



**San Francisco Financial Center  
Customer Advisory Board Conference**

**FMS Programs Access  
Workgroup Project Update**

*Wednesday, March 16, 2011*

**Pilar Rowe**

**Brenda Alexander**

**Bill Radford**

# Agenda

- 
- **User Provisioning**
  - **Workgroup Accomplishments**
  - **What does the future hold?**
  - **Let us know!**



# User Provisioning

- **Obtaining Application Access**
- **Removing Application Access  
Recertification and Life Cycle Rules**
- **UPS to ITIM Migration**
- **User Self-Enrollment and User Self-Service**
- **External Administrator Interface**
- **Planned Enhancements**



# Obtaining Application Access

## • Mainframe, Sybase

- Applications such as STAR, PACER, TOP, TRACS
- Each application has its own internal business process for Form
- RFC/Application enters an access request into ITIM
- Application approver has 7 calendar days to approve after request has been entered
- ITIM sends request to Data Access Control Division (DACD) after approval
- DACD completes request and sends access package to users within 7 calendar days



# Obtaining Application Access

- **LDAP Web Based Applications**
  - Applications such as ASAP, ITS, FedDebt, DebtCheck, IPAC etc.
  - Each app has its own internal business process for Forms
  - Will require DEO/Delegated administrator to submit request to provisioning application (UPS or ITIM)
  - Identity will be created in LDAP, SSO account issued and access to application granted via automation from provisioning application. Credentials are sent via email to user



# Obtaining Application Access

- **PKI FOB**

- Each app has its own internal business process for Forms
- DACD does not act on request until they receive fully completed form (must have all signatures)
- Once DACD receives form request is processed in 5 calendar days
- PKI Level 3 package is sent to Trusted Registered Agent (TRA)
- PKI Level 2 package is sent to User



# Removing Application Access Life Cycle Rules and Recertification

- **DEO's/Delegated Administrators can remove access via Provisioning application (UPS or ITIM)**
- **Life Cycle Rules for Mainframe and SSO accounts**
  - Follows FMS policy to disable accounts if not activity for 90 days and remove accounts with no activity for 13 months



# Removing Application Access Life Cycle Rules and Recertification

- **Recertification available via Provisioning Application**
  - During recertification user access is reviewed and removed if no longer needed FMS policy that powerful users be recertified every 6 months and non-powerful users once a year
  - Provisioning application (UPS or ITIM) can automate the process for applications



# UPS to ITIM Migration

- **Preliminary Requirements Questionnaire**
  - Aids in developing proper approach and migration schedule
  - All questionnaires were received by Jan 31, 2011
  - Preliminary review complete
  - Proposed migration schedule created



# UPS to ITIM Migration

- **Applications Interviews**
  - **Meet and Greet - get to know you and your application**
    - **Review proposed schedule and confirm dates for each applications migration**
    - **Review lessons learned from new apps that have been Implemented to ITIM**
    - **Address specific questions and concerns**
    - **Agree on Next Steps**
    - **Plan interviews to be conducted Feb – Apr 2011**



# User Self-Enrollment and Self-Service

- **ITIM User Self-Enrollment**

- Transfers responsibility for initiating the Enrollment Process from the DEO/Delegated Administrator to the user who is requesting access.
- Reduces the workload of the DEO's/Delegated Administrators
- Gives the requestor ownership of the process
- Eliminates paper forms
- Streamlines the process by reducing the overhead that may occur while waiting for a DEO to enter the requestor's data



# User Self-Enrollment and Self-Service

- User will be granted an Identity/Profile, ITIM account and Single Sign-On account
- User will be sent link to access User Self-Service to continue request for access to your specific application



# User Self-Enrollment and Self-Service

- **ITIM User Self-Service** feature allows users to reset SSO passwords, change personal information, request additional access to applications, and ability to access and respond to “to do” items
- **User Self-Enrollment** is currently available for ITIM managed Web applications



# External Administrator Interface

- The ITIM External Interface is a custom built application with built-in security controls
- It allows for DEO's/Delegated Administrators and Approvers to log into ITIM on behalf of their application to request access for application users



# External Administrator Interface

- **Allow DEO's/Delegated Administrators to run reports from WebFocus**
- **This interface was mainly designed be used FPA's and Financial Institutions**
- **Only specific application owners and users with specific assigned roles may access it**

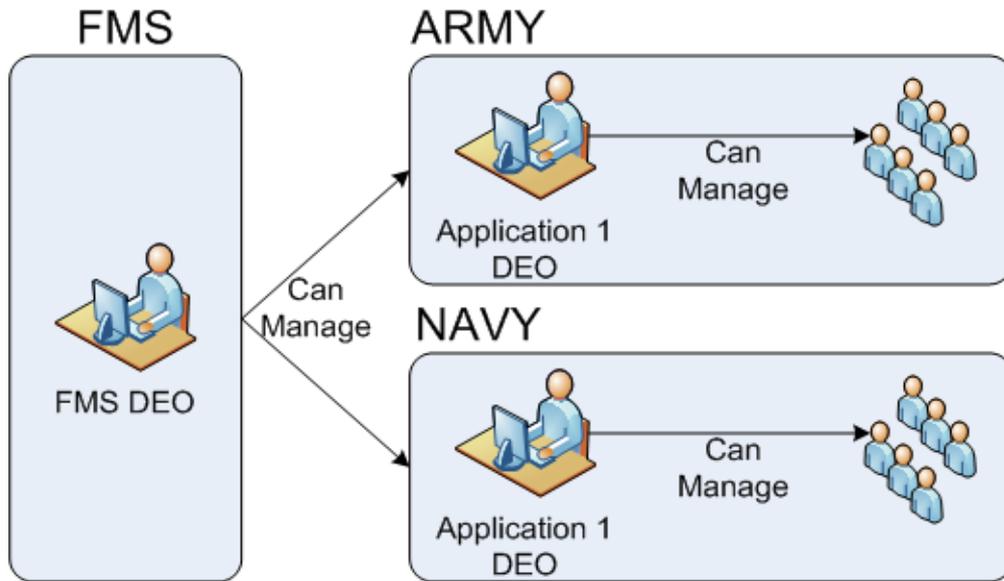


# Organizational Silos

- Application DEOs can only be granted access to manage an organization by an existing DEO authorized to manage the organization
- Application DEOs can only set a new person's organization to one of the organizations they're authorized to manage
- If a person moves between organizations, an FMS DEO must make the modification to the person's organization



# Organizational Silos

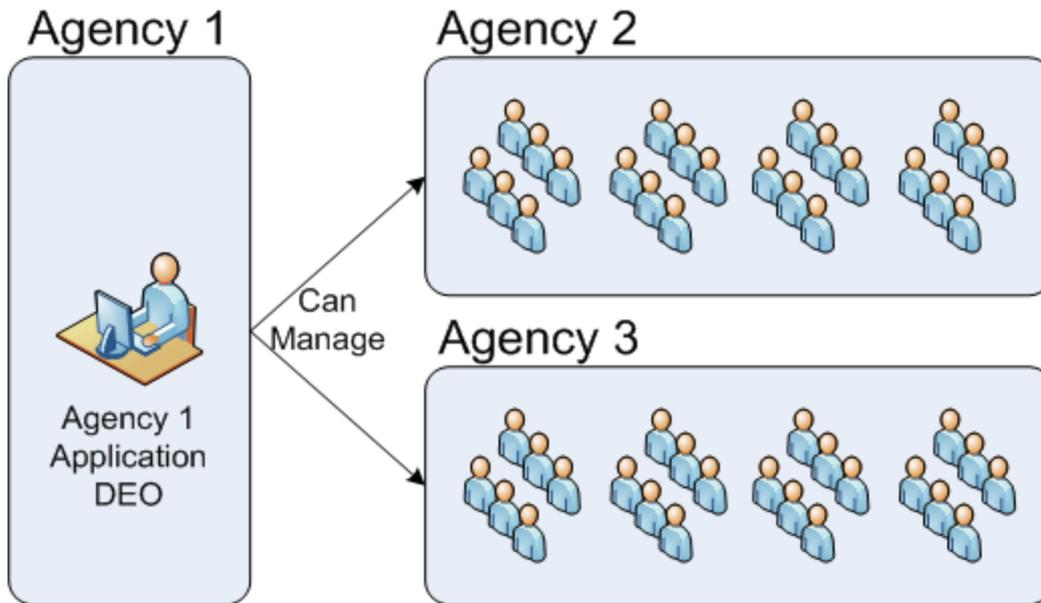


- Army “Application 1 DEO” can only create DEOs that can manage Army
- Army “Application 1 DEO” can only view identities and create accounts for Army users
- Navy “Application 1 DEO” can only create DEOs that can manage Navy
- Navy “Application 1 DEO” can only view identities and create accounts for Navy users



# Organizational Silos (Cross-Agency Administration)

- Multiple organizations' application access may be managed by a single entity if appropriate



- In this example, a DEO at Agency 1 is responsible for providing access to an application across for Agency 2 and Agency 3



## Other Planned ITIM Enhancements

- Full Integration with WebFocus for reports – March 2011
- Provisioning to Mainframe – December 2011
- Full Support for Role Based Access Control – Date TBD



# Other Planned ITIM Enhancements

- Full support PIV PAC&LACS for Internal FMS Employees and Contractors – In Progress
- CASE Application: In support of HSPD-12, ITIM is configured to accept credentials from external agencies to create identities and populate FSLDAP – Full Rollout TBD



# What has been accomplished?

- Consolidated Web Page
- Single Sign On



# What has been accomplished?

About FMS

**FINANCIAL MANAGEMENT SERVICE**  
A Bureau of the United States Department of the Treasury  
[fms.treas.gov](http://fms.treas.gov)

[Home](#) | [FAQ's](#) | [Training & Events](#) | [Publications](#) | [Programs](#) | [About FMS](#) | [A-Z Index](#) | [Navigation Help](#)

[Advanced Search](#) | [RSS](#) | [Subscribe](#) | [Contact FMS](#)

[▶ FIRST-TIME VISITORS](#)

[▶ GOVERNMENT AGENCIES/  
FINANCIAL INSTITUTIONS](#)

[▶ FMS PUBLICATIONS](#)

[▶ FMS PROGRAMS](#)

[▶ FMS SYSTEMS ACCESS](#)

[▶ SEARCH](#)

[▶ SUBSCRIBE](#)

---

[▶ FMS Overview](#)  
[▶ Navigating the FMS Web Site](#)  
[▶ FMS Organization](#)  
[▶ Fact Sheets](#)  
[▶ Strategic Plan](#)  
[▶ Legislative & Public Affairs](#)  
[▶ Locations & Directions](#)

**Quick Navigation**

**Links to Information on FMS Systems for Federal Program Agencies and Financial Institutions**

The table below contains enrollment and contact information for FMS online applications.

Application/ Forms Link	Contact Information	
ASAP (Federal Program Agencies) <a href="#">Forms</a>	(202) 874-6542	<a href="mailto:carole.cole@fms.treas.gov">carole.cole@fms.treas.gov</a>
ASAP (Recipient Organizations) <a href="#">Forms</a>	(202) 874-6542	<a href="mailto:carole.cole@fms.treas.gov">carole.cole@fms.treas.gov</a>
Card Acquiring Service <a href="#">Forms</a>	(202) 874-0807	<a href="mailto:dena.corson@fms.treas.gov">dena.corson@fms.treas.gov</a>
CASHLINK II (Federal Program Agencies) <a href="#">Forms</a>	1 (800) 346-5465	<a href="mailto:cashlink2@pnc.com">cashlink2@pnc.com</a>
CASHLINK II (Financial Institutions) <a href="#">Forms</a>	1 (800) 346-5465	<a href="mailto:cashlink2@pnc.com">cashlink2@pnc.com</a>
DebtCheck	(202) 874-0540	<a href="#">Comment Form</a>
EFTPS <a href="#">Forms</a>	1 (800) 982-3526	<a href="mailto:eftps.questions@fms.treas.gov">eftps.questions@fms.treas.gov</a>
ETA (Financial Institutions) <a href="#">Forms</a>	1 (888) ETA-FRBK (382-3725)	
ETA (Individuals) <a href="#">Forms</a>	1 (888) 382-3311	<a href="http://www.eta-find.gov">http://www.eta-find.gov</a>



# What has been accomplished?

- **Single Sign On**
  - **What is Single Sign On?**
    - Single Sign On is an authentication service offered by FMS
    - Customers log in once with a single credential and can access multiple FMS applications Single Sign On supports users from all branches of Government, Financial Institutions, Private Collection Agencies, State & Local Governments, Non-Profits, Educational Institutions, Corporations, and the General Public



# What has been accomplished?

- **Single Sign On Service**
  - Single Sign On supports three types credentials for authentication:
    - SecurID Passcode and Token
    - PKI Certificate
    - User ID and Password



# What has been accomplished?

- **What applications use SSO today?**

- Debit Gateway (4)
- DebtCheck (4)
- TCIS (4)
- JFICS (3)
- TOP/CTS (3)
- Cashtrack (2)
- FedDebt (2)
- SAM (2)
- FIRST(SID) (2)
- SIMS IV (2)
- GWA (2)
- ITIM (2)
- TROR (2)
- UPS (2)

– You will not be prompted to log in again as long as the application does not require a higher protection level.



# What has been accomplished?

**fms** [Change Password](#) [Forgot your Password?](#) [Forgot your User Id?](#) [Register](#) [?](#)

**Enterprise Single Sign On**

Log In To: [https://tolar.fms.treas.gov/enrole/custom\\_logon](https://tolar.fms.treas.gov/enrole/custom_logon)

Select an authentication method and enter your credentials

<b>Log In using your FMS:</b>	<p>To log in using your FMS Single Sign On User ID and Password, please enter your User ID and Password.</p> <p>User ID: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Log In"/> <input type="button" value="Reset"/></p> <p><a href="#">Forgot your User Id?</a></p> <p><a href="#">Forgot your Password?</a></p>
<b>SSO User ID and Password</b> ▶	
<a href="#">SecurID Token</a>	
<a href="#">PKI Certificate</a>	

**WARNING**  
**WARNING**  
**WARNING**

You have accessed a United States Government computer. Unauthorized use of this computer is a violation of federal law and may subject you to civil and criminal penalties. This computer and the automated systems, which run on it, are monitored. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. Communications made using this system may be disclosed as allowed by federal law.

[Accessibility](#) | [Contacts](#) | [Privacy Policy](#)  
U. S. Department of the Treasury - Financial Management Service



# What does the future hold?

- Improvements to the web page
- HSPD-12
- CASE
- Fiscal IT



# What does the future hold?

- **Improvements to the web page**
  - Addition of more application information to the page
  - Addition of prerequisites that are required before requesting access to certain applications
  - Addition of information regarding the average time it takes to gain access to a specific application



# What does the future hold?

- **Homeland Security Presidential Directive 12**
- **HSPD-12's objective is to standardize the forms of identification used by the Federal Government to identify its employees and contractors (sometimes known as PIV – Personal Identification Verification)**



# What does the future hold?

- Applies to identification presented for physical access to government facilities, as well as, logical access to government computer systems
- Applies to:
  - “Executive departments” and agencies listed in title 5 U.S.C. § 101, and the Department of Homeland Security; “independent establishments” as defined by title 5 U.S.C. §104(1); and the United States Postal Service (title 39 U.S.C § 201).
  - “Government corporations” as defined by title 5 U.S.C. § 103(1) are exempt, but encouraged to comply
  - Legislative and Judicial Branches are also exempt from compliance



# What does the future hold?

## Types of Personal Identification Verification (PIV) Cards



PIV Compliant Card	PIV Interoperable Card	PIV Compatible Card
•Can only be issued by Federal Entities	•Can only be issued from a CA cross-certified with the Federal Bridge for PIV-I	•Can be issued by anyone
•Requires a National Agency Check with Written Inquiries (NACI)	•Does not require a National Agency Check with Written Inquiries (NACI)	•Does not require a National Agency Check with Written Inquiries (NACI)
•Are interoperable with and trusted by <u>all</u> Federal government relying parties	•Issued in a manner that <u>allows</u> Federal government relying parties to trust the card if they choose	•Has <u>not</u> been issued in a manner that assures it is trustworthy by Federal government relying parties
•Fully complies with all aspects of FIPS 201	•Follows FIPS 201 technical specification	•Follows FIPS 201 technical specification
•Must follow the card layout in FIPS 201	•Must be visibly distinct from a PIV Compliant Card	•Must be visibly distinct from a PIV Compliant Card



# What does the future hold?

- **HSPD12**

- Treasury IT Security Policy allows Treasury to accept PIV Compliant and PIV Interoperable credentials for multi-factor authentication to systems
- For customers who are not required to comply with HSPD-12 but require multi-factor authentication to our systems, we are investigating the use of PIV Interoperable Cards
- Example:
  - Veterans Affairs – PIV Compliant
  - SSA – PIV Compliant
  - FRB – Investigating PIV Interoperable
  - US Courts – Investigating PIV Interoperable



# What does the future hold?

- **What will I need to use my PIV Card for access to FMS applications?**
  - Activated PIV Card from your Agency
  - Smartcard reader attached to your workstation
  - Ability to log into your workstation or agency hosted web applications with your PIV Card



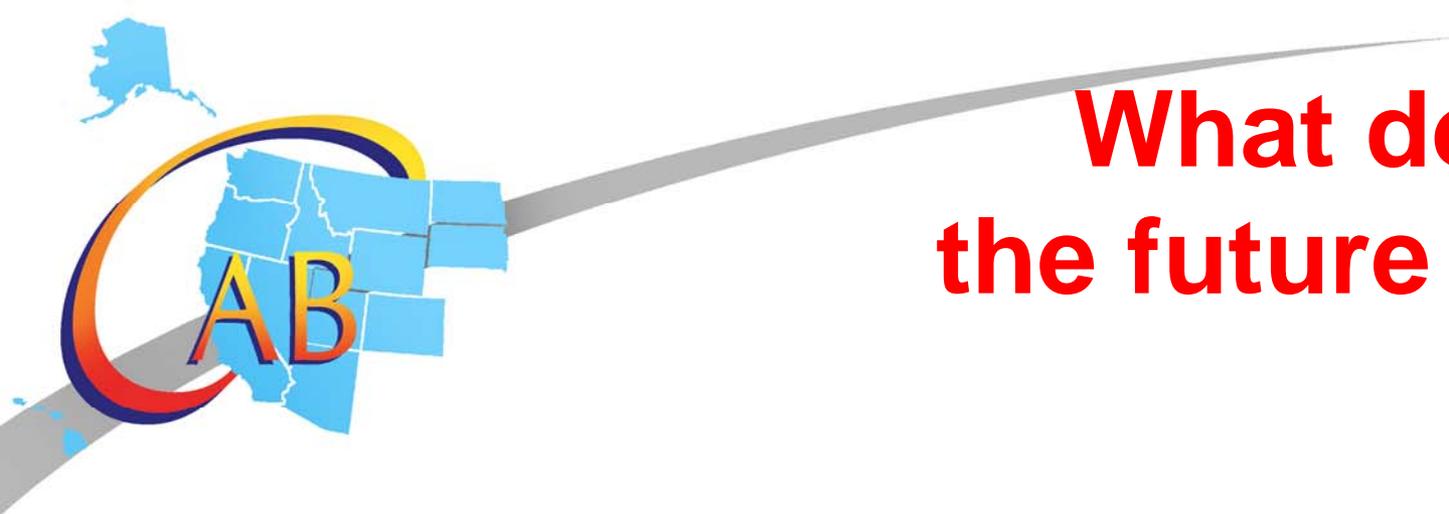
# What does the future hold?

- **Certificate Activation and Self-Enrollment (CASE)**
- **Activation**
  - User already has access to FMS applications and an SSO account.
  - Allows the user to transition from username/password, SecureID or Fiscal Service PKI to PIV for FMS application access



# What does the future hold?

- **Certificate Activation and Self-Enrollment (CASE)**
- **Self-Enrollment**
  - Allows a new customer to enroll for FMS application access using the PIV card.
  - Once the enrollment is complete AND the user has been provided authorization for their application, the PIV card used during enrollment can be used to authenticate to the application via SSO.



# What does the future hold?

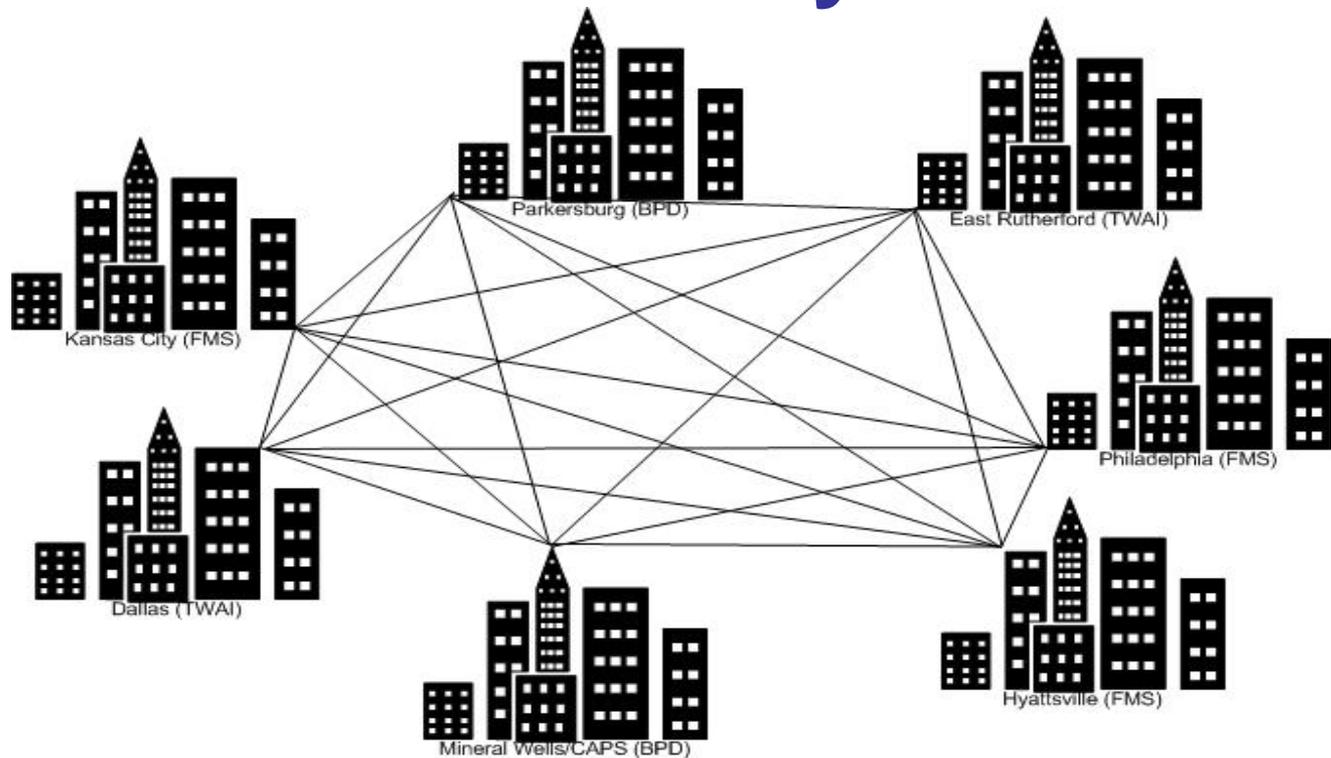
- **Fiscal IT**

- An effort to reduce the number of data centers within Treasury
- FMS and BPD (Bureau of Public Debt) will consolidate Information Technology services under one umbrella



# What does the future hold?

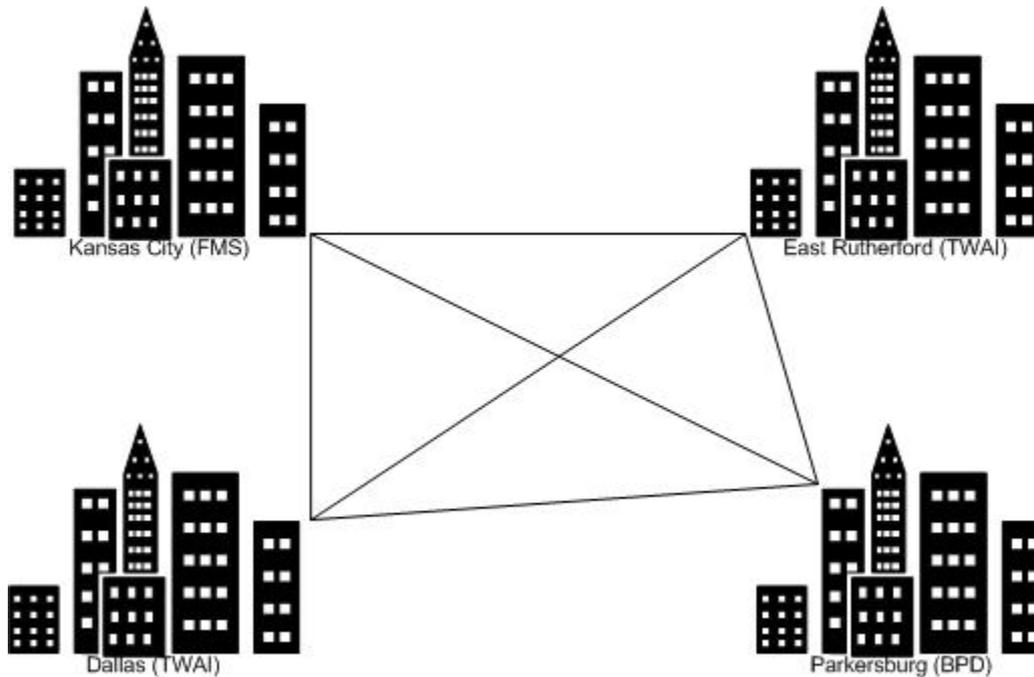
- Fiscal IT Today





# What does the future hold?

- **Fiscal IT Tomorrow**





**Let Us Know!**

*We want to hear from you  
about what things you want to  
FMS to accomplish in order  
to make your job easier.*