

WELCOME TO THE ANNUAL DEPARTMENT SECURITY OFFICER BRIEFING

March 22, 2013

COMMONWEALTH OF MASSACHUSETTS

OFFICE OF THE COMPTROLLER
INFORMATION TECHNOLOGY DIVISION



Follow us
on Twitter
@MA_Comptroller



Agenda

- CTR Annual Security Update
 - Scott Olsen, Director of Department Assistance
- MMARS Security
 - Dan Frisoli, CTR Security Administrator
- HR/CMS Security
 - Lenny Montone, CTR Systems Security Analyst
- ITD Annual Update
 - Kevin Burns, Commonwealth CISO
- Identity and Access Management
 - Darrel Harmer, Chief Capital Planning Officer
 - Raoul Sevier, MMIS Engineer
- Wrap Up and Questions



CTR ANNUAL SECURITY UPDATE

Scott Olsen

Director of Department Assistance Bureau

Office of the Comptroller



Security Officer Responsibilities

- Obtain UAIDs
- Assist Management in identifying roles for personnel
- Assist Management in identifying individuals as Authorized Signatories and obtain evidence of the Department Head approval prior to the request for such designation.



Security Officer Responsibilities

- Request access and assign roles for HR/CMS, CIW, and DocDirect via the ITD InTempo application.
- Request access and assign roles for MMARS using the UDOC MMARS transaction.
- Process role and DHSA changes using the UDOC MMARS transaction.



Security Officer Responsibilities

- Attend all Security related meetings and training sessions, train staff as part of the assignment and ongoing maintenance of security roles, and periodically reminds staff of the responsibilities related to security access, Administrator role responsibilities, electronic signatures for MMARS documents and the duty to comply with state finance law.
- Maintain communication with the Security Administration Unit in the Office of the Comptroller (CTR) and ITD on all security related issues.



Security Officer Responsibilities

- Monitor the Department's organization for any changes that should impact a user's access, such as termination of an employee or changes to an employee's duties.
- Notify CTR of any situation which requires immediate deactivation of a user's access to MMARS and HR/CMS.
- Notify ITD of any situation which requires immediate deactivation of a user's access to CIW, InTempo, and Doc Direct.



Security Officer Responsibilities

- Perform password resets for users in the department as needed.
- Complete the Annual Department Security Officer Review of Enterprise Security Systems for staff access.
- Facilitate the Annual Department Head Approval of Enterprise Systems Security during the Close/Open period.....



Security Officer Responsibilities

...and your regular day job.

Thank You!



DEPARTMENT HEAD ANNUAL SECURITY REVIEW AND APPROVAL



Department Head Security Review and Approval

- Review of systems security is key to assuring that access reflects current responsibilities and changes in personnel
- Formally two times a year
- Reports available monthly



Annual Department Head Security Review and Approval

- Announced via Fiscal Year Memo in May
- Due by June 28th

- MMARS/LCM
 - SECMMARS
- HR/CMS
 - SECHRCMS
- CIW
 - SECCIW
- InTempo
 - SECINTEM



Security Reports

- SECMMARS, SECHRCMS, SECCIW, SECINTEM
 - Run Monthly, twice during review periods
- Access can be granted to Dept Heads, CFOs, and Primary DSOs
- Granting access to SEC reports is DSO responsibility



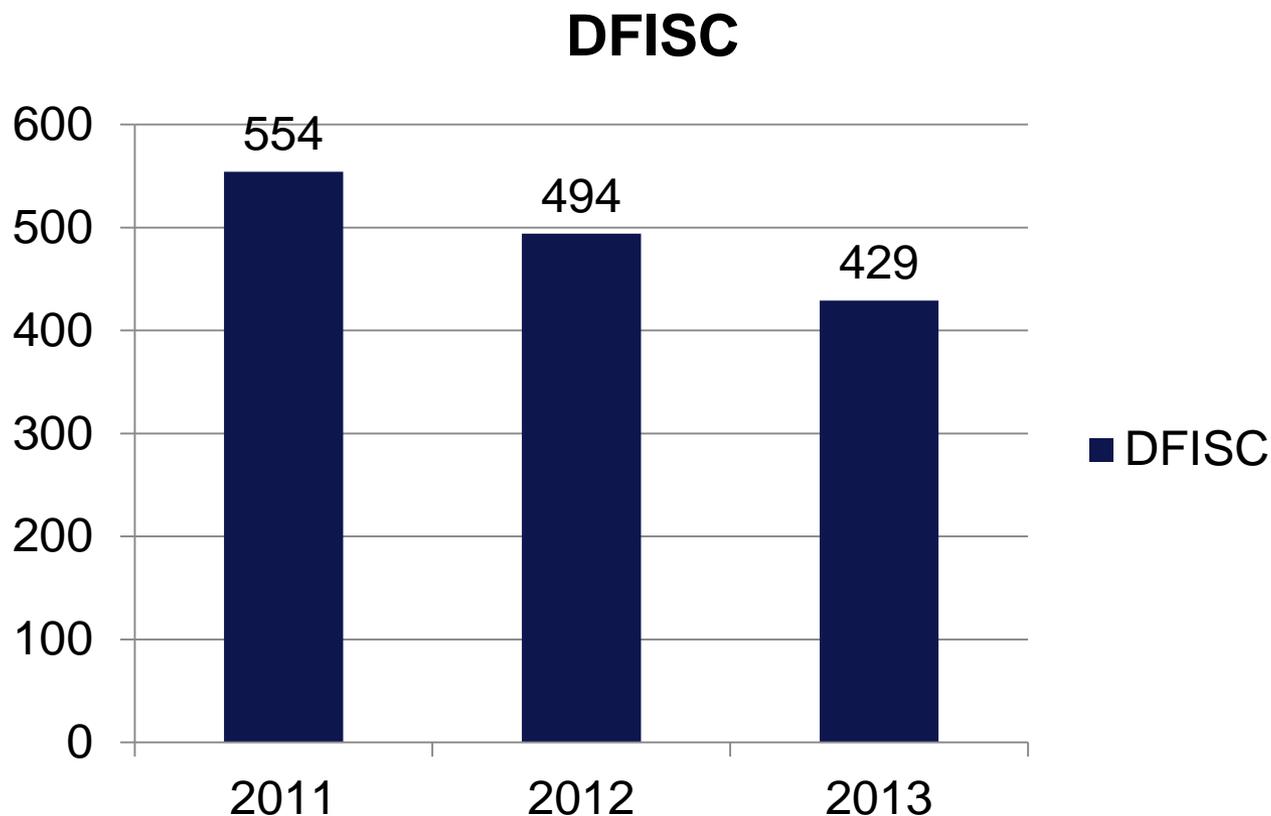
Department Head Security Review and Approval

- Certification must come directly from the Department Head, either as an e-mail from their account or as a hard copy with the Department Head's signature. Use the Department Head Annual Approval of Statewide Enterprise Systems Security Form
- Latest enterprise security reports available via DocDirect
- The Comptroller's Office for MMARS or HR/CMS issues Dan Frisoli (617) 973-2614 or Lenny Montone (617) 973-2570
- ITD for CIW and InTempo, CommonHelp (866) 888-2808



DFISC - Fiscal Admin for All Functions

- Reduce DFISC as part of annual review



DFISC - Fiscal Admin for All Functions

- All requests for DFISC will be initially rejected pending adequate justification
- DSOs should work with management to determine the appropriate roles for users

Summary of High-Level Roles

Total MMARS Processors	78
Total DFISC Staff	7
DFISC Staff Percentage	8.97%
Total AP and Encumbrance Admin Staff	16
AP and Encumbrance Admin Staff Percentage	20.51%

Summary of High-Level Roles

Total MMARS Processors	31
Total DFISC Staff	2
DFISC Staff Percentage	6.45%
Total AP and Encumbrance Admin Staff	2
AP and Encumbrance Admin Staff Percentage	6.45%



Updated Form

Department Head
Annual Approval of Statewide Enterprise Systems Security
CIW, HRCMS, MMARS & InTempo

- 1) **REVIEW** security reports for each enterprise system generated for your department. If changes are necessary, contact the appropriate system security administrator and submit all change requests for staff access as appropriate.
- 2) **SUBMIT** this completed form to SecurityRequest@MassMail.State.MA.US by the due date indicated below.

I have reviewed all statewide enterprise system security reports for (3 letter dept code)_____ and I personally approve all statewide system accesses for agency staff to CIW and HRCMS, and approve all security roles and Department Head Signature Authorization Designations (DHSA) in MMARS. If I have made changes to security access for any enterprise system, these changes have been submitted to the appropriate system security administrator. This approval, along with any changes that may have been made as well as all restrictions and limitations, have been incorporated in our Departmental Internal Control Plan as mandated. I understand that failure to submit this approval evidence form to the Office of the Comptroller by the due date indicated above may result in delays in processing department requests.

I certify my Department has a process in place to monitor and review all user activity in MMARS.



User Activity Report

NMF580W

Report ID: NMF580W

Run Date: 3/13/2013

Run Time: 03:45 PM

COMMONWEALTH OF MASSACHUSETTS
MMARS User Activity Report
TRANSACTIONS PROCESSED FEBRUARY 2013

<u>Created By</u>	<u>DFISC</u>	<u>DHSA</u>	<u>DOC TYP</u>	<u>Transactions</u>	<u>Submitted By</u>
	Yes	No	CR	1	
	Yes	No	CT	1	
	Yes	No	GAX	1	
	Yes	No	GAX	3	
	Yes	No	IE	2	
	Yes	No	IE	1	
	Yes	No	ITA	3	
	Yes	No	ITA	1	
	Yes	No	PRC	1	
	Yes	No	PRC	18	
	Yes	No	VCC	5	
	Yes	No	VCM	1	
	Total Transactions for [REDACTED]:			<u>38</u>	
	Yes	No	UDOC	1	
	Total Transactions for [REDACTED]:			<u>1</u>	
Total Transactions for Department [REDACTED]:				39	



Segregation of Duties Report

NMF581W

Report ID: NMF581W

Run Date: 3/13/2013

Run Time: 04:10 PM

COMMONWEALTH OF MASSACHUSETTS
VERIFICATION OF SEGREGATION OF DUTIES: ENCUMBRANCES AND PAYMENTS
TRANSACTIONS PROCESSED JULY 2012

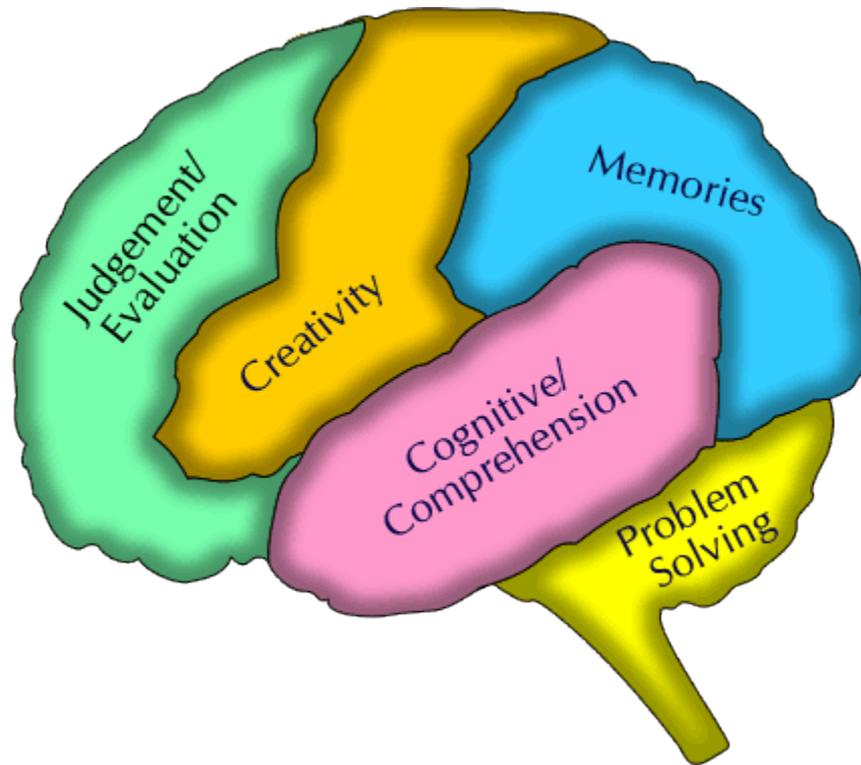
<u>Encumbrance Submitter</u>		<u>DFISC</u>	<u>DHSA</u>			
		Yes	No			
<u>Payment Document</u>	<u>Encumbrance Document</u>			<u>Encumbrance Creator</u>	<u>Payment Creator</u>	<u>Payment Submitter</u>
GAX 3184003XXXXXXXX070212	GAE 3184003XXXXXXXX070212					
GAX 3205001XXXXXXXX072312	GAE 3205001XXXXXXXX072312					
Total Encumbrances Created By User				:	2	
Total Encumbrances Created By Department				:	2	



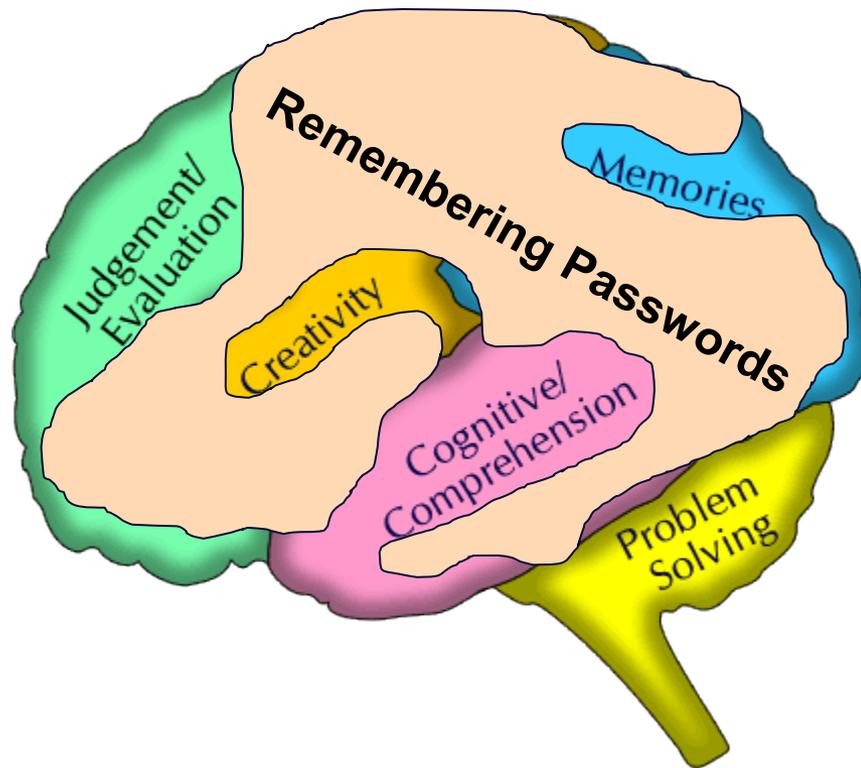
PASSWORD MANAGEMENT



The Past



Today



Password Management

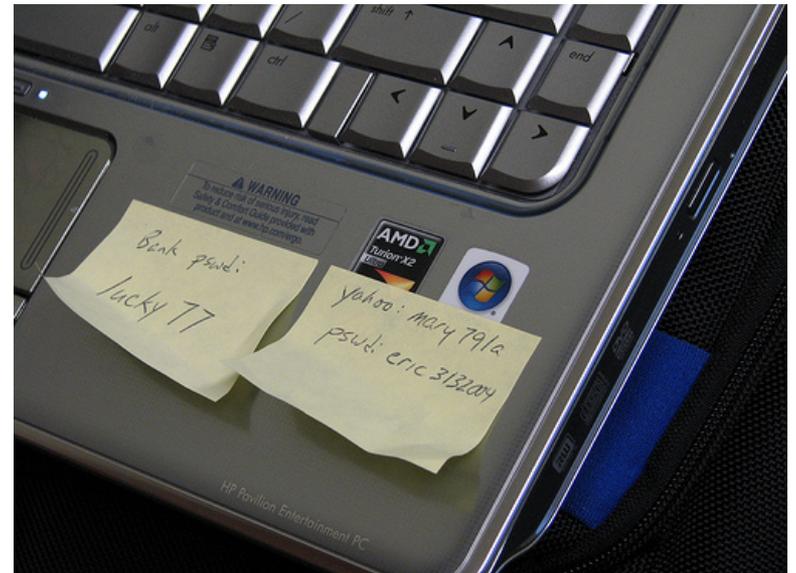
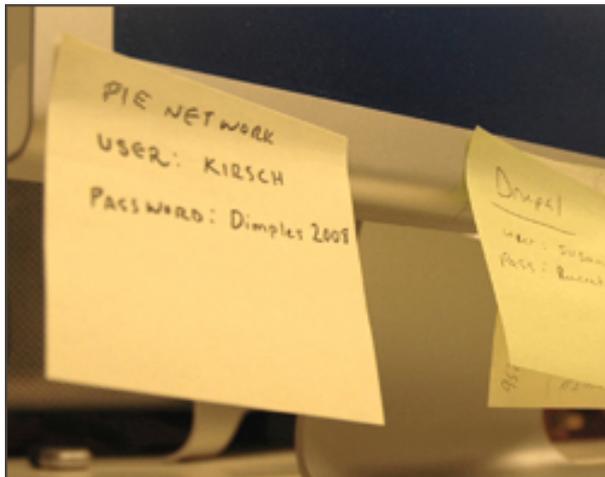
- Sharing of security system IDs (UAIDs, passwords, etc.) is prohibited
- See Security Guide for password conventions



(@n Y0u R3@d Th1\$?

- Use a strong password containing numbers, letters and special characters
- Don't be obvious (names, birthdays, SS#)
- Change it regularly
- Use a completely unique password for each account
- Never write a single one down
- Don't let the browser "remember" passwords
- Don't just change the last # (i.e. redsox01, redsox02, redsox03....)





WORST PASSWORDS OF 2012

rank	password	change from 2011
#1	password	—
#2	123456	—
#3	12345678	—
#4	abc123	⤴1
#5	qwerty	⤵1
#6	monkey	—
#7	letmein	⤴1
#8	dragon	⤴2
#9	111111	⤴3
#10	baseball	⤴1

legend:

unchanged — up ⤴# down ⤵#



UDOC

- Rejection rate remains 25%
- Most common reason for reject
 - Not 'locking' and 'inactivating' on a user delete request
- Additional Training this year



Emergency Deletions

- Contact us via phone with any emergency deletion requests
- CTR will immediately deactivate and ask for email as authorization



PartnerNet

- Add Users
- Password Resets
 - Remind users of password self service
- Request Dropbox and Application access via CTR form
- Increase in activity (ICQ, new documentation)



InTempo

- First step in the process
 - Request UAID from ITD
- Match application access
 - Check off “MMARS” and “PartnerNet” when applicable
- Use assigned UAID in UDOC request
- Delete in both InTempo and MMARS (UDOC)
- New SSTA roles for HR/CMS



New Security Officers

- We're always here to help!
- Contact us for an orientation with the Security Team
- CTR Helpdesk 617-973-2468
- Comptroller Security Mailbox
 - SecurityRequest@State.MA.US



Follow us
on Twitter

@MA_Comptroller



DHSA

Department Head Signature Authorization



DHSA

Department Head Signature Authorization

- Department Head remains responsible for all activities conducted by the Department
 - Can delegate signature authority
- Authorized Signatories flagged in MMARS
- Departments can define additional signatory limits



DHSA

- All Authorized Signatories of a Department Head must be assigned a MMARS UAID with a DHSA flag even if they will never access MMARS
- Audits of DHSA rely on reports from MMARS identifying who are authorized signatories



DHSA

- Individuals granted DHSA may not sub-delegate Department Head Signatory Authority to others
- Department Head Signature Authorization may NOT be delegated to:
 - Contract employees
 - Non Employees
 - Employee of another Department since these individuals may NOT act as agents of the Department Head



Electronic signature and Department Head Authorization of MMARS Transactions

- Administrator Security with DHSA
 - no wet signature required for the MMARS transaction
- Administrator Security without DHSA
 - Wet signature from an authorized signatory approving the transaction PRIOR to submitting the transaction to final



DHSA Flags

▼Authorized Signatory - Departments

Accounts Payable :	<input checked="" type="checkbox"/>	Encumbrances :	<input checked="" type="checkbox"/>	LCM Rules :	<input type="checkbox"/>
Accounts Receivable :	<input type="checkbox"/>	Fiscal Administrator - All Functions :	<input type="checkbox"/>	Payroll :	<input type="checkbox"/>
Authorized Chargeback :	<input type="checkbox"/>	Fixed Assets :	<input type="checkbox"/>	Trust :	<input type="checkbox"/>
Batch Interface Events :	<input type="checkbox"/>	LCM Adjustments :	<input type="checkbox"/>	Vendor/Customer :	<input type="checkbox"/>
Budget :	<input type="checkbox"/>	LCM Administrator - All Functions :	<input type="checkbox"/>	None :	<input type="checkbox"/>
Credit Cards :	<input type="checkbox"/>	LCM Labor Default/Exceptions :	<input type="checkbox"/>	Other :	<input type="text"/>



Identifying DHSA in Reports

		DAPU	Accounts Payable User
		DPROU	Procurement User
		DSCSW	Statewide Scan
		DVCU	Vendor/Customer User
		REFOSDMA	SCAN ACCESS ONLY-OSD CREATED MA's
		DSCAN	Department Scan
		LALLF	LCM-All Functions Administrator
		PRRVSUB	PRRV Document Processing-Submit Allowed
		DSCAN	Department Scan
		LADJU	LCM-Adjustments User
		LALLF	LCM-All Functions Administrator
		PRRVVAL	PRRV Document Processing-No Submit Allowed
		DARA	Accounts Receivable Administrator
		DSCAN	Department Scan
		DVCA	Vendor Customer Administrator
			Authorized Signature: Accounts Receivable
		DFAU	Fixed Asset User
		DSCAN	Department Scan
		DSCAN	Department Scan
		DARA	Accounts Receivable Administrator
		DSCAN	Department Scan



UAID:

Password:

DEPARTMENT HEAD SIGNATURE AUTHORIZATION
ELECTRONIC SIGNATURE IN MMARS
RESPONSIBILITIES OF DEPARTMENT STAFF

MMARS LOG IN ADMINISTRATOR CERTIFICATION

By entering your UAID and password you acknowledge that you are responsible for entries made under your UAID. If you submit a document for final processing, you agree that you are certifying under the pains and penalties of perjury that it is your intention to attach an electronic signature approval and date to the MMARS document and that either:

- you have been delegated signature authorization by your Department Head to approve the document and supporting documentation as part of Internal Controls OR
- the document you are processing and any supporting documentation have received prior written approval by an authorized signatory of the Department Head, Secretariat and other required entities, and that a copy of these written approvals is available at the Department referencing the MMARS document number.

Approval of the MMARS document and any underlying supporting documentation shall operate as the Department Head's certification that these documents are accurate and complete and that the expenditure or other obligation is supported by sufficient legislatively authorized funds and is made in accordance with the Department's legislative mandates and funding authority, and complies with all applicable laws, regulations, policies and procedures.



**DEPARTMENT HEAD SIGNATURE AUTHORIZATION
ELECTRONIC SIGNATURE IN MMARS
RESPONSIBILITIES OF DEPARTMENT STAFF**

MMARS LOG IN ADMINISTRATOR CERTIFICATION

By entering your UAID and password you acknowledge that you are responsible for entries made under your UAID. If you submit a document for final processing, you agree that you are certifying under the pains and penalties of perjury that it is your intention to attach an electronic signature approval and date to the MMARS document and that either: you have been delegated signature authorization by your Department Head to approve the document and supporting documentation as part of Internal Controls

OR

the document you are processing and any supporting documentation have received prior written approval by an authorized signatory of the Department Head, Secretariat and other required entities, and that a copy of these written approvals is available at the Department referencing the MMARS document number.

Approval of the MMARS document and any underlying supporting documentation shall operate as the Department Head's certification that these documents are accurate and complete and that the expenditure or other obligation is supported by sufficient legislatively authorized funds and is made in accordance with the Department's legislative mandates and funding authority; and complies with all applicable laws, regulations, policies and procedures.



QUESTIONS?

Scott.Olsen@state.ma.us

617-973-2360



DAN FRISOLI

Security Administrator
Department Assistance Bureau
Office of the Comptroller



MMARS SECURITY REQUESTS AND MMARS PASSWORD RESETS

UDOC / UDOCPR



What is UDOC

- Online MMARS Transaction for use by Security Officers
- Add/Update/Delete MMARS Security Roles, Signature Authority and Directory information for MMARS Users
- Make all changes for a given user at a given time with one UDOC
- UDOCs are submitted into a pending state by the DSO and are then reviewed by the CTR Security Unit



Where is UDOC?

- UDOC is located in the MMARS Financial application
- UDOC transactions will appear in the same Document Catalog as other financial transactions such as CTs and PRCs



Why UDOC?

- Saves paper
- Historical Official record
- Quick turn-around



Security Request Form



COMMONWEALTH OF MASSACHUSETTS
MMARS Security Request Form
For Departmental Internal Use Only

Security Request Type
<input type="checkbox"/> New
<input type="checkbox"/> Change
<input type="checkbox"/> Delete (User)

Department Code: _____ UAID: _____
 Last Name: _____ First Name: _____
 Employee ID: _____ Telephone: _____ Ext: _____
 Locality: _____ E-Mail: _____

Previous UAID: _____ (Please supply this UAID if the user has transferred from another Department)

AUTHORIZED SIGNATORY DESIGNATIONS

- | Add | Del | | Add | Del | |
|--------------------------|--------------------------|---------------------|--------------------------|--------------------------|------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | ACCOUNTS PAYABLE | <input type="checkbox"/> | <input type="checkbox"/> | AUTHORIZED CHARGEBACK |
| <input type="checkbox"/> | <input type="checkbox"/> | ACCOUNTS RECEIVABLE | <input type="checkbox"/> | <input type="checkbox"/> | FISCAL - ALL FUNCTIONS |
| <input type="checkbox"/> | <input type="checkbox"/> | BUDGET | <input type="checkbox"/> | <input type="checkbox"/> | CREDIT CARDS |
| <input type="checkbox"/> | <input type="checkbox"/> | FIXED ASSETS | <input type="checkbox"/> | <input type="checkbox"/> | INTERFACE |
| <input type="checkbox"/> | <input type="checkbox"/> | PROCUREMENT | <input type="checkbox"/> | <input type="checkbox"/> | LCM ADJUSTMENTS |
| <input type="checkbox"/> | <input type="checkbox"/> | TRUST | <input type="checkbox"/> | <input type="checkbox"/> | LCM LABOR DEFAULT/EXCEPTIONS |
| <input type="checkbox"/> | <input type="checkbox"/> | VENDOR/CUSTOMER | <input type="checkbox"/> | <input type="checkbox"/> | LCM RULES |
| <input type="checkbox"/> | <input type="checkbox"/> | PAYROLL | <input type="checkbox"/> | <input type="checkbox"/> | LCM - ALL FUNCTIONS |

MMARS SECURITY ROLES

- | Add | Del | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | ALL SCAN DEPARTMENT (DSCAH) |
| <input type="checkbox"/> | <input type="checkbox"/> | ALL SCAN STATEWIDE (DSCSW) |
| <input type="checkbox"/> | <input type="checkbox"/> | ACCOUNTS PAYABLE USER (DAPU) |
| <input type="checkbox"/> | <input type="checkbox"/> | ACCOUNTS PAYABLE ADMINISTRATOR (DAPA) |
| <input type="checkbox"/> | <input type="checkbox"/> | ACCOUNTS RECEIVABLE USER (DARU) |
| <input type="checkbox"/> | <input type="checkbox"/> | ACCOUNTS RECEIVABLE ADMINISTRATOR (DARA) |
| <input type="checkbox"/> | <input type="checkbox"/> | BUDGET USER (DBGU) |
| <input type="checkbox"/> | <input type="checkbox"/> | BUDGET ADMINISTRATOR (DBGA) |
| <input type="checkbox"/> | <input type="checkbox"/> | FIXED ASSETS USER (DFAU) |
| <input type="checkbox"/> | <input type="checkbox"/> | FIXED ASSETS ADMINISTRATOR (DFAA) |
| <input type="checkbox"/> | <input type="checkbox"/> | PROCUREMENT USER (DPROU) |
| <input type="checkbox"/> | <input type="checkbox"/> | PROCUREMENT ADMINISTRATOR (DPROA) |
| <input type="checkbox"/> | <input type="checkbox"/> | TRUST USER (DTRSU) |
| <input type="checkbox"/> | <input type="checkbox"/> | TRUST ADMINISTRATOR (DTRSA) |
| <input type="checkbox"/> | <input type="checkbox"/> | VENDOR/CUSTOMER USER (DVCU) |
| <input type="checkbox"/> | <input type="checkbox"/> | VENDOR/CUSTOMER ADMINISTRATOR (DVCA) |
| <input type="checkbox"/> | <input type="checkbox"/> | AUTHORIZED CHARGEBACK ADMIN (DACA) |
| <input type="checkbox"/> | <input type="checkbox"/> | FISCAL ADMINISTRATOR - ALL FUNCTIONS (DFISC) |
| <input type="checkbox"/> | <input type="checkbox"/> | SECURITY OFFICER (DSO) |

MMARS LCM-SPECIFIC

- | Add | Del | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | SCAN ALL (Includes Labor History) (LSCII) |
| <input type="checkbox"/> | <input type="checkbox"/> | SCAN LIMITED (Does not include Labor History) (LSCIL) |
| <input type="checkbox"/> | <input type="checkbox"/> | ADJUSTMENTS USER (LADJU) |
| <input type="checkbox"/> | <input type="checkbox"/> | ADJUSTMENTS ADMINISTRATOR (LADJA) |
| <input type="checkbox"/> | <input type="checkbox"/> | LABOR DEFAULT/EXCEPTIONS USER (LLDEU) |
| <input type="checkbox"/> | <input type="checkbox"/> | LABOR DEFAULT/EXCEPTIONS ADMIN (LLDEA) |
| <input type="checkbox"/> | <input type="checkbox"/> | RULES USER (LRULU) |
| <input type="checkbox"/> | <input type="checkbox"/> | RULES ADMINISTRATOR (LRULA) |
| <input type="checkbox"/> | <input type="checkbox"/> | LCM ADMINISTRATOR - ALL FUNCTIONS (LALLF) |

MMARS INTERFACE ROLE (For Interface Dept. Only)

- | Add | Del | |
|--------------------------|--------------------------|-----------|
| <input type="checkbox"/> | <input type="checkbox"/> | INTERFACE |

Comments / Requests:

I certify that the Department Head has personally approved any requests for Administrator roles and Department Head Signature Authorization designations. This approval is maintained as part of Department Internal Controls.

For Departmental Internal Use Only. Do Not Submit to CTR Security Unit. All Security Requests Must be Processed Via the MMARS UDOC Transaction.



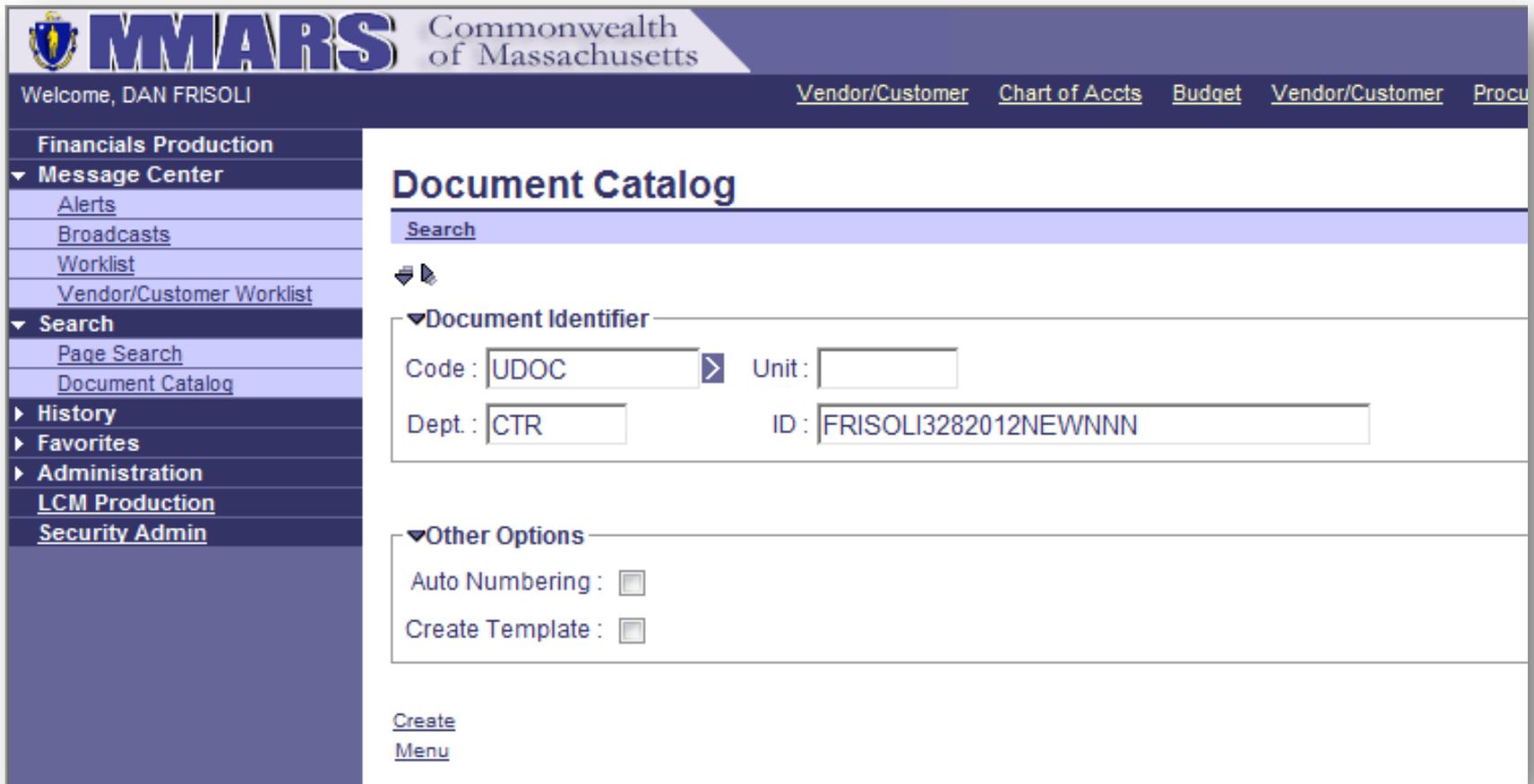
Three Different uses for UDOC

- **Create a New User**
 - Add security roles
 - Add DHSA
 - Add Directory information. Name, Email Phone
- **Update an Existing User**
 - Add and/or remove security roles
 - Add and/or remove DHSA
- **Deactivate an Existing User**
 - User is locked out and flagged as INACTIVE
 - All security roles must have DELETE radio button checked
 - Remove Signature Authority



UDOC --Document Catalog

Perform from Financial Document Catalog, not Security Admin



The screenshot shows the MMARS (Massachusetts Management and Reporting System) interface. The header includes the MMARS logo and the text "Commonwealth of Massachusetts". Below the header, a navigation bar contains links for "Vendor/Customer", "Chart of Accts", "Budget", "Vendor/Customer", and "Procurement". The main content area is titled "Document Catalog" and features a search form. The search form includes a "Document Identifier" section with fields for "Code" (set to "UDOC"), "Unit", "Dept." (set to "CTR"), and "ID" (set to "FRISOLI3282012NEWNNN"). There is also an "Other Options" section with checkboxes for "Auto Numbering" and "Create Template". A "Create" button and a "Menu" link are located at the bottom of the search form.

MMARS Commonwealth of Massachusetts

Welcome, DAN FRISOLI

[Vendor/Customer](#) [Chart of Accts](#) [Budget](#) [Vendor/Customer](#) [Procurement](#)

Document Catalog

[Search](#)

Document Identifier

Code : Unit :

Dept. : ID :

Other Options

Auto Numbering :

Create Template :

[Create](#)

[Menu](#)



UDOC – User ID, Directory Info and Home Organization

- Obtain UAID from InTempo first
- All User IDs must be entered in lower case
- Enter 3 Letter Department Code Only

Welcome, DAN FRISOLI [Vendor/Customer](#) [Chart of Accts](#) [Budget](#) [Vendor/Customer](#) [Procurement](#) [Accts Payable](#) [Accts Receivable](#)

UDOC CTR FRISOLI3282012NEWNNN

Document View

- ✓ Header
- Directory Information
- Home Organization
- Account Options
- Password Maintenance
- Applications
- Authorized Signatory - Depart
- Authorized Signatory - CTR
- Security Roles
- Workflow Roles
- Workgroups
- Document Comments
- Document Attachments
- Document History
- Document Reference
- Future Triggering
- Forms

UDOC - CTR- FRISOLI3282012NEWNNN- 1- New- Draft Action Menu

*Action : Add Update

*User ID : Populate From Existing User

▼Directory Information

Last Name : Locality : Phone Number :

First Name : Room Number : Ext. :

Email Address : Fax Number :

▼Home Organization

Government Branch : Division : District :

Cabinet : Group : Bureau :

Department : Section : Unit :



UDOC – Account Options, Password Maintenance and Applications

- If Deactivating User - Check "Locked Out" and "Inactive Boxes"
- New User - Password alpha-numeric exactly 8
- Applications – Defaults Financial and HR (LCM)
- Administrator & Password Reset for DSOs/helpdesk

Welcome, DAN FRISOLI [Vendor/Customer](#) [Chart of Accts](#) [Budget](#) [Vendor/Customer](#) [Procurement](#) [Accts Payable](#) [Accts Receivable](#)

UDOC CTR FRISOLI3282012NEWNN

Document View

- ✓ Header
 - Directory Information
 - Home Organization
 - Account Options
 - Password Maintenance
 - Applications
 - Authorized Signatory - Depar
 - Authorized Signatory - CTR
- Security Roles
- Workflow Roles
- Workgroups

Document Comments

Document Attachments

Document History

Document Reference

Future Triggering

Forms

▼Account Options

Override Errors :

*Bad Logins Count :

Locked out : Standard Reporting User :

Inactive : Power Reporting User :

Logging : Primary Reporting Group :

Use Default Home Page Window :

▼Password Maintenance

Reset Password : Password :

▼Applications

ADVANTAGE Financial : VSS Password Reset : PASSWORD RESET :

ADVANTAGE HR : ADVANTAGE Administrator :

ADVANTAGE VSS : ADVANTAGE ESS :

UDOC – Authorized Signatory - Departments

- New User - Select “None” or at least one of the other selections.
- Deactivating User - Uncheck all and check “None”
- If modifying DHSA add Document Comment

▼Authorized Signatory - Departments

Accounts Payable : <input type="checkbox"/>	Encumbrances : <input type="checkbox"/>	LCM Rules : <input type="checkbox"/>
Accounts Receivable : <input type="checkbox"/>	Fiscal Administrator - All Functions : <input type="checkbox"/>	Payroll : <input type="checkbox"/>
Authorized Chargeback : <input type="checkbox"/>	Fixed Assets : <input type="checkbox"/>	Trust : <input type="checkbox"/>
Batch Interface Events : <input type="checkbox"/>	LCM Adjustments : <input type="checkbox"/>	Vendor/Customer : <input type="checkbox"/>
Budget : <input type="checkbox"/>	LCM Administrator - All Functions : <input type="checkbox"/>	None : <input checked="" type="checkbox"/>
Credit Cards : <input type="checkbox"/>	LCM Labor Default/Exceptions : <input type="checkbox"/>	Other : <input type="text"/>



UDOC – Authorized Signatory - Departments

- A Department Head delegates signature authority personally to Department employees who will be responsible for conducting business on behalf of the Department Head in accordance with applicable law, regulations, policies and procedures.

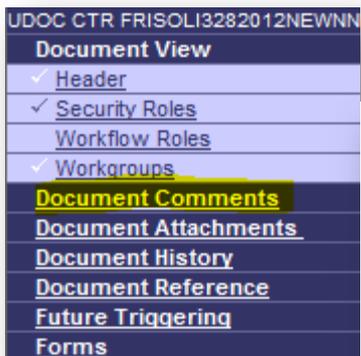
▼Authorized Signatory - Departments

Accounts Payable : <input checked="" type="checkbox"/>	Encumbrances : <input checked="" type="checkbox"/>	LCM Rules : <input type="checkbox"/>
Accounts Receivable : <input type="checkbox"/>	Fiscal Administrator - All Functions : <input type="checkbox"/>	Payroll : <input type="checkbox"/>
Authorized Chargeback : <input type="checkbox"/>	Fixed Assets : <input checked="" type="checkbox"/>	Trust : <input type="checkbox"/>
Batch Interface Events : <input type="checkbox"/>	LCM Adjustments : <input type="checkbox"/>	Vendor/Customer : <input type="checkbox"/>
Budget : <input type="checkbox"/>	LCM Administrator - All Functions : <input type="checkbox"/>	None : <input type="checkbox"/>
Credit Cards : <input type="checkbox"/>	LCM Labor Default/Exceptions : <input type="checkbox"/>	Other : <input type="text" value="PAYMENTS UNDER 100K"/>



UDOC – Document Comments

- Add Document Comments to describe detailed changes
- Add Comments at any stage, draft, pending, or final
- CTR Security will add Document Comments when rejecting UDOC



Document Comments

UDOC - CTR- FRISOLI3282012NEWNNI

Version	Date/Time	User	Phase	Subject
✓ 1	3/29/2012 11:46:27 AM	ctraut	Draft	

First Prev Next Last

[Save](#) [Undo](#) [Insert](#) [Copy](#) [Paste](#) [Search](#)

Document Code : UDOC

Document Dept. Code : CTR

Document ID : FRISOLI3282012NEWNNI

Version : 1

User : ctraut

Phase : Draft

*Subject : Name

*Comment :
Changed last name and removed
Encumbrances Signature Authority.

Document Comments

UDOC - CTR- FRISOLI3282012NEWNNI

Version	Date/Time	User	Phase	Subject
✓ 1	3/29/2012 11:46:27 AM	ctraut	Draft	

First Prev Next Last

[Save](#) [Undo](#) [Insert](#) [Copy](#) [Paste](#) [Search](#)

Document Code : UDOC

Document Dept. Code : CTR

Document ID : FRISOLI3282012NEWNNI

Version : 1

User : ctraut

Phase : Draft

*Subject : Rejected

*Comment :
Please add workgroup 27 and enter
at least 1 security role.



UDOC – Security roles

- If adding a role always insert a new line. Never type over an existing role
- If deleting role use the Delete radio button. Never use the Scissors to delete a role

UDOC - CTR- FRISOLI3282012NEWNNN- 1- New- Draft

User ID : ctr123 Last Name : Frisoli First Name : Daniel

	Security Role ID	Description	Precedence
<input type="checkbox"/> 	DSCAN	Department Scan	1
<input checked="" type="checkbox"/> 	DAPU	Accounts Payable User	2

[Insert New Line](#) [Insert Copied Line](#)

*Action : Add
 Update
 Delete

*Security Role ID :

Description : Accounts Payable User

*Precedence :

UDOC - CTR- FRISOLI3282012NEWNNN- 1- New- Draft

User ID : ctr123 Last Name : Frisoli First Name : Daniel

	Security Role ID	Description	Precedence
<input type="checkbox"/> 	DSCAN	Department Scan	1
<input checked="" type="checkbox"/> 	DAPU	Accounts Payable User	2

[Insert New Line](#) [Insert Copied Line](#)

*Action : Add
 Update
 Delete

*Security Role ID :

Description : Accounts Payable User

*Precedence :



UDOC – Security roles

- Security Roles with Descriptions can be found in the Security Guide to Statewide Enterprise Systems (page 86) in the Security Officer drop box in PartnerNet.

CTR_SecurityGuide.pdf - Adobe Reader

File Edit View Window Help

90 / 223 100%

Tools Comment

Bookmarks

- Cover
- Using the Guide
- Table of Contents
- Enterprise Systems
- InTempo
- Enterprise Passwords
- MMARS
- HR/CMS
- CIW
- DocDirect
- PayInfo
- PartnerNet
- FAQ

Security Guide Page 86 of 218

MMARS Security Roles and Documents Processed

MMARS Security Role Security Role Description

DACA **Authorized Chargeback Administrator**

Staff with this Security Role are 'Sellers' who prepare Intergovernmental Encumbrances and Vouchers.

Documents Processed with DACA

IE	Internal Encumbrance
IET	Internal Exchange Transaction
ITI	Internal Transaction Initiator

DAPA **Accounts Payable Administrator**

Staff with this Security Role have access to all Accounts Payable Documents such as the Accounting Template, Automated Disbursement Document, Electronic Funds Transfer Document, and General Accounting Expenditure Document.



ALL UDOCS will go to workflow

- UDOC will workflow to be reviewed by CTR Security Unit
- CTR will review and either approve or reject UDOCs within one day of submission
- If a UDOC is determined to be incorrect it will be rejected, a comment will be added to the UDOC with instructions on how to correct
- Monitor Doc Catalog for Approved/Rejected UDOCs
- DSOs will not receive an email
- CTR will not contact users directly



UDOC – Search

- Use the Doc Catalog to find rejected UDOCs

Document Catalog

[Create](#)

☰

▼ Document Identifier

Code : Unit :

Dept : ID :

▼ User Information

Create User ID : Create Date :

▼ Document State

Function : Status :

Phase :

[Browse](#) [Clear](#)

[Action Menu](#)

[Open](#) [Validate](#) [Submit](#) [Copy](#)

	Code	Dept.	Unit	ID	Comments	Version	Function	Phase	Status	Date	User ID	Amount	Active
<input type="checkbox"/>	UDOC	CTR		<u>FRISOL3282012NEWNNN</u>	Yes	1	New	Draft	Rejected	3/28/12	ctrout	0.00	true

First Prev Next Last

[Menu](#)



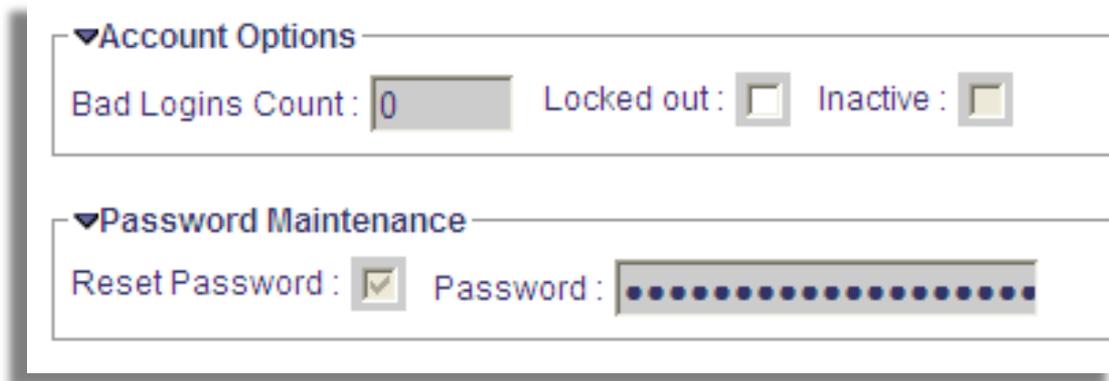
Emergency Deactivations

- **Contact CTR in emergency deactivation situations**
- Dan Frisoli 617-973-2614
- Lenny Montone 617-973-2570
- Scott Olsen 617-973-2360
- Help Desk 617-973-2468



UDOCPR – MMARS Password Resets

- Do NOT use UDOC for password resets, use UDOCPR
- Does not workflow
- Communicate with your user
- 8 characters, alpha - numeric



▼Account Options

Bad Logins Count: Locked out: Inactive:

▼Password Maintenance

Reset Password: Password:



Who has access to UDOCPR?

- All Security Officers have access to UDOCPR
- A separate role called “HELP_DESK” can be assigned to Help Desk Representatives. This role provides access to UDOCPR but NOT UDOC





Dan Frisoli - 617-973-2614

Lenny Montone - 617-973-2570

SecurityRequest@massmail.state.ma.us

Security Guide in [PartnerNet](#)



Webcasts for UDOCs



QUESTIONS?



MMARS SECURITY DATA IN THE COMMONWEALTH INFORMATION WAREHOUSE (CIW)



What is the Commonwealth Information Warehouse

- CIW is a central repository for enterprise data that is maintained in separate source applications.
- Accessed via Microsoft Access or Excel.
- Customize Queries to fit business needs.



CIW

MMARS Security Views

- Department Heads, CFOs and DSOs are allowed access to Security Views
- View security for users in your department
- View Signature authority for users in your department
- Tool to ensure segregation of duties



4 Security Views currently available in the CIW

1. Current MMARS user profiles
DBO_M_Security_MMARS_SCUSER
2. UDOC and UDOCPR
DBO_M_Security_MMARS_UDOC
3. User Activity Details
DBO_M_USER_ACTIVITY_DETAILS
4. User Activity Report
DBO_M_USER_ACTIVITY_REPORT



CIW Security Role

Request the NM_SECURITY_DEP role via InTempo. Type directly into the comments section of the Warehouse tab.

"NM_SECURITY_MD" for multiple departments.

User Information ViewDirect HR/CMS **Warehouse**

Information Warehouse Governmental Access

	Classic MMARS	Human Resource Standard	Human Resource Additional	Compensation Management Standard	Compensation Management Additional	MMARS	LCM	CAPS	PMIS
A. Departmental	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
B. Multiple Departments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
C. Secretariat (Cabinet)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
D. Branch of Government	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E. State Wide	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
F. Delete User DB Access	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
G. Default	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Select for LCM Statewide FULL

MMARS Code:

Specify Secretariat:

Specify Branch:

CIW Pin:

List Multiple Departments:

Selected Departments:

Specify Other:

Comments:



Starter Queries

- Queries based on commonly asked questions
- Designed for ease of use and customization
- Database with starter queries in PartnerNet
- DSOs and CFOs already have access to database in PartnerNet



Current MMARS User Profile View

- Profiles in the CIW are as of close of previous business day
- UAIDs, Names, Dept Codes, Location Codes
- Phone numbers and emails
- Security Roles & Workflow Roles
- Department Head Signature Authorization (DHSA)



Starter Queries Available

- All Active Users w/ Security Roles
- All Active Users by Locality
- Roles by UAID
- Roles by Name
- DHSA by UAID
- Accounts Payable Signature Authority
- Users who can Submit Payments
- OTHERS



All Active Users w/ Security Roles

user_id	first_name	last_name	security_role_id
ctr123	DANIEL	FRISOLI	SECURITY_OFFICER
ctr123	DANIEL	FRISOLI	DSCAN
ctr123	DANIEL	FRISOLI	LSCN
ctr345	SCOTT	OLSEN	DSCAN
ctr345	SCOTT	OLSEN	SECURITY_OFFICER
ctr678	LENNY	MONTONE	LALLF
ctr678	LENNY	MONTONE	LSCN
ctr678	LENNY	MONTONE	DSCAN
ctr678	LENNY	MONTONE	DAPA



CIW

MMARS User Activity Views

- Department Heads, CFOs and DSOs are allowed access to User Activity Views
- Used to track user activity in MMARS
- Used to determine appropriate security access.
- Reduce the use of powerful roles such as DFISC
- Tool to ensure segregation of duties



Webcasts for MMARS User Security in the CIW



QUESTIONS?



DFISC

Fiscal Administrator All Functions



DFISC

- DFISC is a very powerful security role in MMARS
- Allows the assignee to submit most MMARS Financial transactions and to edit department related MMARS pages.



DFISC - Document Access

- AR Advance Refund
- BGCN Central Expense
- BGCP Capital Spending Expense
- BGCS Central Subsidiary Expense
- BGDN Departmental Expense
- BGDR Departmental Revenue
- BGDS Departmental Subsidiary Expense
- BGPR Program Budget
- BGRE Phase-Specific Reimbursable
- BGRG Grant Reimbursable



DFISC - Document Access Continued

- BGTS Central Subsidiary Expense - Non CTR
- CEC Commodity Encumbrance Correction
- CL Referral to Collection Agency
- CR Cash Receipt
- CT Contract
- EA Expenditure for Advance
- EAV Encumbrance for Advance
- ER Expenditure Refund
- EX Expenditure Correction



DFISC - Document Access Continued

- FA Fixed Asset Acquisition
- FC Fixed Asset Cancellation
- FD Fixed Asset Disposition
- FE Fixed Asset Depreciation Expense
- FI Fixed Asset Increase/Decrease
- FM Fixed Asset Modification
- FP Fixed Asset Selling Price Change
- FT Fixed Asset Transfer
- FX Fixed Asset Type Change
- GAE General Accounting Encumbrance



DFISC - Document Access Continued

- GAEC General Accounting Encumbrance Correction
- GAP General Accounting Pre Encumbrance
- GAX General Accounting Expense/Expenditure
- GX9 Summary Payment Voucher
- GXR Retainage Release
- IN Invoice
- INP Incidental Payment
- MA Master Agreement
- ME Fixed Asset Mass Depreciation Expense



DFISC - Document Access

- MA Master Agreement
- ME Fixed Asset Mass Depreciation Expense
- PC Commodity Purchase Order
- PH Payroll Hold
- PRC Commodity Based PR
- PRM Matching PR - Normal
- RA Request for Advance
- RE Receivable
- RF1 Revenue Refund Payment
- RIN Recurring Invoice



DFISC - Document Access Continued

- RPO Recurring Payment Order
- RQS Standard Requisition
- RT Receipt of Trust
- TV Trust Voucher
- VCC Vendor/Customer Creation



DFISC – Page Access

- ACTPL- Accounting Template
- CNTAC - CONTACT
- DOBJ - Department Object
- SIG - Scheduled Invoice Generation
- DISRQ - Disbursement Request
- CACT - Customer Account options
- FDT - Future Document Triggering
- PSCHD - Payment Plan
- TASK - Task



With DFISC
I have all
the power



Reduce DFISC

- Review Security Reports in Doc Direct
- Utilize MMARS User Activity views in CIW
- Talk to the DFISC user
- Call CTR DAB Security for assistance



QUESTIONS?



HR/CMS Security



Segregation of Duties (SoD)

- An internal control activity to help prevent or decrease the occurrence of undetected innocent errors or intentional fraud
- Ensure that no single individual has control over all phases of a transaction
- Eliminate the assignment of incompatible duties to an employee
- In situations where SoD cannot be followed then establish compensating internal controls



The Importance of SoD

- Decrease risk of fraud
- Deter dishonest employees
- Prevent undetected innocent errors



High Risk Combinations of Roles

- HR Job Part or Full
- Payroll A/U/D
- Time and Labor A/U/D



InTempo Requests

Requesting roles that conflict with established best practices



Self Service Time and Attendance



SS_TA_ADMIN

Functions of the Role

- Setup and Maintain SSTA Time Reporter Data (e.g., Time Reporter Type, Rule Element, Workgroup, Schedule)
- Enter and Adjust Restricted Time Reporting Codes (TRCs) (e.g., Leave with Pay, Buyback codes)
- Approve Payable Time via Manager Dashboard
- View SSTA online reports to resolve exceptions

Who Should Have the Role?

- HR/Payroll core users



SS_TA_Delegate

Functions of the Role

- Delegate time approval on behalf of a Manager/Supervisor if needed

Note: Managers/Supervisors should delegate time approval to another manager if they will be out of the office and unable to approver their employees' time. This security role is a back-up to enable someone to delegate time approval in the event that the Manager/Supervisor is away and unable to do the delegation themselves.

Who Should Have the Role?

- HR/Payroll core users
- Select Managers/Supervisor in a department that would have the information needed to delegate time approval on behalf of another Manager/Supervisor



MA_TL_PS_QUERY_VW

Functions of the Role

- This role allows access to online self service reports and allows users to access data that exceeds the limitation of 1,000 rows.

Who Should Have the Role?

- HR/Payroll core users / Fiscal Staff



SS_PWRD_EMAIL_RESET

*Non ESC Supported agencies only

Functions of the Role

- Re-set employee passwords for SSTA
- Re-set email address (email used to send employees alerts about their timesheets when necessary)

Note: SSTA will offer employees the opportunity to re-set their password through a forgotten password function. Employee may also update their email address. This security is intended as a failsafe in the event an employee has attempted several logins and been locked out of the system, or cannot get to a computer and needs support.

Who Should Have the Role?

- This role should be should be given to whoever is going to be supporting Self-Service users at non ESC supported agencies.



SS TA Labor Distribution

*For Labor Distribution agencies only

Functions of the Role

- Page allows update access to User Defined fields for LD agencies and view access to Combo Code Page

Who Should Have the Role?

- HR/Payroll core users / Fiscal Staff



SS TA Badge Update

*For TCD agencies only

Functions of the Role

- Role to allow users to update employee TCD Badge Information

Who Should Have the Role?

- HR/Payroll core users / Fiscal Staff



HR/CMS Webcast



Available Resources



Security Guide

Contents of Dropbox [Help](#) [My Home](#) [My Profile](#) [Logout](#)

[Search User](#) | [Filter](#) | [Upload Files](#)

[User Reports](#)

[Search File](#)

[Department](#)

[Application](#)

[Drop Box](#)

[Role](#)

[System Parameters](#)

[File Delete](#)

Filter Filenames

File Name (full or partial)

Last Updated Date From  To 

For Department

[Apply Filter](#)

Contents of Dropbox : Security Officer
(Click on underlined column headings to sort)

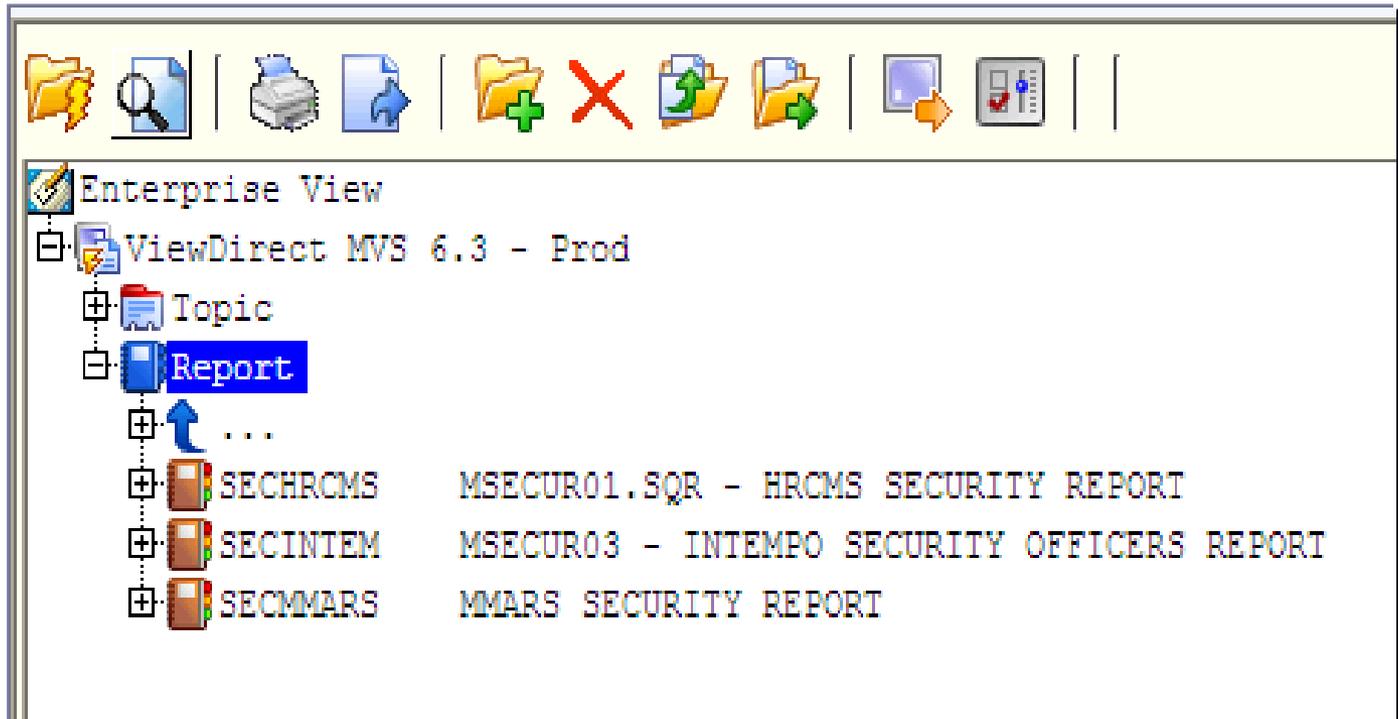
	<u>File Name</u>	<u>Size</u>	<u>Uploaded On</u>	<u>Uploaded By</u>	<u>By Department</u>
View	CTR_SecurityGuide.pdf	4108.3K	3/29/2011 12:10:24 PM	CTR	CTR - Office Of The Comptroller (CTR)

File(s) Found: **1** Files per page [Change](#)



Doc Direct Report

"SECHRCMS"



CTR Systems Security

- Dan Frisoli
 - Dan.frisoli@state.ma.us
- Lenny Montone
 - Lenny.montone@state.ma.us
- Security Inbox
 - securityrequest@state.ma.us



Questions?



ITD UPDATE

Kevin Burns, Commonwealth CISO





Identity and Access Management

OSC Annual Security Officers' Briefing

March 22, 2013

Rev. 2

Administration and Finance

Information Technology Division

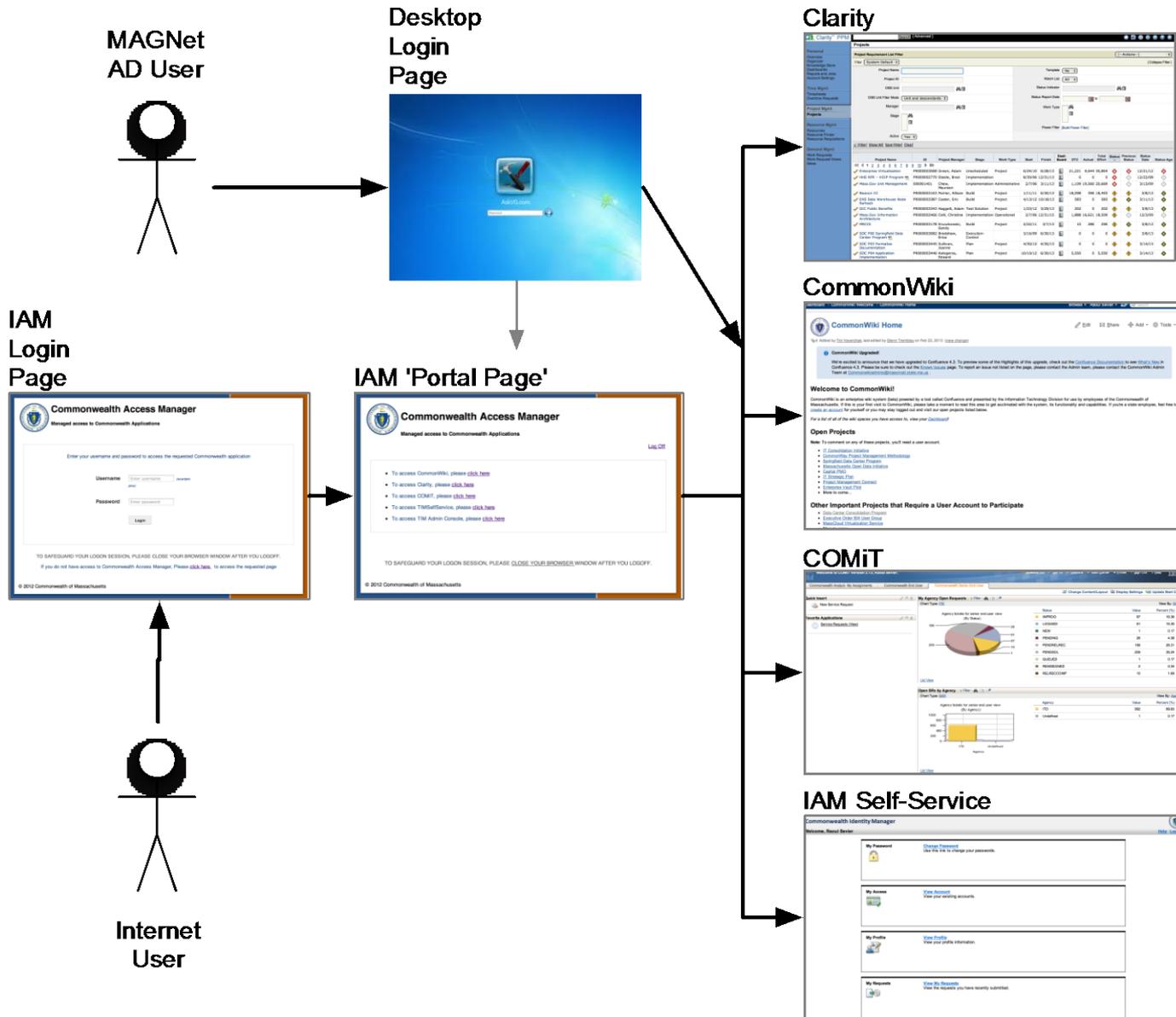


Agenda

- Main 'Use Cases'
- Deployment Roadmap
- Cost Model
- Program Outcomes

IAM - Identity & Access Management

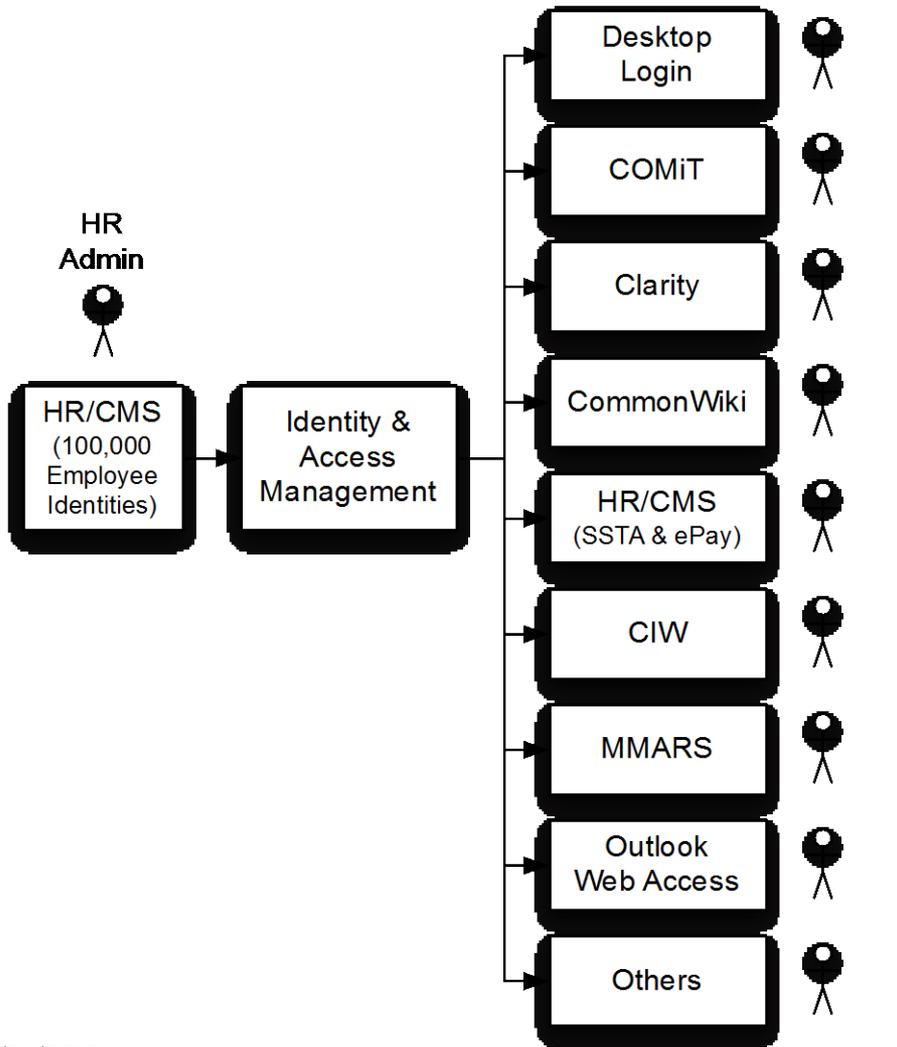
User's Experience



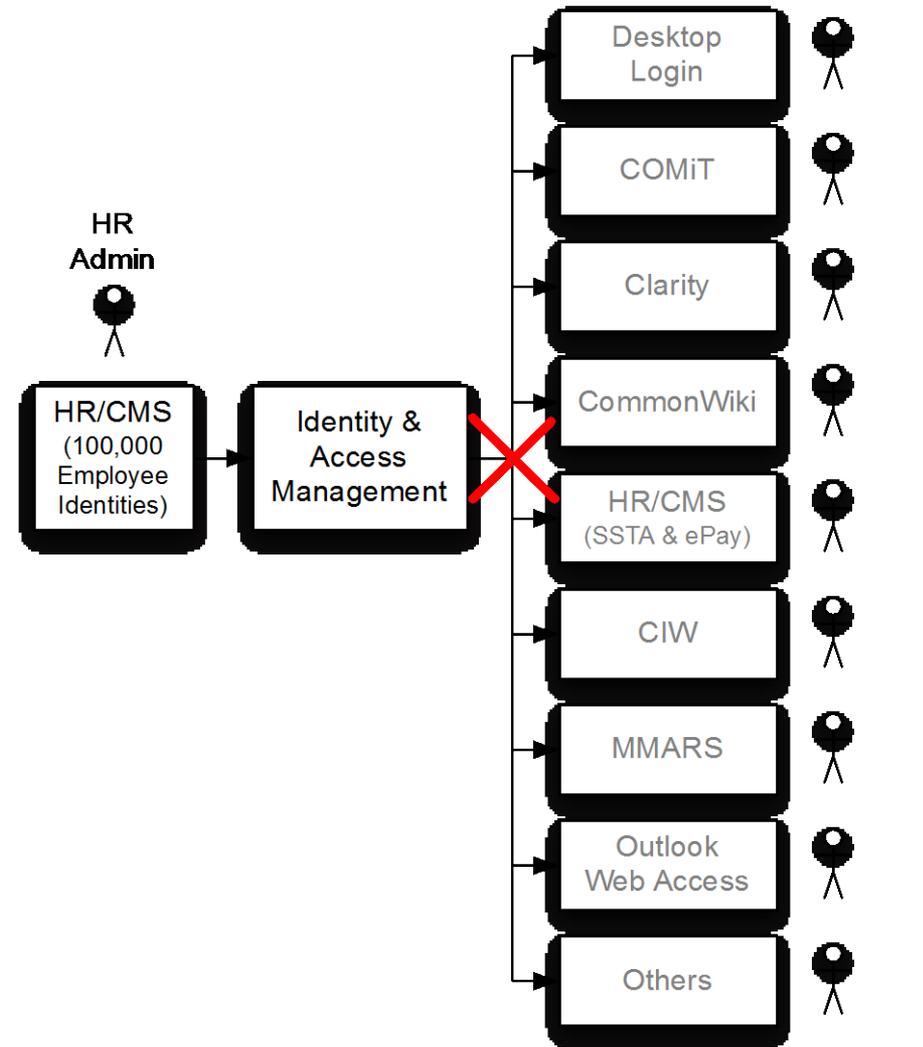
IAM - Identity & Access Management Administrator's Experience



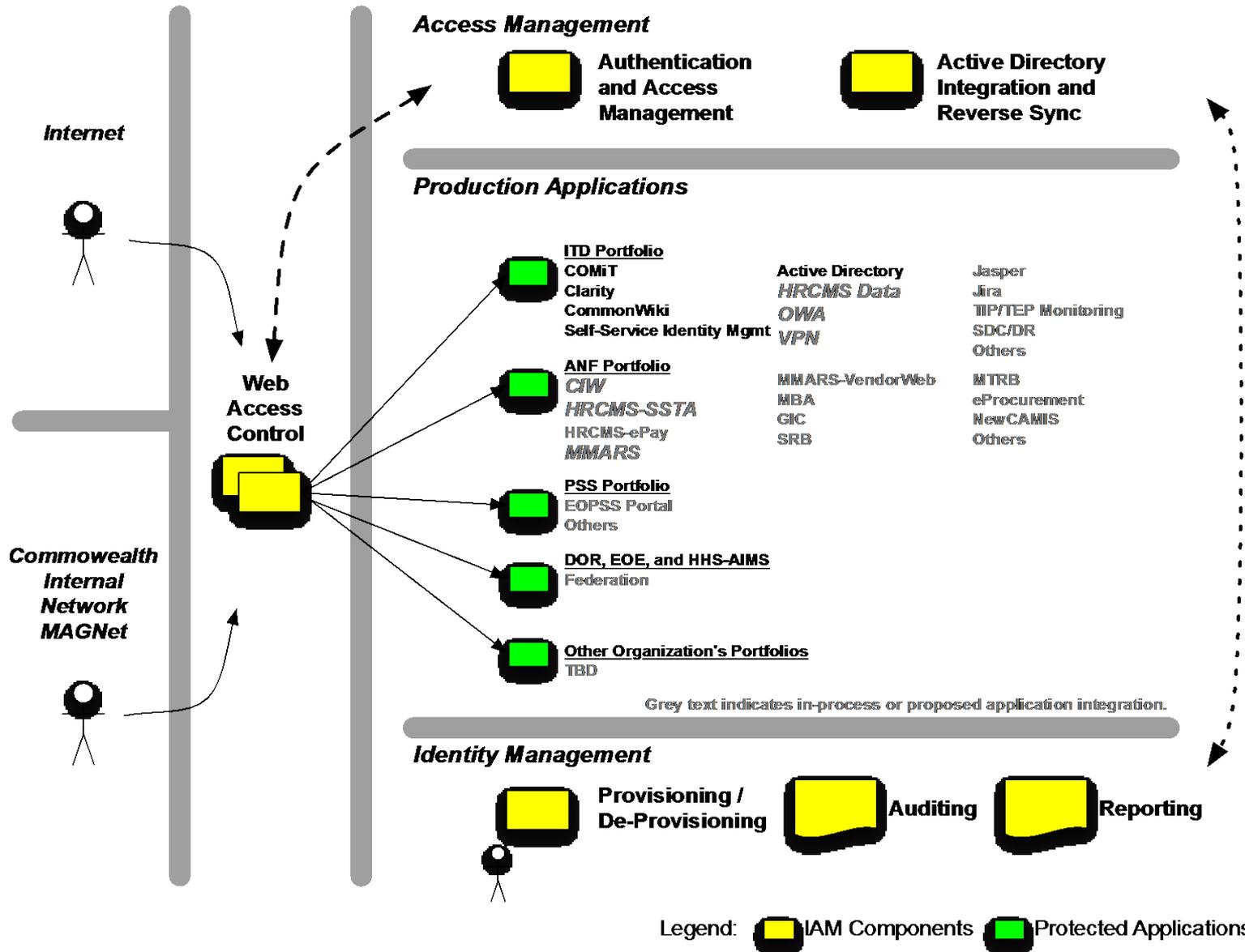
Provisioning



De-Provisioning



IAM Deployment Roadmap Vision





IAM Cost Model

- **Application Integration with Identity Management**
 - Initial costs covered by capital
 - Future integrations may be covered in-whole or in-part by capital, at least for some period of time

- **Operation of the Identity Management Solution**
 - Initial costs covered by capital
 - Transition to internal cost recovery viewed by FY15
 - Cost Drivers
 - ITD Infrastructure
 - Infrastructure Operations
 - Software Maintenance
 - Application Support FTEs and Contractors
 - Annual operating cost approximately \$1m
 - Amortization across 100,000 HRCMS employee identities yields a cost per employee of \$10/year, or \$0.90 per month
 - Additional cost recovery by application, or for partner and citizen use may be possible



IAM Program – Key Outcomes

Executing our program allows us to achieve key outcomes needed to provide business-centric IAM Services to key stake holders.

IAM As a Service

Establish a model for ITD to provide IAM services such as identity provisioning, access control, auditing, and compliance reporting to Commonwealth agencies.

Alignment to Industry Guidelines and Framework

Establish a trust based interoperable architecture that addresses IAM requirements for various laws, regulations, and standards and positions the commonwealth for future market trends.

Key Outcomes

Internal Consumers

Provide ease of use (e.g. single login to multiple applications, operations efficiency, compliance, and security).

External Consumers

Provide seamless access to various government services and provide a level of security based on risk and trust.

Additional Materials





Cybersecurity Challenges

The results of the 2012 Deloitte-NASCIO Cybersecurity survey highlight the pressing challenges facing State Chief Information Officers (CIOs), Chief Technology Officers (CTOs) and Chief Information Security Officers (CISOs) today.

- As states progress towards a future of internet-hosted applications using new technologies, like big data, mobile solutions, and cloud computing, and continue to grow their electronic repositories of valuable resident data, addressing the issue of protecting personally identifiable information (PII) and state systems is of utmost importance

Cybersecurity challenges continue in 2012 amidst escalating threats

92%

State officials feel cybersecurity is very important for the state

CISOs are very confident in protecting state's assets against external threats

Only 24%

50%

CISOs manage a team of one to five cybersecurity professionals only

CISOs feel that staff have the required cybersecurity competency

Only 32%

Only 14%

CISOs feel that they receive appropriate executive commitment and adequate funding for cybersecurity

CISOs indicate "Lack of sufficient funding" is the key barrier to address cybersecurity

86%

70%

CISOs have reported a breach

CISOs feel "phishing and pharming" as their top cybersecurity threat

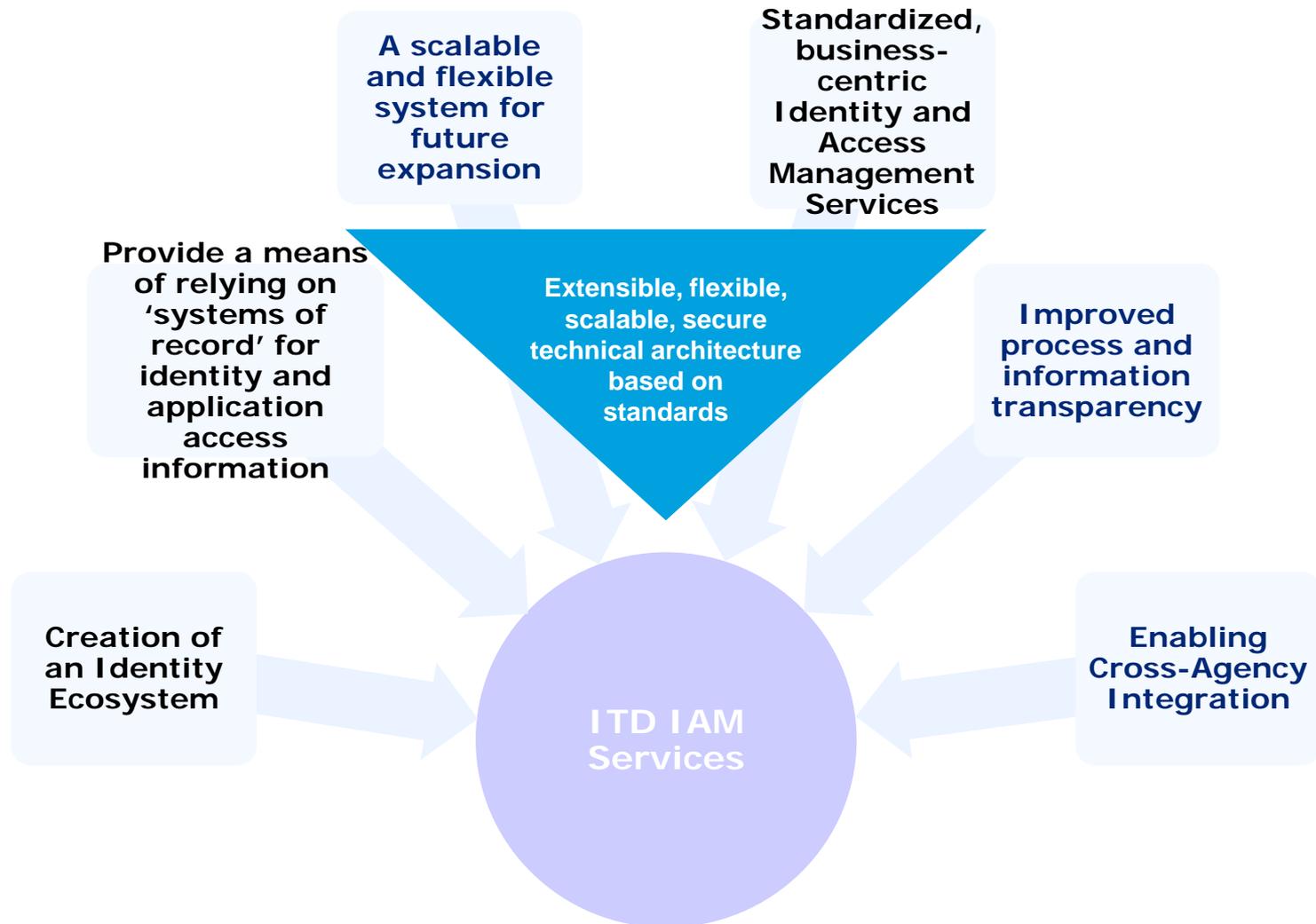
82%

IAM continues to be top of mind for executives and an integral part of the Cybersecurity program

ITD's Identity and Access Management Vision



ITD's vision is to provide enhanced security, improved access request process and reduced user administration through standardized, business-centric IAM Services.



ITD Pilot



IDMS Pilot provides a viable, scalable and extendible foundation aligned with industry frameworks and positioned to expand for entire Commonwealth.

Pilot Highlights

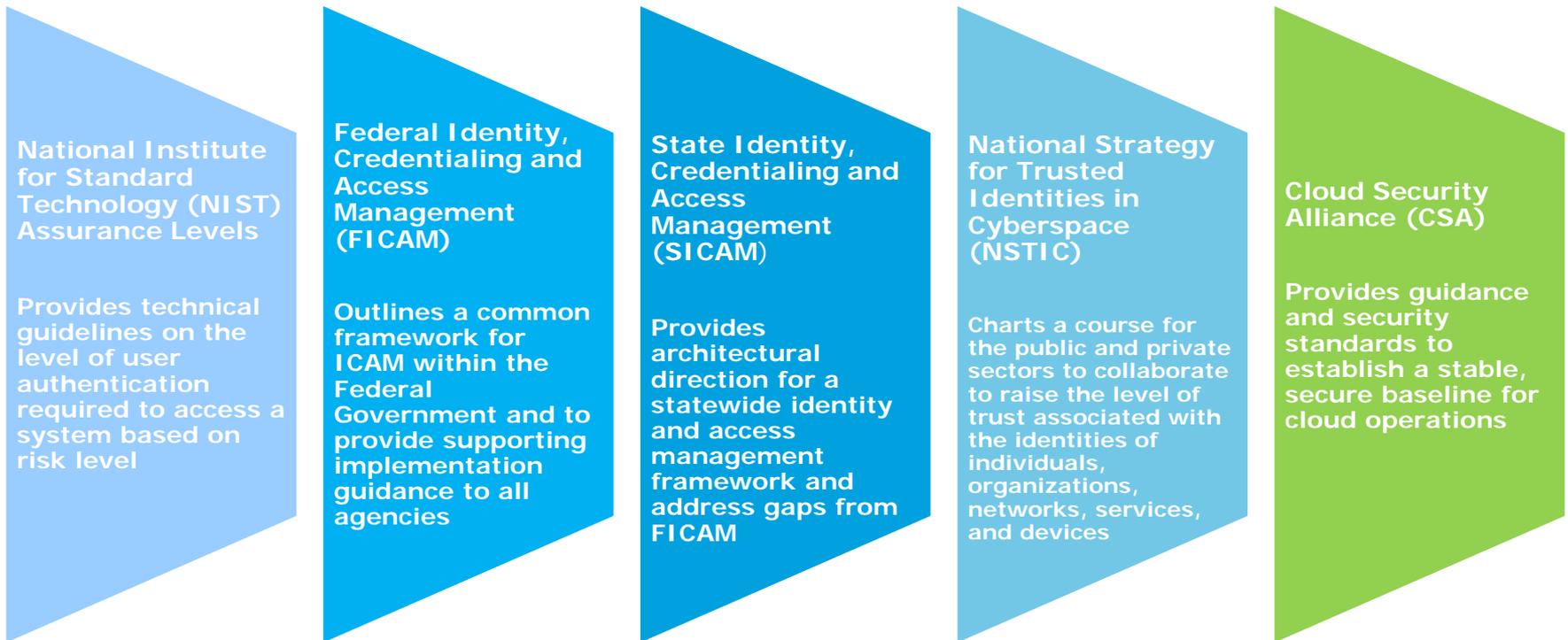
- Deployed for 435 ITD Users
- Application Integrated
 - COMiT – Helpdesk
 - Clarity – Project & Resource Management
 - CommonWiki – Collaboration
 - Active Directory – Network Services
- Identity Management Services
 - Automated Identity Provisioning
 - Automated Identity De-Provisioning
 - Self-Service Password Management (bi-directional)
 - Password Synchronization
 - Auditing
 - Compliance Reporting

- Access Management Services
 - Desktop Single Sign-On (DSSO) (via MAGNet)
 - Web-based Forms Single Sign-On (via Internet)
 - Active Directory (Network Login) Integration
- Key Design Aspects
 - Leverages existing business processes (ANF IT and CommonHelp)
 - Role based access control
 - One system to grant access and enforce controls for managed end points
 - High-availability for critical web access management components
 - Infrastructure to handle future needs



Frameworks and Guidelines

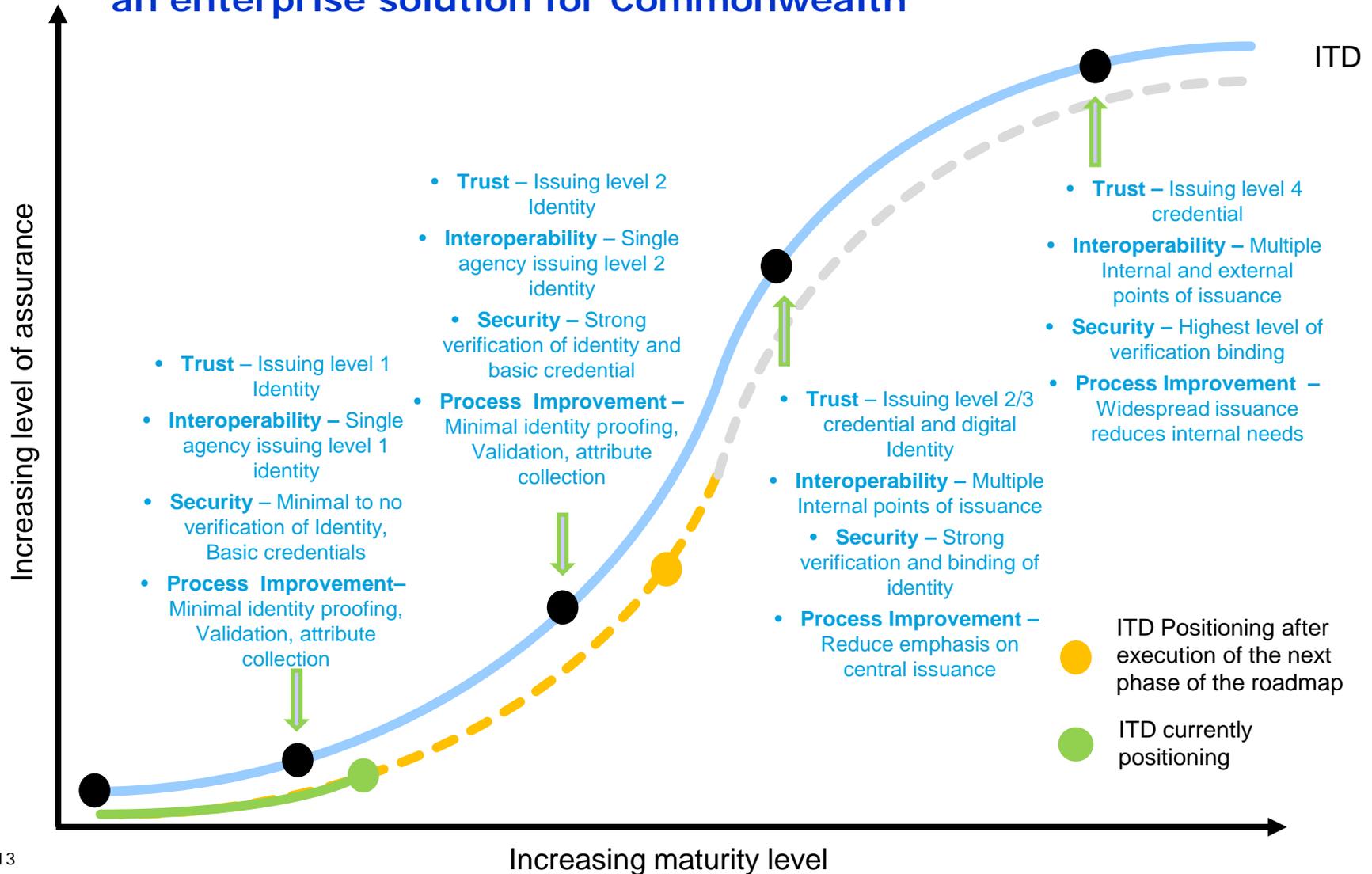
While there is no single government-wide forum responsible for coordinating and homogenizing IAM efforts across the U.S. government, there have been some key developments to guide organization over the past two years.





IAM Alignment

ITD is aligning itself with SICAM and positioning to establish an enterprise solution for Commonwealth





Four Key Goals

The industry frameworks and guidelines applicable for IAM have similar goals and objectives to facilitate the implementation.

Goal 1: Trust

- Establish trusted identity
 - Align state business processes with ICAM processes
- Establish trusted relationship with Federal, State, Local and Open providers
- Promote public confidence through transparent ICAM practices
- Ensure only qualified employees, contractors, residents and business partners access services

Goal 2: Interoperability

- Facilitate access to other interstate agency services
 - Align processes with external partners
- Leverage standards and Commercial Off-the-Shelf Technologies
 - Increase Interoperability and reuse of ICAM programs and systems

Goal 3: Security

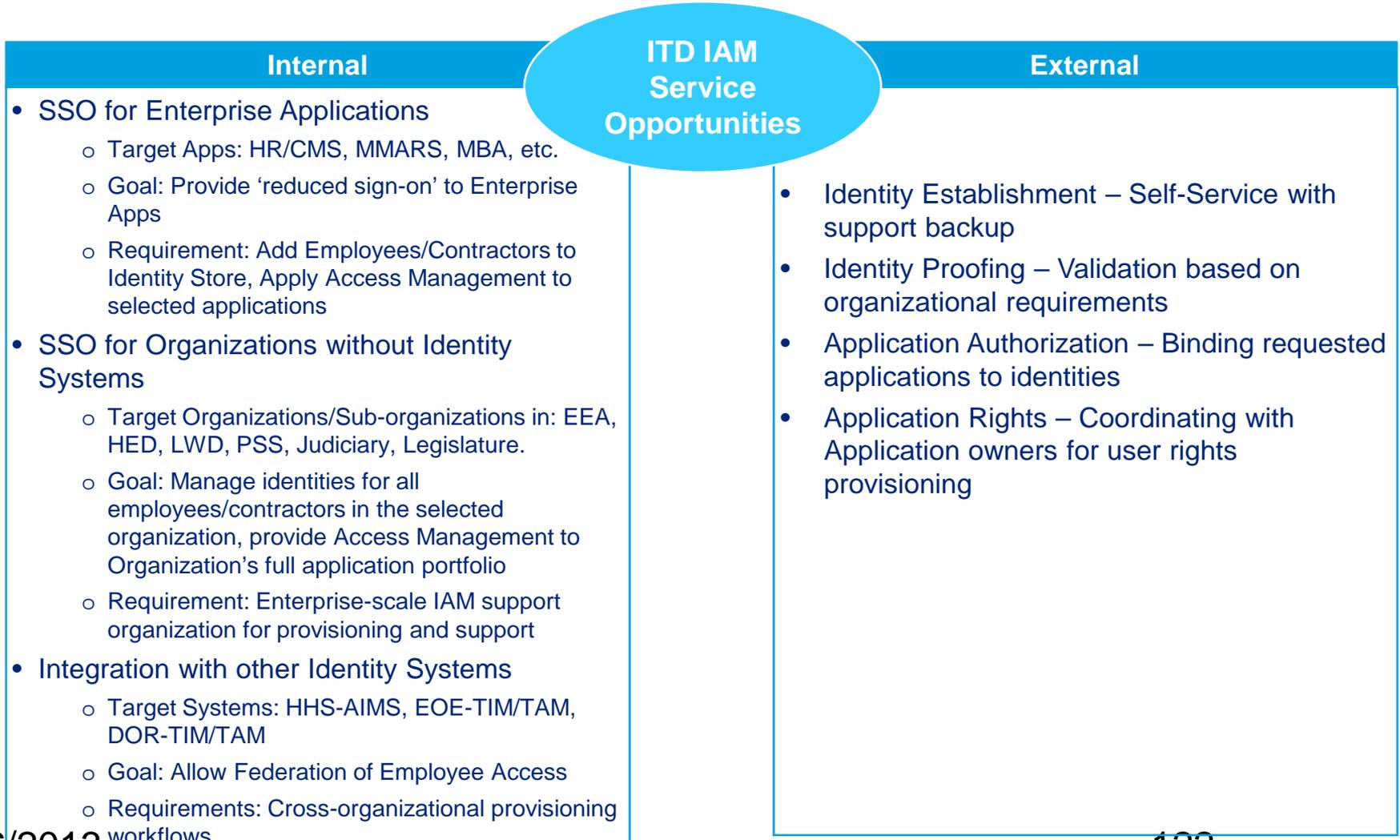
- Enable multi-factor authentication
- Expand secure access to data and systems
 - Enable cyber security programs
- Integrate electronic verification with physical security
- Enable risk-based access control frameworks
 - Improve electronic audits capabilities

Goal 4: Process Improvement

- Improve citizen facing services
 - Facilitate secure online transactions
- Offer non-repudiation through digital signatures
- Reduce administrative burden associated with performing ICAM tasks
 - Align existing and reduce redundant ICAM programs

ITD IAM Services

ITD has a unique opportunity to influence the direction and strategic positioning of the Commonwealth for IAM by capitalizing the various services opportunities made possible by implementing the roadmap



Questions?



CTR Systems Security

- Security Inbox
 - securityrequest@state.ma.us
- Scott Olsen
 - Scott.Olsen@state.ma.us
- Dan Frisoli
 - Dan.frisoli@state.ma.us
- Lenny Montone
 - Lenny.montone@state.ma.us
- Comptroller Help Desk
 - 617-973-2468



Follow us
on Twitter
@MA_Comptroller

