

Supplemental Instructional Document for the SecurID Control Form

The Federal Reserve IT Security group is in the process of replacing all expiring SecurID Tokens. Please review instructions (in **red**, below) to complete sections **A**, **D**, **G**, and **F** of the SecureID token form.

Section A: Provide Date of Request

- Date should be consistent with the date the completed SecurID Control Form is emailed to the Shared National Credit Support Office at the Federal Reserve Bank of Kansas City. Email address: kcstatcs@kc.frb.org

Section D: Provide User Information

- Tokens will be shipped 10-15 days following receipt of the required user access forms (Access Control Form and SecurID form)
- In light of widespread remote working arrangements, please identify the physical address where the token should be mailed to you. (*This may differ from your organization's main mailing address.*)

SecurID Control Form for External Users of Federal Reserve Board (FRB) Systems, including secure Websites

Section A: Request for a New SecurID To be completed by your organization's FRB Site Administrator or by the User if there is no FRB-designated Administrator.		(FRB Use Only)	
<input type="checkbox"/> New Request (Required only for a new request)		New SecurID/NT login ID:	
Date of Request :		SecurID Access Serial Number:	
Name of FRB System/Website for which access is requested: eSNC		Replacement SecurID Access Serial Number:	
Section B: Request for a Replacement SecurID To be completed by your organization's FRB Site Administrator or by the User if there is no FRB-designated Administrator		SecurID Access Serial Number:	
<input type="checkbox"/> Replacement Request (Required only for a replacement request)		Date of Request :	
Section C: Request for the Deactivation of a SecurID To be completed by your organization's FRB Site Administrator or by the User if there is no FRB-designated Administrator.			
<input type="checkbox"/> Deactivation (Required only for deactivation request)	Date of Deactivation:	SecurID/NT login ID:	
Section D: User Information To be completed by the User			
Last Name:		First Name:	M.I.:
Name of Organization:		Organization's Address (City/State/Country/Zip Code)	
User's Work Email Address:		User's Telephone No.:	
Section E: Administrator Information To be completed by your organization's Administrator if your organization has an FRB-designated Administrator.			
Last Name: NA		First Name: NA	
Name of Organization: FRBKC		Department: Statistics, Structure & Reserves	Mail Stop / Room Number / Suite:
Organization's Address : 1 MEMORIAL DRIVE, 10 TH FLOOR			
City: KANSAS CITY		State: MO	Country: USA Zip Code: 64108
Administrator's Work Email Address : kcstatcs@kc.frb.org		Administrator's Office Telephone No.: (800) 333 2898	

Note: Failure to complete all required sections may result in a significant processing delay.

Note: If the Organization has an FRB-designated Administrator, SecurIDs will be mailed to the Administrator.

Section F: Authorization

- This section should be signed by your organization's official SNC contact with *one exception, as follows*: If the token request is for the SNC contact, a different individual must complete section F. In such instance, the alternate approver may be a senior official within the SNC contact's organization.
- A physical signature is *typically* required (and still preferred); however, in light of widespread remote working arrangements in response to the COVID-19 pandemic, electronic digital signatures will be temporarily accepted with the understanding a physical signature will be requested when normal (pre-pandemic) working arrangements are resumed.

Section F: Authorization

To be completed by the User's Senior Officer/Director/Authorized Designee (Required for new or replacement requests). NOTE: The Senior Officer/Director/Authorized Designee must be a senior level official of the organization and at least two supervisory levels above the User.

I request approval for the above-named employee to be issued a SecurID to access FRB systems. I have determined that the above-named employee meets the conditions for access described in the Access Agreement between my organization and the FRB. I, or my organization FRB-designated Administrator, will notify the designated FRB contact as soon as the above-named employee leaves my area of responsibility, or no longer requires a SecureID to access FRB systems to perform his or her work.

Senior Official _____

Signature

Date

Print Name

Section G: SecurID User Agreement

To be completed by the User (Required for new or replacement requests)

As a condition for access, Users must abide by all FRB requirements that apply to the SecurID and to the FRB system or website that is being accessed. These requirements include, but are not limited to, agreeing that he/she:

1. Will not either directly or indirectly (such as by providing an electronic gateway), use his/her SecurID to allow others to access the Board's computers, networks, or databases.
2. Will not allow anyone to use his/her SecurID for any reason.
3. Will not leave his/her SecurID unattended in an unsecured location and will assume personal responsibility for the safekeeping of his/her SecurID.
4. Will establish and protect the secrecy of his/her PIN number (which is required to operate the SecurID) and will not share his/her PIN number with anyone.
5. Will immediately return the SecurID to the FRB or to his/her organization's FRB-designated Administrator when access is no longer required, employment is terminated, or upon request by the FRB.
6. Will take all necessary precautions to minimize the risk of virus infection to the Board's systems.
7. Will connect to the Board's computers, networks, or databases using a device owned by the employee's employer.
8. Will not attempt to circumvent any FRB authentication and authorization processes and procedures.
9. Will not leave his/her computer unattended and active in a manner that is vulnerable to unauthorized access to the FRB's systems.
10. Will immediately contact the FRB or his/her organization's FRB-designated Administrator if any of the following events occur:
 - his/her SecurID is lost, stolen, damaged, or broken;
 - his/her employment status changes;
 - he/she is unable to recall the PIN number or other access code; or
 - he/she suspects or knows unauthorized use of his/her SecurID is occurring or has occurred.

I have read this SecurID User Agreement. I understand that by accepting a SecurID to access the FRB's systems, I am agreeing to abide by the FRB's requirements, including the requirements described above. I understand that unauthorized access to the FRB's systems is a federal crime under 18 U.S.C. 1030. I also understand that violating any of the FRB requirements for access may result in revocation of my SecurID and my FRB access privileges and may also result in legal prosecution.

User _____

Signature: _____

Date: _____

Print Name: _____

Section G: User Agreement -

- Sign and print name (to be signed by the "user" as identified in section D)
- A physical signature is *typically* required (and still preferred); however, in light of widespread remote working arrangements in response to the COVID-19 pandemic, electronic digital signatures will be temporarily accepted with the understanding a physical signature will be requested when normal (pre-pandemic) working arrangements are resumed.