

TEAM Training for Local Security Managers

The User Management Process

Last update 9/20/2006

Why ?

- A 2005 audit identified that we did not follow a secure overall process for user management in TEAM. We need:
 - Standard practices / form
 - A method to ensure that TEAM users are who they say they are
 - Internal controls for Staff access and authorization

Local Security Manager Responsibilities

- First line of defense against fraud or other systems misuse
- Ensure the accurate completion, processing, and filing of all TEAM user access forms
 - And OASIS employee separation notices
- Notify Administrative Officer (AO) of all Staff TEAM Users (for OASIS TEAM User Group)
- Reset passwords for users assigned by your office

Managing Users is a BIG JOB!

Active Users, 9/20/2006		User Type			
Cost Center Name	Cost Center Code	FTA	Recipient	Contractor/Auditor	Grand Total
TAD	TAD	46	1	5	52
TCC	TCC	7			7
TPACA	TPACA	4			4
TPM	TPM	106	39	54	199
TBP	TBP	40	2	12	54
TRI	TRI	77	110	7	194
TCR	TCR	17		2	19
TAD Central	TAD Central	11		3	14
TPE	TPE	27			27
LMRO	LMRO	9	8		17
TSS	TSS	8	1		9
TRO1	TRO1	15	162	1	178
TRO2	TRO2	33	176	27	236
TRO3	TRO3	24	296		320
TRO4	TRO4	29	684	1	714
TRO5	TRO5	28	715	1	744
TRO6	TRO6	22	327	1	350
TRO7	TRO7	16	118		134
TRO8	TRO8	14	109		123
TRO9	TRO9	31	506	3	540
TRO10	TRO10	22	381		403
Grand Total		586	3,635	117	4,338

The TEAM User Access Forms

- Package posted:
 - TEAM Home Page, FTANet, and FTA Public Website
- Includes 2 Forms:
 - Staff/Contractor/Auditor
 - Grantee
- Includes Complete instructions:
 - Which form to use
 - Where completed forms go for processing
 - What additional documents may be needed
 - What Authorizations may be necessary

Local Security Managers

- In the TEAM User Access Form Instructions
- Listed on the TEAM Home Page

<http://ftateamweb.fta.dot.gov/frames.htm>

Staff Forms

- All staff access to TEAM should be signed by their supervisor
- Special access to job-specific functions should be signed by an HQ representative for that function (*Authorizations for Special Functions, page 18*)
 - Accounting Functions
 - Legal Signoff
 - Civil Rights Functions
 - PIN Number for Obligation Activities, Earmark Management, etc
- Notify Administrative Officer to add new staff to OASIS TEAM User Group

Contractor Forms

- Contractors acting as FTA staff who require access to TEAM MUST be Authorized by their Contracting Program Manager.
 - Example – Triennial Review Contractor must be Authorized by Triennial Review Program Manager

Auditor Forms

- Auditors who require access to TEAM MUST be Authorized by the FTA Audit Liason in TBP.
- This access should be promptly removed when audit activities are complete.

Grantee Access

- Ensure that Grantee Users are authorized to have the functions they are requesting
- Have the grant manager sign off to ensure they 'are who they say they are'
- Make sure 'Designation of Signatures' are on file for users "PINning" on behalf of others in their office

Good Practices

- Add notes to the user record to note user record activities, password resets, access changes, etc.
- Use TEAM to notify user of username and password.
- DO NOT put a username, and password in the same email.
- DO NOT email a PIN, send it to the snail mail address on file, or leave it in a voice mail box with a matching name for the user account.
- DO NOT change email address without verifying user identity
- Attach scanned user access forms to the user record, if possible

More Good Practices

- Do NOT add/modify users without proper documentation
- Do not reset email addresses or passwords without verifying user information.
- If you aren't sure about a user – ask questions!
- Always err on the safe side – collect another signoff or ask another question

Example: Password Reset

- A user calls and asks to reset their password. You should:
 - Pull their user file
 - Ask them for the last 4 digits of their SSN (or other memorable number as recorded on their User form)
 - Verify their office phone and address
 - Verify email
 - Send new password to the email address on file using TEAM

What does this do?

- It ensures the person who is calling is the person who should be using the account
- It ensures that the information remains accurate in TEAM

Staff/Contractor/Auditor Form

- Collect the form
- Verify the information & Authorizations



Multiple Authorizations may be required for special access!

- LSM signs as FTA Operational Approval
- Process the form in TEAM (Verify & Certify!)
- File the form (attach in TEAM, keep on 'paper' file until user account is terminated)
- Local Security Managers must notify your office Administrative Officer to add new users to OASIS TEAM User Group (Staff only)

Transportation Electronic Award Management System (TEAM) Staff/Contractor/Auditor User Access Request

Check Applicable Box:		<input type="checkbox"/> New User With Pin	<input type="checkbox"/> Modify User	<input type="checkbox"/> Username
		<input type="checkbox"/> New User Without Pin	<input type="checkbox"/> Delete User	
Warning: The information contained in this form is protected under Public Law 93-579, Privacy Act.				
USER INFORMATION				
		Gender	M / F (Optional)	
First Name*	MI	Last Name*	Office Phone*	SSN (Last 4 Digits)*
Title		FAX Number		
Organization Name*		Email Address*		
Mailing Address(Street Number, City, State and ZIP Code)*				
		FTA Functional Approval MUST be provided below		
		(see instructions for required approvals and where to submit this form)		
<small>This information is required to establish or modify your TEAM user account. By completing this form, you expressly attest that information provided is true and complete to the best of your knowledge. Invalid information will be grounds for refusal to establish a new user account or the basis for deletion of an existing TEAM account.</small>				
APPLICATION ACCESS (Check all that apply).				
Budget Functions		Accounting Functions		Cost Center (s) (indicate Below)
<input type="checkbox"/> Award (PIN Required)	<input type="checkbox"/> Deobligate	<input type="checkbox"/> Maintain Funds Control (PIN Required)	<input type="checkbox"/> Approve Advice (PIN Required)	_____
<input type="checkbox"/> Approve Budget Revision	<input type="checkbox"/> Maintain Projects	<input type="checkbox"/> Approve Operating Budget (PIN Required)		_____
<input type="checkbox"/> Civil Rights	<input type="checkbox"/> Financial Purpose Transfers			_____
<input type="checkbox"/> Legal Concurrence		Other Functions		Database
<input type="checkbox"/> Earmark Management		<input type="checkbox"/> Help Desk		<input type="checkbox"/> Production
<input type="checkbox"/> Earmark Administration		<input type="checkbox"/> Local Security Manager		<input type="checkbox"/> Quality Assurance
<input type="checkbox"/> Earmark HQ Manager		<input type="checkbox"/> Auditor Access (Inquiry Only)		<input type="checkbox"/> Both Production and QA
<input type="checkbox"/> Earmark Financial Manager		<input type="checkbox"/> Other Rights (Please Describe) _____		
<small>(Underlined Functions require special authorizations. See instructions.)</small>				
ACKNOWLEDGMENT OF RULES OF CONDUCT FOR SYSTEM USE				
As a TEAM user, I understand that I am personally responsible for the use and misuse of my TEAM login ID and password. I understand that by requesting TEAM access and accepting/using such access that I must comply with the following:				
<ol style="list-style-type: none"> When downloading sensitive information, I will ensure that the information has the same level of protection as FTA applications. I will <u>not</u> permit anyone to use my TEAM access information (i.e. user ID, password or other authentication). My password (or other authentication) will be kept private, not stored in a place that is accessible by anyone other than the myself (i.e. family members, friends, etc.). If stored, the password will not be in text format. I will follow standard password procedures and change my password every ninety (90) days. My passwords will be at least eight (8) alphanumeric characters and contain at least one (1) capital letter and one (1) number. I will report any security problems and anomalies in system performance to the appropriate FTA Office. I will notify the appropriate FTA Office to eliminate my TEAM access in the event of job transfer, termination, or if TEAM access is no longer required. I understand that if I am not using FTA-supplied equipment and FTA suffers a security breach or compromise that is my fault, I may be required to allow access to my equipment by authorized representatives of the Federal Government to determine the causes and to take corrective action(s). 				
I agree to and will comply with all of these conditions and understand that failure to do so will result in permanent removal of my TEAM access, and may result in other disciplinary or legal action. By signing my name in the space below, I hereby acknowledge this agreement, and certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same.				
Signature _____		Date _____	Printed Name _____	
FTA AUTHORIZATIONS			FTA Operational Approval	
FTA Functional Approvals, If required by Access Request				
Supervisor/Program Manager Authorization Name/Signature	Date			
TCR Authorization Name/Signature	Date			
TCC Authorization Name/Signature	Date	Signature of Local Security Manager		
TBP Authorization Name/Signature	Date	Printed Name		
TPM Authorization Name/Signature	Date	Title / Office		
TAD Authorization Name/Signature	Date	Date Processed	UserID	PIN

FTA Authorizations

- Identifies the appropriate individuals that must provide signature to authorize access to special functions
- One or more FTA authorizations may be required
 - Attach/file additional authorizing documents as necessary

Supervisor Authorization

- A Supervisor MUST sign to authorize for staff access
- Administrative Officers MUST be notified to add new staff users to the OASIS TEAM User Group

This ensures that the Office maintains awareness of systems access!

Authorization for Special Functions

Regular Access - Employee's Supervisor or COTR

Special Access

- Help Desk Functions/Local Security Manager Functions
 - TEAM Project Manager or Director of Information Technology (TAD)
 - Authorizing Officials: Jacquelynn Lopez, Dave Hostetter
- Accounting and Budget Functions
 - Director of Financial Systems or Director of Budget (TBP)
 - Authorizing Officials: Gwen Daniel, Kristen Clarke
- Earmark Administration Functions
 - Director of Transit Programs (TPM)
 - Authorizing Officials: Mary Martha Churchman, Henrika Buchanan-Smith
- Civil Rights Functions
 - Civil Rights Officer, HQ (TCR)
 - Authorizing Officials: Sandra McCrea, Janice Barnes
- Legal Signoff
 - Chief Counsel or Deputy Chief Counsel (TCC)
 - Authorizing Officials: Dave Horner
- FTA Obligation Authority (Award Access and PIN, also listed on picklist for 'Paper' Grants)
 - Only as indicated in the Federal Transit Administration Delegations of Authority
- Auditor Access
 - FTA Audit Liason (TBP)
 - Authorizing Officials: Felicia Jones

Grantee Form

•Collect the form

•Verify the information & Authorizations



Additional documents may be required for special access!

•LSM signs as FTA Operational Approval

•Process the form in TEAM (Verify & Certify!)

•File the form (attach in TEAM, keep on 'paper' file until user account is terminated)

Transportation Electronic Award Management System (TEAM) Grantee / Recipient User Access Request

Check Applicable Box:		New User With Pin	<input type="checkbox"/>	Modify User	<input type="checkbox"/>	Username	<input type="text"/>
		New User Without Pin	<input type="checkbox"/>	Delete User	<input type="checkbox"/>		
Warning: The information contained in this form is protected under Public Law 93-579, Privacy Act.							
USER INFORMATION							
First Name*		M/I	Last Name*		Gender	M / F (Optional)	
Title		Office Phone*		SSN (Last 4 Digits)*			
Organization Name*		Recipient ID		FAX Number			
Mailing Address(Street Number, City, State and ZIP Code)*		Email Address*		User's Authorizing Signature (see Instructions)			
		Printed Name of above		Date			
<small>*This information is required to establish or modify your TEAM user account. By completing this form, you expressly attest that information provided is true and complete to the best of your knowledge. Invalid information will be grounds for refusal to establish a new user account or the basis for deletion of an existing TEAM account.</small>							
APPLICATION ACCESS (Check all that apply).							
Recipient Access Type		Recipient PIN Functions			Designated Recipient ID(s) (Indicate Below)		
<input type="checkbox"/> Inquiry Only		<input type="checkbox"/> Submit Application			_____		
<input type="checkbox"/> Modify/Update		<input type="checkbox"/> Execute Awards			_____		
		<input type="checkbox"/> Certify as Lawyer			_____		
		<input type="checkbox"/> Certify as Official			_____		
		<input type="checkbox"/> Certify as Both Lawyer and Official			Metropolitan Planning Organization (MPO) ID		
		<input type="checkbox"/> Provide Supplemental Agreement			_____		
<i>(PIN Functions require Designation of Signature Authority on Organization/Agency Letterhead. See instructions).</i>							
ACKNOWLEDGMENT OF RULES OF CONDUCT FOR SYSTEM USE							
As a TEAM user, I understand that I am personally responsible for the use and misuse of my TEAM login ID and password. I understand that by requesting TEAM access and accepting/using such access that I must comply with the following:							
<ol style="list-style-type: none"> When downloading sensitive information, I will ensure that the information has the same level of protection as FTA applications. I will <u>not</u> permit anyone to use my TEAM access information (i.e. user ID, password or other authentication). My password (or other authentication) will be kept private, not stored in a place that is accessible by anyone other than the myself (i.e. family members, friends, etc.). If stored, the password will not be in text format. I will follow standard password procedures and change my password every ninety (90) days. My passwords will be at least eight (8) alphanumeric characters and contain at least one (1) capital letter and one (1) number. I will report any security problems and anomalies in system performance to the appropriate FTA Office. I will notify the appropriate FTA Office to eliminate my TEAM access in the event of job transfer, termination, or if TEAM access is no longer required. I understand that if I am not using FTA-supplied equipment and FTA suffers a security breach or compromise that is my fault, I may be required to allow access to my equipment by authorized representatives of the Federal Government to determine the cause and to take corrective action(s). 							
I agree to and will comply with all of these conditions and understand that failure to do so will result in permanent removal of my TEAM access, and may result in other disciplinary or legal action. By signing my name in the space below, I hereby acknowledge this agreement, and certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same.							
Signature		Date		Printed Name			
FTA AUTHORIZATION							
FTA Functional Approval				FTA Operational Approval			
Signature of Authorizing FTA Official		Date		Signature of Authorizing FTA Official			
Printed Name				Printed Name			
Title / Office				Title / Office			
				Date Processed		UserID	
						PIN	

Designation of Signature

- Template available in User Form Instructions
- Used to delegate signature or “PIN” authority to someone other than the Official Named on the Resolution Authority

Designation of Signature Authority

FTA need not obtain a separate legal opinion for authority of the Applicant's CEO to enter his or her on behalf of the Applicant, PROVIDED THAT:

1. The individual seeking TEAM access is the Applicant's CEO, and
2. IF:
 - A. The Applicant's CEO has selected certs and assurances on behalf of the Applicant for the current fiscal year,
 - B. The Applicant's CEO has entered his or her PIN in the TEAM Affirmation of the Applicant, and
 - C. Either:
 - a) The Applicant's attorney has entered his or her PIN in the TEAM Attorney's Affirmation signifying that the Applicant's actions are authorized by law, or
 - b) The Applicant has on file an Affirmation of the Attorney dated during the current fiscal year, and the CEO has entered his or her PIN in the place for the Applicant's Attorney's PIN.

Notification of Attorney's Affirmation

1. FTA prefers that the Applicant's Attorney enter his or her own PIN in the Affirmation of Attorney.
2. On the other hand, FTA permits the individual authorized to act on behalf of the Applicant to enter his or her PIN on behalf of the Applicant's Attorney, provided the Applicant has on file a current Affirmation of Attorney pertaining to the Applicant's authority to enter into agreements with FTA, comply with Federal requirements, and acknowledging that statements made by person signing the certs and assurances on behalf of the applicant are correct.

(Among other things, this statement implies that only the proper individuals have been authorized to commit an Applicant to comply with FTA's terms and conditions for assistance.)

Authorizing Resolution

- In general, a public body must have an authorizing resolution from its board of directors or be otherwise properly authorized under state and local law before it can take any action.
- Consequently, FTA expects the Applicant/Recipient to retain that resolution in its files, but it is desirable for the Applicant/Recipient to scan it and attach it in TEAM.

TEAM User Security Screens

See the TEAM User Guide located at <http://ftateamweb.fta.dot.gov/static/userguide.html> chapter 10. for detailed walkthroughs of the screens

Salutation:	None	Organization:	
First Name/MI:		Building/Room:	
Last Name:		Address:	
Phone/Ext:		City:	
Alt Phone/Ext:		State/Zip:	0 - 0
Fax:		Routing:	
E-mail:		Acronym:	
Title:			

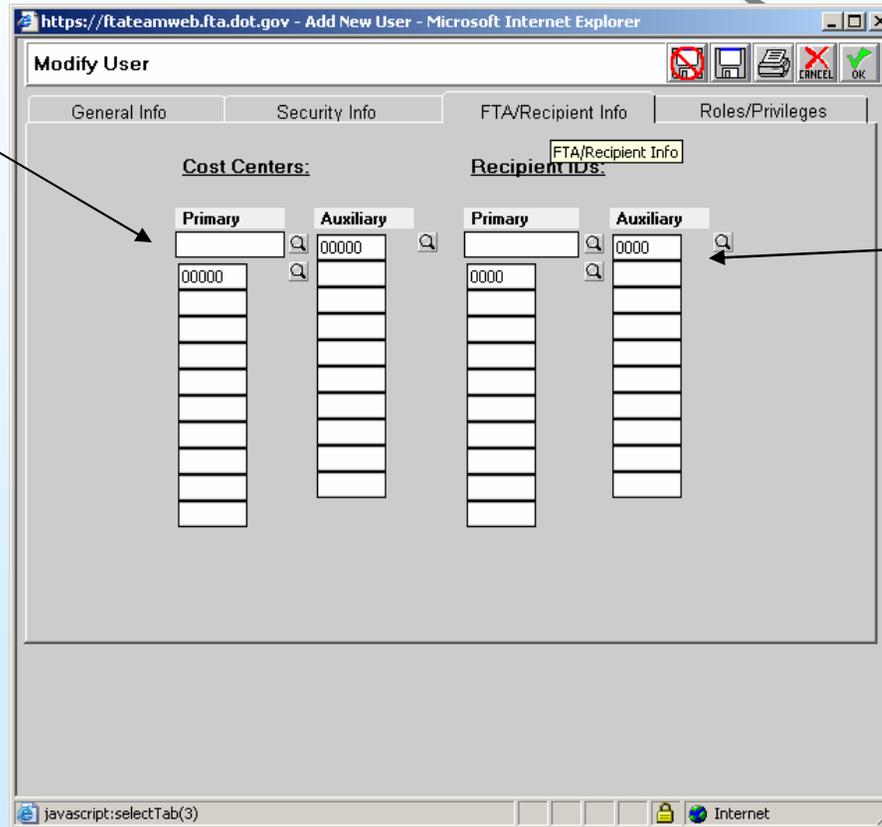
User Iden:	MEHTABS	Last Login:	4/11/2006
Username:	SINGHM		
Created:	7/6/2001	Modified:	7/6/2001
Password:	*****	Changed:	3/23/2006
PIN:	****	Activated:	9/14/2005
Suspended:		Deleted:	
Certified Date:		Certified By	
Remark:			
User Note:			

- Set Password
- Set PIN
- Activate PIN
- Delete PIN
- Delete Account
- Suspend User
- Reactivate User
- Certify User

Click "Certify User" to record that an Authorized User Access form is on file

User Screens, continued

Office or cost centers the user has access to view and/or edit (depending on Roles/Privileges)

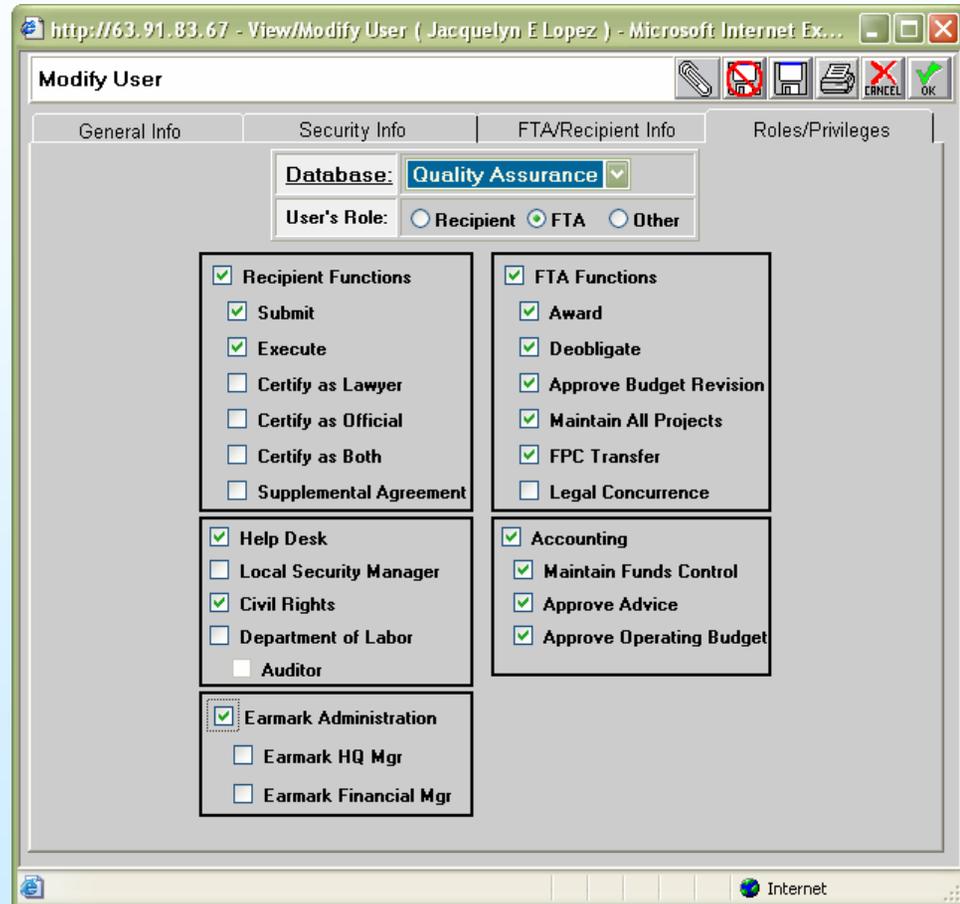


Recipient IDs the user has access to view and/or edit

(depending on Roles/Privileges)

Security Roles/Privileges

- It is important that you understand these boxes and how to accurately reflect the user's job function in both the form and the TEAM user account.
- Security Roles Reference Document located at : <http://ftateamweb.fta.dot.gov /static/Guidance-HQ/>
- Contact the User, the FTA Authorizer, or the TEAM help desk if you are still uncertain of the type of access they need, or how to assign it in TEAM!



Modify User

Database: Quality Assurance

User's Role: Recipient FTA Other

<input checked="" type="checkbox"/> Recipient Functions <input checked="" type="checkbox"/> Submit <input checked="" type="checkbox"/> Execute <input type="checkbox"/> Certify as Lawyer <input type="checkbox"/> Certify as Official <input type="checkbox"/> Certify as Both <input type="checkbox"/> Supplemental Agreement	<input checked="" type="checkbox"/> FTA Functions <input checked="" type="checkbox"/> Award <input checked="" type="checkbox"/> Deobligate <input checked="" type="checkbox"/> Approve Budget Revision <input checked="" type="checkbox"/> Maintain All Projects <input checked="" type="checkbox"/> FPC Transfer <input type="checkbox"/> Legal Concurrence
<input checked="" type="checkbox"/> Help Desk <input type="checkbox"/> Local Security Manager <input checked="" type="checkbox"/> Civil Rights <input type="checkbox"/> Department of Labor <input type="checkbox"/> Auditor	<input checked="" type="checkbox"/> Accounting <input checked="" type="checkbox"/> Maintain Funds Control <input checked="" type="checkbox"/> Approve Advice <input checked="" type="checkbox"/> Approve Operating Budget
<input checked="" type="checkbox"/> Earmark Administration <input type="checkbox"/> Earmark HQ Mgr <input type="checkbox"/> Earmark Financial Mgr	

What's done, what's next?

- 5/15/2006, TAD20 suspended NON-FTA TEAM users who had not been “Certified”.
- On or about 1/8/2007, TAD20 will suspend FTA TEAM users who have not been “Certified”. (Local Security Managers will be notified)
- In response to audit findings in 2006, TEAM User roles will be reviewed, with possible revisions made. (Local Security Managers will be notified)
- All TEAM users will continue to use this form and user management process for any new users, modifications to existing users, or deletions of user accounts.

Questions?

Contact the TEAM Help Desk for assistance!

Hours of Operation

M-F 8:00a.m. to 5:00p.m. (EST)

Telephone Number

888 - 443 - 5305

Email Address

Team.HelpDesk@dot.gov

Clarifications

1. Local Security Managers will generally process the forms in TEAM for the people that work out of their locality. A local Security Manager has authority to add/modify staff users from authorized forms for other offices to TEAM. In any case, be sure to note where the access forms & supporting documentation is filed if it is not attached to the user record in TEAM.
 2. "Grantee User Supervisor" or "FTA Point of Contact" on the User Form
From Linda Sorkin: Please have the CEO, board chair or other delegated authority send us a delegation of signature with an org chart stating that any one who is the supervisor for a TEAM user can sign for that person.
 3. Access to these TEAM Financial Functions now require Accounting/Budget Signoff (Gwen Daniels/Kris Clarke)
 - o Obligation
 - o Deobligation
 - o FPC Transfer
 - o Accounting Functions
 - o Maintain Funds Control
 - o Approve Advice
 - o Approve Operating Budget
 4. The Local Security Manager has the authority to "Certify" that an authorized access form or accompanying documentation is on file. In cases where the form and/or accompanying documentation is expected on or about a certain date, and interruption in TEAM access would cause delays in grant processing, it is at the discretion of the Local Security Manager to "certify" users. In any case, be sure to add notes to the User's record indicating the expected dates of the documentation.
 5. For temporary Local Security access rights to assist in the initial recertification through May of 2006, an email indicating temporary authorization for specific individuals can be sent by Jacquelyn Lopez or David Hostetter in TAD-20 and would serve in lieu of a special form signature.
 6. Local Security Managers have the authority to accept prior forms and authorization materials for users in their Cost Center processed between 4/1/2005 and 3/31/2006. These users can be "Certified" by the Local Security Managers at their discretion based on the existing Authorization Materials provided and remaining on file for that user during this time.
 7. For recertification of existing grantee users, the FTA regional knowledge of grantee's organization may be sufficient basis for accepting the supervisor's signature. For audit purposes, it would be good to attach a copy of the grantee's org chart and/or supervisory chain of command to the recipient profile information. That could be done as a matter of routine business after the certification. Of course, if there is any question about the signature authority, the security manager should request the documentation suggested in the guidance provided following the TPM biweekly conference call and now incorporated in the grantee instructions.
- For certification of new grantee users, the org chart and other evidence of the signature authority should be requested up front at the time of the initial certification.
8. PINs should NOT be emailed. A paper copy can be mailed to the address on the User Account, or a Voice Mail left to an inbox with a matching User Name.

Updates to this document

- 6/29/2006, Lopezj. Updated this document with:
 - updates page 38, a clarifications page 37, and modified the Good Practices page 11 with a bullet on PINS
- 9/1/2006, Lopezj
 - Changes to reflect new earmark administration access and approvals