGNATURE.** This will prevent others from being able to sign the form.

**An active agency SailPoint "AppApprover" signature is required to add any new "AppApprover(s)" to the agency SailPoint "AppApprover" group.**

*Existing SailPoint "AppApprover" Signature	
*Name:	
*Email Address:	
*Date:	
*Approver's Signature: <i>Digital signature (PIV,PIV-I,CAC)</i>	

\* Required Information

**Official Agency Authorized Approver signature is ONLY REQUIRED when there is no active agency "AppApprover" in the agency SailPoint "AppApprover" group.**

*Official Agency Authorized Approver to setup initial AppApprover(s)	
*Name:	
*Title:	
*Email Address:	
*Date:	
*Approver's Signature: <i>Digital signature (PIV,PIV-I,CAC)</i>	

\* Required information

By signing as an **Agency Authorized 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 an agency "AppApprover" for the above-named ALC(s).

## Due Diligence Guidelines

It is very important to verify the identity of the Federal Program Agency, their Agency Approvers, and End Users. The general rule is the more sensitive the information, the more exhaustive the verification process.

1. The **Federal Program Agency** will provide a name of **two “AppApprovers”** per agency bureau, Agency Location Code (ALC) or Payroll Office Number (PON), designated with the authority to determine whether an End User should be authorized as an “AppApprover” and/or End User for the application. This is to ensure there is at minimum one backup to approve IPAC/RITS user’s access requests. The agency can identify additional “AppApprovers”, if necessary.

2. The “AppApprover” will receive an email after the **End User’s** SailPoint “Manager” approves the 1<sup>st</sup> access request submitted via SailPoint IdentityIQ. The “AppApprover” is responsible to provide the final approval (2nd approval) for all agency user access requests. The “AppApprover” is responsible to confirm the End User submitting the access is authorized to access the functionality in application for the roles being requested. When the “Manager” and “AppApprover” receives the pending access request email, they must login to SailPoint IdentityIQ and approve/reject the request. If the request is not fully approved within 14 calendar days, the user must reinitiate the request.

1. **Federal Program Agency** – business entity requiring access to the IPAC application.
2. **AppApprover**- term for the individual(s) identified by other “AppApprovers” or the “Official Agency Authorized Approver” who are authorized to approve a user access request thereby granting access to the IPAC/RITS application.
3. **End User** – person employed by a Federal Program Agency who has a business need to access the IPAC/RITS application.

### COMMENTS:

#### [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.

**Please complete the required information and return the completed form to the Treasury Support Center email ([IPAC@stls.frb.org](mailto:IPAC@stls.frb.org)). If this is an expedited request, please specify in the email.**