THE FEDERAL RESERVE
FedLine® Solutions

FedLine® Solutions Security and Resiliency Assurance Program Guide

2022 Program Year

Table of Contents

Program Purpose

The Federal Reserve Banks' FedLine® Solutions are a critical component of the U.S. electronic payments system and provide access to FedACH® Services, Fedwire® Services, FedCash® Services and other electronic payment and information solutions. While FedLine Solutions benefit from numerous embedded security features, institutions and their service providers with access to these solutions ("Organizations") play a vital role in safeguarding the endpoints that are used to interact with the Federal Reserve Banks. Accordingly, the Federal Reserve Banks require Organizations to comply with Federal Reserve Bank policies, procedures, and security controls ("Security Requirements").

The Security & Resiliency Assurance Program ("Assurance Program") ensures each Organization, at least annually, conducts a self-assessment of compliance with the Security Requirements ("Self-Assessment") by requiring that the Organization attest to having conducted such Self-Assessment, as outlined in Appendix A, Section 3 of Operating Circular 5. These measures are intended to protect against unauthorized access or use of information that could result in substantial harm to an Organization.

The Assurance Program is risk-based and informed by industry best practices, federal standards (including National Institute of Standards and Technology ("NIST") standards), and relevant supervisory guidance (including Federal Financial Organizations Examination Council ("FFIEC") guidance). The program engages your Organization's senior management in the FedLine security review process to encourage holistic risk management practices and risk-based decision making.

The purpose of the Assurance Program is to:

- Reduce the risk of fraudulent transactions and promote executive-level awareness of any gaps or control deficiencies within an Organization.
- Enhance an Organization's risk management and resiliency focus to help ensure endpoint environments are secure and resilient.
- Increase confidence that controls are in place and being monitored to protect payment systems and customers.
- Enhance an Organization's vigilance against cyber-attacks and foster discussions and planning to address key risks and develop timely remediation plans for any non-compliance or deficiencies.

Organization Responsibilities

By accessing services or applications from the Federal Reserve Banks or by sending data to or receiving data from the Federal Reserve Banks, an Organization agrees to the Security Requirements. Some Organizations may elect to outsource some or all of their payment or electronic connections to a third-party service provider. Although the use of third-party agents is permitted, these outsourcing arrangements do not transfer an Organization's obligation or responsibility to comply with required security measures and controls.

Organization Responsibilities (continued)

Your Organization must perform the following to complete the Assurance Program:

- Conduct a Self-Assessment of its compliance with the Security Requirements.
- If required by the Federal Reserve Banks, ensure the Self-Assessment is conducted or reviewed by an independent internal function or third party. This information will be included in the body of the Assurance Program email, if required; see Appendix A for additional information.
- Review and agree to the provisions of the attestation letter. A description of the attestation provisions is set forth in Appendix C. Attest that the Self-Assessment was completed by having a senior management official or executive officer, in charge of electronic payments operations or payments security for the Organization, sign the provided attestation letter.

Plan and Prepare

All End User Authorization Contacts (EUACs) for your Organization will receive the annual Assurance Program communications, typically sent in the month of January. Please ensure the contact information for your Organization's EUACs is current with the Federal Reserve Banks. Ensure the AdobeSign domain (@adobesign.com) is added to your Organization's safe senders list and locate the Assurance Program email communication.

It may be helpful to identify a primary point of contact that will coordinate and facilitate the Assurance Program process. This individual will coordinate completion of the Self-Assessment and submission of your Organization's attestation letter which indicates the completion of the program for that year.

When preparing for the annual Self-Assessment, identify a senior management official within your Organization who will attest, among other items (See Appendix C), that the Self-Assessment was conducted. This individual should be an official or executive officer in charge of electronic payments operations or payments security for the Organization.

Some Organizations may be required to conduct an *independent* Self-Assessment. The following information will be in the body of the Assurance Program email if your Organization is required to perform an independent Self-Assessment:

> **Your organization is requested to perform an independent self-assessment to ensure compliance with the security requirements as outlined in Appendix A of the FedLine Solutions Security and Resiliency Assurance Program Guide.**

Additional instructions on the independent Self-Assessment are provided in Appendix A.

Get Started

To get started, review all Assurance Program materials for your Organization which can be accessed within the Assurance Program email, distributed annually be the Federal Reserve Banks to all EUACs for each Organization, and sent with the domain name adobesign@adobesign.com.

The email will contain a secure link to the materials for your Organization which includes the Quick Reference, Program Guide, and attestation letter.

To assist your Organization in conducting the annual Self-Assessment, gather the relevant reference materials (e.g., FedLine Solutions Security and Control Procedures). See Appendix B for supporting documentation.

Conduct the Self-Assessment

Once relevant supporting documentation is gathered, the Self-Assessment can be conducted.

Your Organization is ***not*** required to submit the results of your Self-Assessment to the Federal Reserve Banks as part of the attestation process. However, your Organization is responsible for retaining its Self-Assessment and related artifacts in accordance with your internal record retention policy. These artifacts may support your internal compliance and remediation efforts and may facilitate engagements with external auditors or regulatory agencies.

If any areas of noncompliance are identified in the Self-Assessment, remediation plans should be in place to promptly address any areas of noncompliance with the Security Requirements.

Service Providers and Third-Party Agents

To the extent the Organization uses a third party service provider or other agent with respect to an electronic connection used to access Federal Reserve Bank services or applications, the Organization is responsible for that service provider's or other agent's compliance with the Security Requirements.

For Organizations that connect to FedLine only through a third party provider, that Organization can look to its third party provider to obtain information necessary to submit its attestation. Exactly what the Organization needs from its third party provider in order to submit the Organization's attestation is up to each Organization, but for example could include such items as (i) obtaining a copy of the third party provider's attestation to the Federal Reserve Banks, or (ii) obtaining a separate confirmation or other information from the third party provider indicating that the required Assurance Program Self-Assessment was completed. The Organization might then elect to use that information to support its own attestation.

Review and Sign the Attestation Letter

Upon completion of the Self-Assessment, the signing official will attest to the provisions outlined in Appendix C and the attestation letter.

If necessary, an EUAC can delegate the Assurance Program materials to the designated signer. If the Assurance Program materials are needed by other individuals in the Organization for awareness only, and not for signature, the Assurance Program materials can be forwarded. Delegation is not required in this circumstance.

Organizations are required to attest that they have completed the Self-Assessment by submitting the signed attestation letter to the Federal Reserve Banks. The substantive provisions of the required attestation are provided in Appendix C.

The Federal Reserve Banks leverage the AdobeSign electronic workflow and signature solution to support the attestation process. The process for completing the attestation letter will be automated within the Assurance Program materials available via the secure link provided by email to your Organization's EUACs. The attestation letter must be signed by a senior management official or executive officer in charge of electronic payments operations or payments security for your Organization.

Upon submission of the electronic signature, a signed copy of the attestation letter will be sent to the Delegated Signer, the Organization's EUACs, and the Federal Reserve Banks. The electronically signed attestation letter is the only document required to be submitted to the Federal Reserve Banks.

Failure to Comply

Failure of an Organization to comply with the Assurance Program is a violation of Operating Circular 5 that may result in the Reserve Banks taking any of the actions set out in section 7.1 of Operating Circular 5. The Reserve Banks may take other actions that they deem appropriate under the circumstances, including but not limited to disclosing the circumstances of noncompliance to the Organization's prudential regulator or other supervisory body, as well as executing limitations on user access and authentications, services, and reporting. See Operating Circular 5 including Section 5 of Appendix A for more information.

Appendix A – Instructions for Independent Self-Assessment

Your Organization will be notified, in the body of the Assurance Program email received annually, if an independent Self-Assessment is required. For those Organizations, the requirement of independence can be satisfied by having:

- An independent third party, such as an audit firm or security consultant, perform the Self-Assessment.
- An independent internal function perform the Self-Assessment, such as internal audit or compliance (i.e., a function that is not in the reporting line of the senior executive in charge of payment services).
- If the Self-Assessment is conducted by a non-independent party or function, an independent third party must review the work conducted in connection with the Self-Assessment to establish that it was designed and conducted in a manner reasonably sufficient to identify any material noncompliance with the Security Requirements.

As part of completing the attestation letter, your Organization will be asked which of the above approaches was used and the contact information for the independent party/function.

Evidence of work performed, or independent opinions, need not be submitted to the Federal Reserve Banks but should be maintained according to the Organization's record retention policy.

Appendix B - Supporting Documentation

To assist your Organization in performing an annual Self-Assessment against the Security Requirements, the following section highlights key reference materials that describe the security measures in greater detail.

FedLine Solutions Security Requirements

Operating Circular 5 – Electronic Access
Operating Circular 5 sets forth the general terms under which an Organization may access services and applications provided by the Federal Reserve Banks over an electronic connection. The Certification Practice Statement and the Password Practice Statement describe supplemental procedures and requirements surrounding digital credentials used to access Federal Reserve Bank services and applications.

The following documents can be found on FRBservices.org® on the Operating Circulars page:

- Operating Circular 5 (Electronic Access)
  - Certification Practice Statement of the Federal Reserve Banks' Certification Authority
  - Certification Practice Statement of the Federal Reserve Banks' Services Public Key Infrastructure
  - Password Practice Statement

FedLine Security and Control Procedures
FedLine Security and Control Procedures contain detailed security requirements and are part of the FedLine documentation provided to your Organization during the FedLine implementation process. These documents are available to the Organization's End User Authorization Contacts (EUACs).

The **FedLine Web® and FedLine Advantage® Security and Control Procedures** documents are available in the EUAC Center, which is accessible via FedLine Home. FedLine Web EUACs have access to the *FedLine Web Security and Control Procedures*, and FedLine Advantage EUACs have access to both the *FedLine Web Security and Control Procedures* and the *FedLine Advantage Security and Control Procedures* documents.

The **FedLine Command® and FedLine Direct® Security and Control Procedures** are contained in Section Orange of the *FedLine Command Security and Implementation Guide* and the *FedLine Direct Security and Implementation Guide*, respectively, which are provided to FedLine Command and FedLine Direct EUACs via encrypted, password-protected email.

Please contact the Customer Contact Center if you need copies of these documents.

Organizations must review the Security and Control Procedures for all FedLine Solutions that they utilize.

Appendix B - Supporting Documentation (continued)

Additional Resources & Contacts

If you are looking for additional information on the Assurance Program, please visit our Security & Resiliency Assurance Program Resource Center, also accessible via FRBservices.org.

- There you will find additional information such as past articles on the Assurance Program and educational materials.
- We also encourage you to review the Frequently Asked Questions. We update FAQs regularly with new questions received from Organizations.

If you still have questions, the following contacts are available to your Organization:

- The Assurance Program Team by email (sys.assurance.program@frb.org).
- Your Federal Reserve Bank Account Executive is also available to assist you. To find a list of Federal Reserve Bank contacts specific to your organization, use the Find Your Contacts tool, accessible via FRBservices.org.
- The Customer Contact Center (CCC) at (888) 333-7010.

Appendix C – Attestation Provisions

The attestation letter you will be required to electronically sign and submit (we will provide you with a form) will include the following substantive provisions:

1. We understand the Organization's responsibility to adhere to the security policies, procedures, and requirements set forth in Operating Circular 5, *Electronic Access*, and its Appendix A, including those for the Organization's use of FedLine Solutions and associated electronic connections used to access Federal Reserve Bank services or applications.

2. We confirm that the Organization has conducted a Self-Assessment of its compliance with the security policies, procedures, and requirements identified in item 1. The Organization calibrated its Self-Assessment based on its view of the risks it faces with respect to complying with such policies, procedures, and requirements.

3. [For Organizations notified an independent Self-Assessment is required: We further confirm that the Self-Assessment was either (i) conducted by an independent third party, (ii) conducted by an independent internal function, such as internal audit or compliance, or (iii) to the extent the Self-Assessment was conducted by a non-independent party or function, an independent third party reviewed the work conducted in connection with the Self-Assessment to establish that it was designed and conducted in a manner reasonably sufficient to identify any material noncompliance with the Security Requirements identified in item 1.]

4. To the extent the Organization uses a third party service provider or other agent with respect to an electronic connection used to access Federal Reserve Bank services or applications, we understand that the Organization is responsible for that third party service provider's or other agent's compliance with the security policies, procedures, and requirements identified in item 1.

5. The Organization has remediation plans in place, including appropriate procedures to escalate concerns to the appropriate leaders within the Organization, to promptly address any areas of noncompliance with the security policies, procedures, and requirements identified in item 1.

6. We understand that the Organization or its third party service provider or other agent must immediately notify the Federal Reserve Banks' Customer Contact Center by telephone at (888) 333-7010 of any suspected or confirmed fraud, infringement, or security breach relating to any electronic connection and must promptly confirm that notification in writing.

7. The Organization shall maintain in its records (1) the Self-Assessment; (2) appropriate documentation supporting the results of the Self-Assessment; and (3) a copy of the electronically signed attestation letter.