



WELCOME TO THE ANNUAL DEPARTMENT SECURITY OFFICER BRIEFING

March 17, 2015

COMMONWEALTH OF MASSACHUSETTS

OFFICE OF THE COMPTROLLER



Follow us
on Twitter

[@MA_Comptroller](https://twitter.com/MA_Comptroller)



Happy St. Patrick's Day





Happy Evacuation Day!





Agenda

- Welcome Remarks & Annual Update
 - Scott Olsen (CTR), Director of Department Assistance
- Identity and Access Management
 - Aldo Pietropaolo, MassIT IAM Technical Lead
- CTR Security Update - MMARS
 - Dan Frisoli (CTR), Security Administrator
- CTR Security Update - HR/CMS
 - Lenny Montone (CTR), Security Analyst
- OSD COMMBUYS Overview
 - Paul Short (OSD), COMMBUYS Functional Lead
- Wrap Up and Questions



CTR ANNUAL SECURITY UPDATE

Scott Olsen

Director of Department Assistance Bureau
Office of the Comptroller



Welcome Chris!



Chris Guido
Deputy Comptroller/ Chief Information Officer



Thank You Security Officers!!





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 30th

- MMARS/LCM
 - SECMARS
- 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



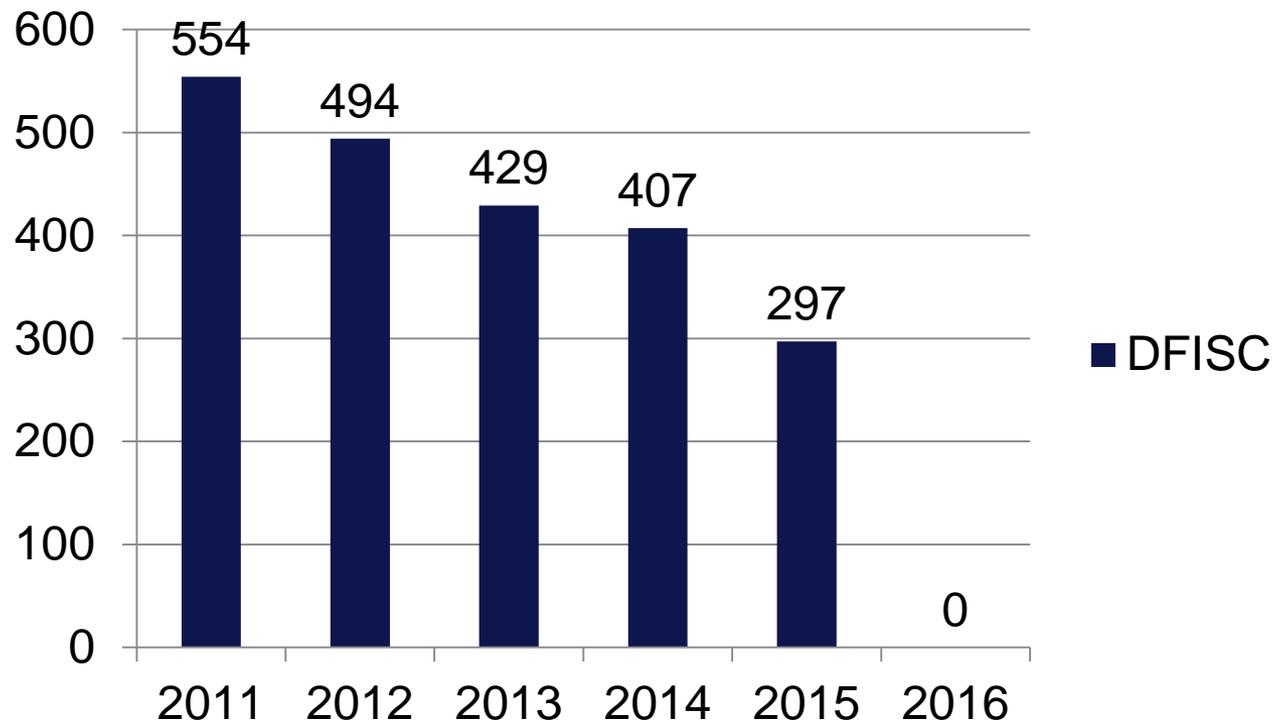
- Certification must come directly from the Department Head, either as an e-mail from their account or as a hard copy with the Department Head's signature. Use the Department Head Annual Approval of Statewide Enterprise Systems Security Form
- Latest enterprise security reports available via DocDirect
- The Comptroller's Office for MMARS or HR/CMS issues 617-973-2468
- ITD for CIW and InTempo, CommonHelp (866) 888-2808



DFISC - Fiscal Admin for All Functions

- We asked you to reduce DFISC as part of annual review, and you did!

DFISC





DFISC - Fiscal Admin for All Functions

- All requests for DFISC will be rejected
- DSOs should work with management, and CTR Security Unit, to determine the appropriate roles for users
- Dan will speak to plan for the retirement of DFISC



Reminders

- **Onboarding**
 - User Responsibility Agreement
- UAID for tracking DHSA delegation
 - Track in your Internal Controls
- Assist Department Management in identifying correct security roles for Department personnel
 - WE CAN HELP!!
- Promote Segregation of Duties
 - WE CAN HELP!!
- Monitor Department organization for changes that impacts a user's access
- **Off Boarding**



MMARS LOG IN 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.



Emergency Deletions

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



For Fastest Service

- Call the Help Desk
 - 617-973-2468
 - Comptroller.info@state.ma.us
- Calls are logged and tracked
- May be able to assist immediately



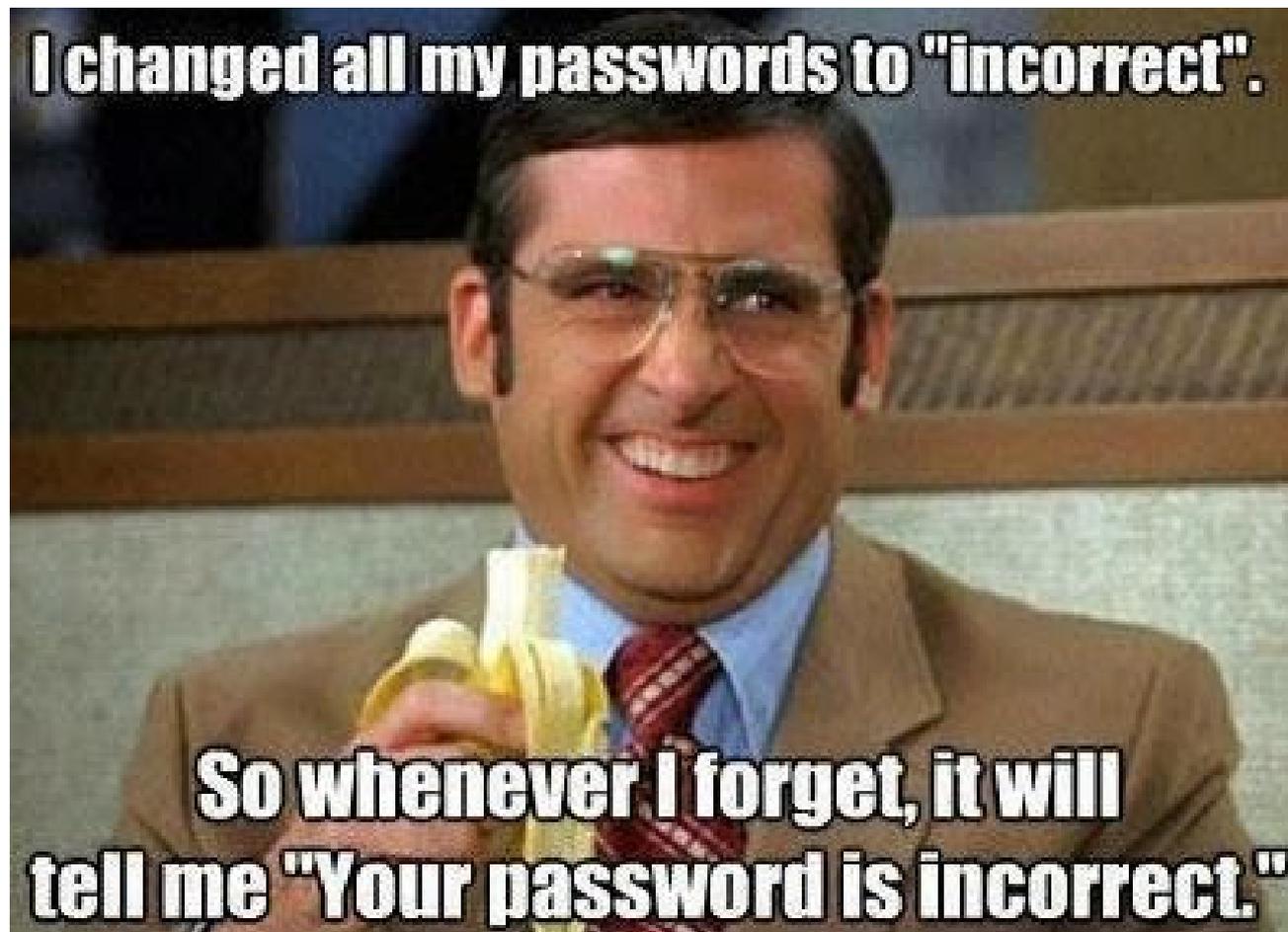
DSO Webcasts

- Plan to offer more based on feedback on the 3.9 Upgrade for UDOC webcasts
- Periodic webcasts throughout the year on specific topics



PASSWORD MANAGEMENT







Password Management

- Sharing of security system IDs (UAIDs, passwords, etc.) is prohibited
- You are responsible for activities under your log in!!
 - User Responsibility Agreement
- See Security Guide for password conventions

WORST PASSWORDS OF 2013

rank	password	change from 2012
#01	123456	⤴1
#02	password	⤵1
#03	12345678	—
#04	qwerty	⤴1
#05	abc123	⤵1
#06	123456789	new
#07	111111	⤴2
#08	1234567	⤴5
#09	iloveyou	⤴2
#10	adobe123	new



legend:

unchanged — up ⤴# down ⤵#





WORST

PASSWORDS OF 2014



- 1 123456
- 2 password
- 3 12345
- 4 12345678
- 5 qwerty
- 6 123456789
- 7 1234
- 8 baseball
- 9 dragon
- 10 football



Strong passwords have all of the following characteristics

- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- “Special” characters (e.g. @#\$%^&*()_+|~-=\`{}[]:”;’<>/ etc)
- Contain at least eight alphanumeric characters



Weak passwords have the following characteristics

- Contains less than eight characters
- Is a word found in a dictionary
- A common usage word such as: Names of family, pets, friends, co-workers, etc.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)



Social Media - TMI?

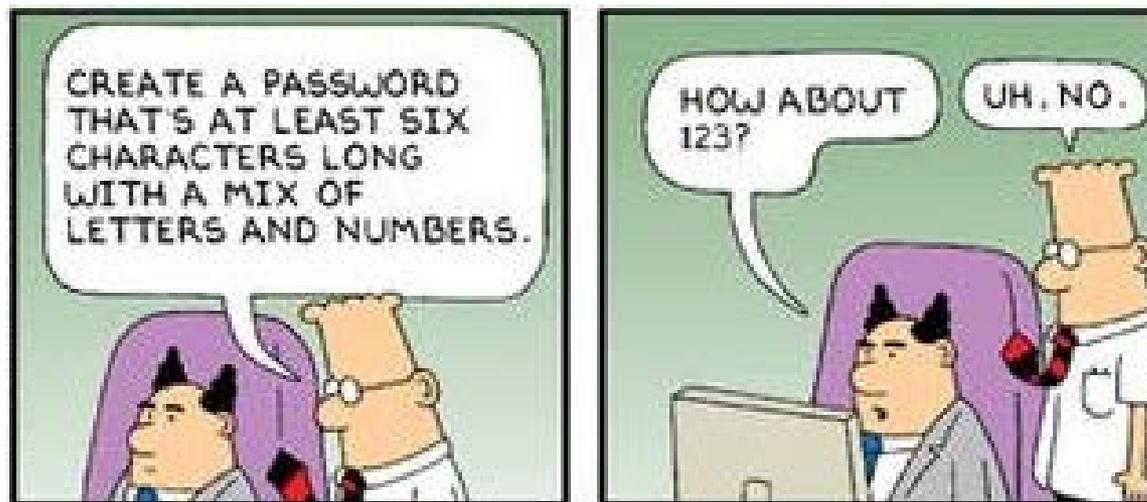


More than 11.6 Million victims of identity fraud in 2011

- 68% of social media users share their birthday
- 63% share their high school name
- 30% share their phone number or pet's name
- *All commonly used to verify identity "Secret Questions"*



We're Getting There....





Help yourself remember your strong password or passphrase by following these tips

- Create an acronym from an easy-to-remember piece of information
 - My son's birthday is 12 December, 2004.
 - Msbi12/Dec,4
- Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase.
 - My son's birthday is 12 December, 2004
 - Mi\$un's Brthd8iz 12124,
 - Microsoft Password Tips



Microsoft Password Checker

Check your password—is it strong?

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

Test the strength of your passwords: Type a password into the box.

Password:

Strength: Weak

Note: This does not guarantee the security of the password. This is for your personal reference only.

What is a strong password?

The strength of a password depends on the different types of characters that you use, the overall length of the password, and whether the password can be found in a dictionary. It should be 8 or more characters long.

Check your password—is it strong?

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

Test the strength of your passwords: Type a password into the box.

Password:

Strength: BEST

Note: This does not guarantee the security of the password. This is for your personal reference only.

What is a strong password?

The strength of a password depends on the different types of characters that you use, the overall length of the password, and whether the password can be found in a dictionary. It should be 8 or more characters long.

For tips about how to create passwords that are easy for you to remember but difficult for others to guess, read [Create strong passwords](#).



Minimize the Damage

- Use completely different sets of passwords for **Work** and **Home** use
- Do not store, document, or write down all in one place.



Staff Training

- Fraud Awareness and Prevention
- Risk Management

- Group Training conducted for Departments
- We will work with you to deliver customized training

617-973-2468

Comptroller.Info@State.MA.US



What Tools Do You Need?

- Security Guide in PartnerNet
- Briefings and Specific Guidance via webcast
- Orientation with the Security Team
 - Call or email to schedule!



We're Always Here to Help!

- CTR Helpdesk 617-973-2468
 - Comptroller.Info@State.MA.US
- Comptroller Security Mailbox
 - SecurityRequest@State.MA.US



Follow us
on Twitter

@MA_Comptroller



QUESTIONS?

Scott.Olsen@state.ma.us

617-973-2360



Identity and Access Management



Massachusetts Office of Information Technology
Executive Office for Administration and Finance

Aldo Pietropaolo (IAM Technical Lead & Industry SME)
MassIT



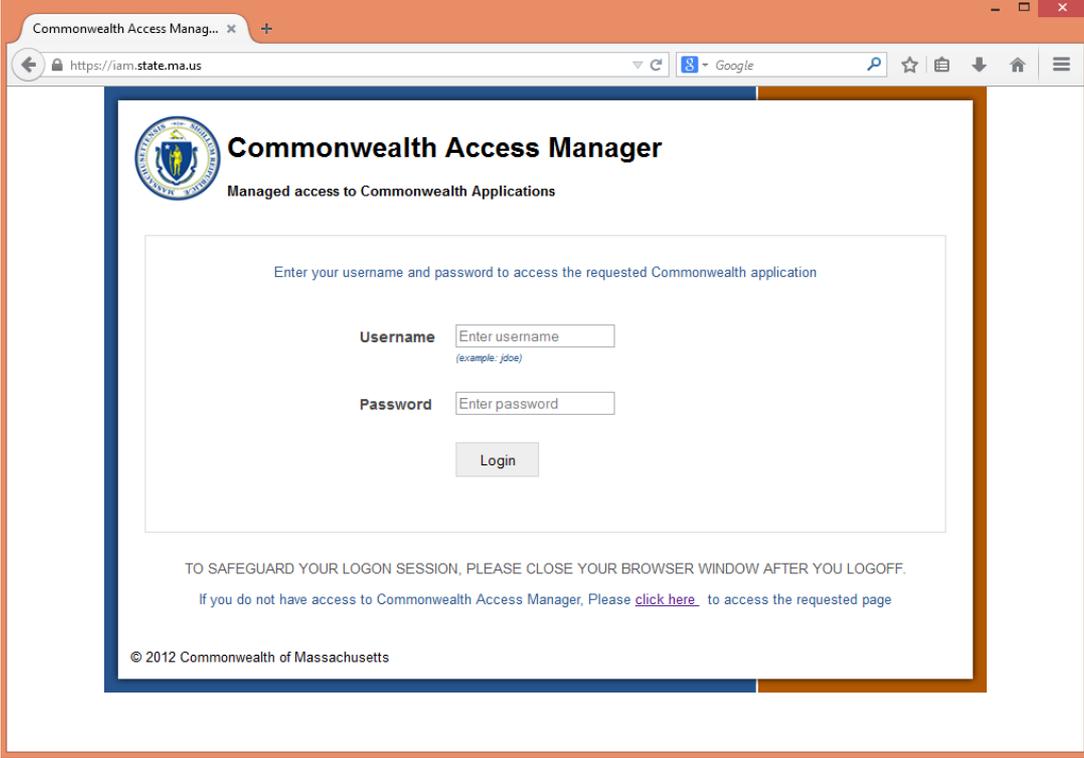
Agenda

- Identity And Access Management
- Addressing The Gaps
- MassIT Common IAM Services
- Use Case
- IAM Commonwealth Operating Models
- Questions



Identity And Access Management

Give the right people the right access to the right resources and applications, at the right time and for the right reasons.

A screenshot of a web browser displaying the Commonwealth Access Manager login page. The browser's address bar shows "https://iam.state.ma.us". The page features the state seal and the title "Commonwealth Access Manager" with the subtitle "Managed access to Commonwealth Applications". A central form prompts the user to "Enter your username and password to access the requested Commonwealth application". It includes input fields for "Username" (with a placeholder "Enter username" and a note "(example: jdoe)") and "Password" (with a placeholder "Enter password"), followed by a "Login" button. Below the form, a security notice reads: "TO SAFEGUARD YOUR LOGON SESSION, PLEASE CLOSE YOUR BROWSER WINDOW AFTER YOU LOGOFF. If you do not have access to Commonwealth Access Manager, Please [click here](#) to access the requested page". The footer contains the copyright notice "© 2012 Commonwealth of Massachusetts".



Addressing The Gaps

Significantly Reduce Implementation Costs And Address Security Gaps

Provide Faster Deployment And Consistent Security And Audit Capabilities

**IAM Assembly Line
(Continuous Delivery)
(Agile)**



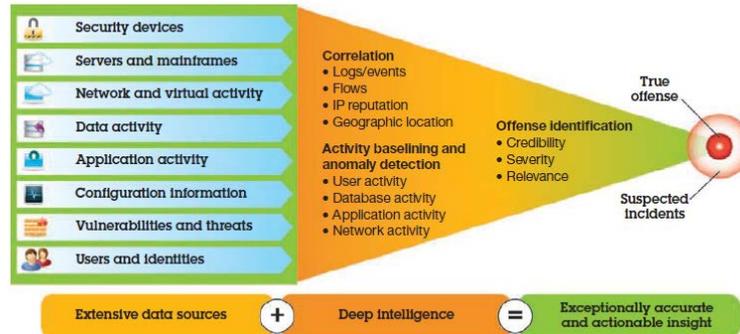
Significantly reduce implementation costs by an estimated 35% – 45%

- By adopting a continuous deployment model, small packages are processed in an assembly line fashion to yield quality results.
- Measurable return on investment for CAPEX and OPEX.
- Commonwealth business requirements and IAM technology roadmap will serve as input to assembly line.

**Increase Security
Safe Guards**



Security Intelligence delivers 360-degree view:

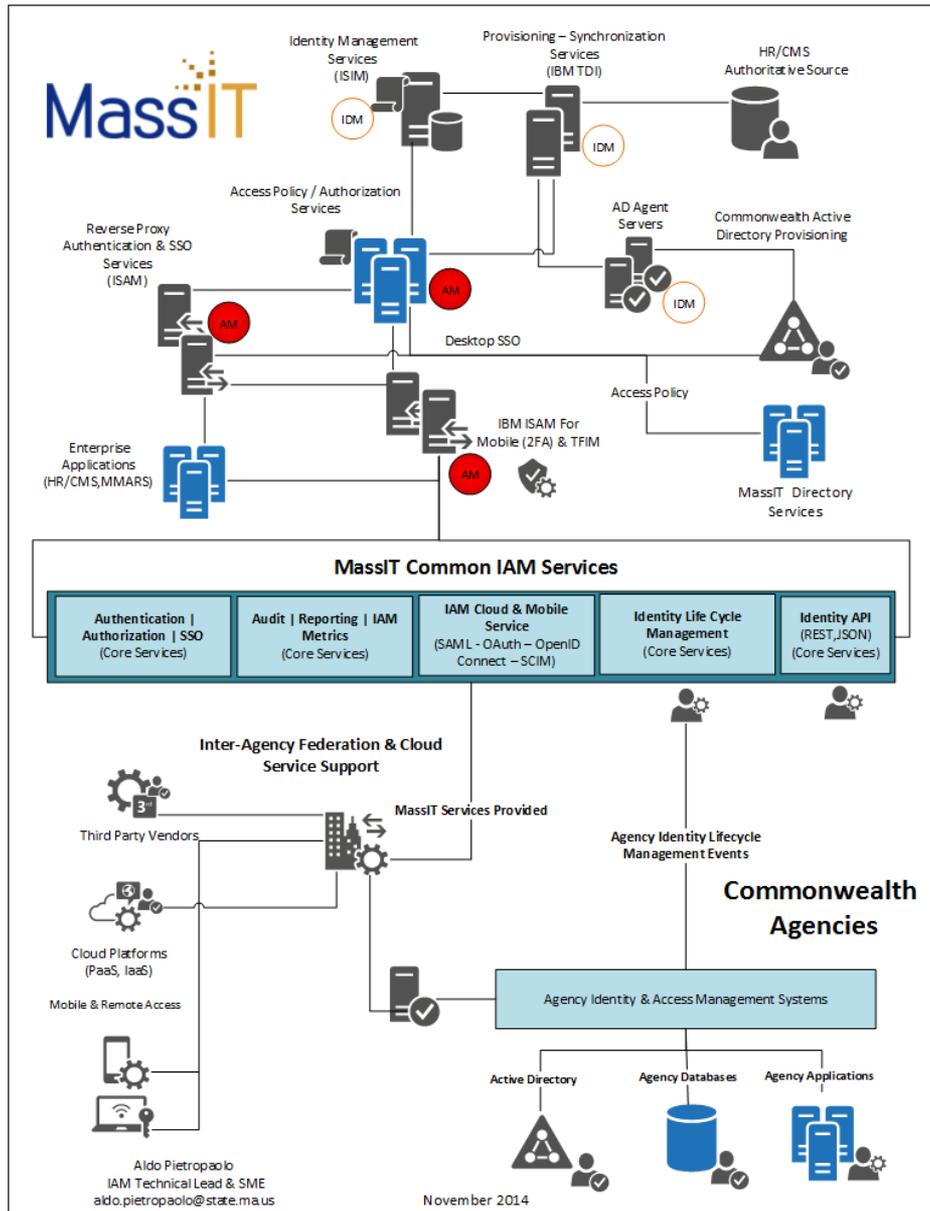


**Audit & Access
Re-Certification
Capabilities**



- Centralized service for knowing who has access to what.
- Access re-certification and revocation process – if a user has access to an application and should not, IAM will remove the access.

MassIT Services Logical Architecture



- Common IAM services in a “Private Cloud” model
- Robust access management, single sign on, and federation capabilities (SAML, OAuth, OpenID)
- Scalable and authoritative Commonwealth identity management system
- Common audit, reporting, and IAM business metrics
- Inter-Agency single sign on and Federation
- Third party vendor and cloud services support



Let's look at a real use case

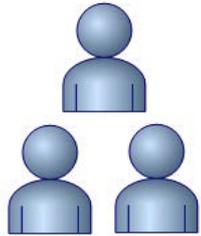


Single Sign On To All Commonwealth Applications

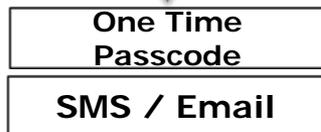
Outside Commonwealth (Internet)

Key Benefits

- One Commonwealth user id and password.
- Auditable access for employees, partners, and vendors across agencies.
- Context based authentication (2FA)



Employees | Partners | Vendors



One Time Passcode

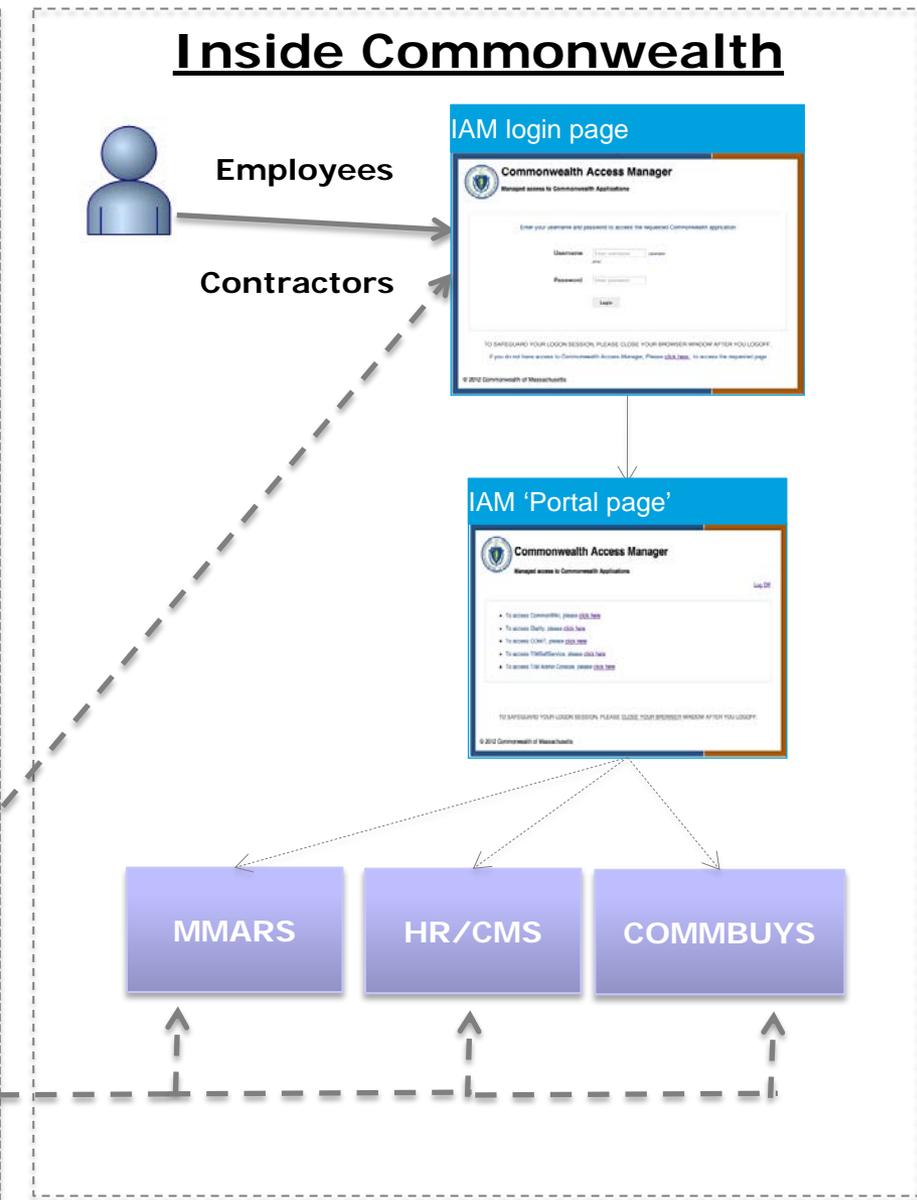
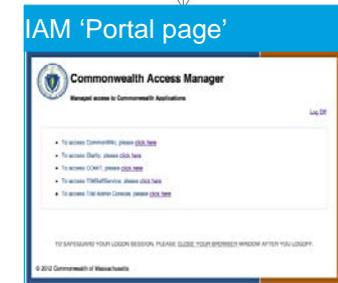
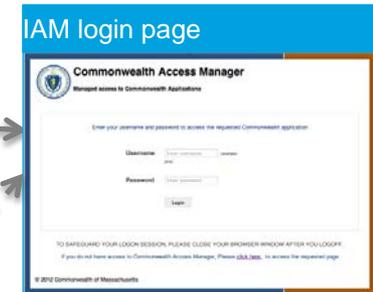


Inside Commonwealth



Employees

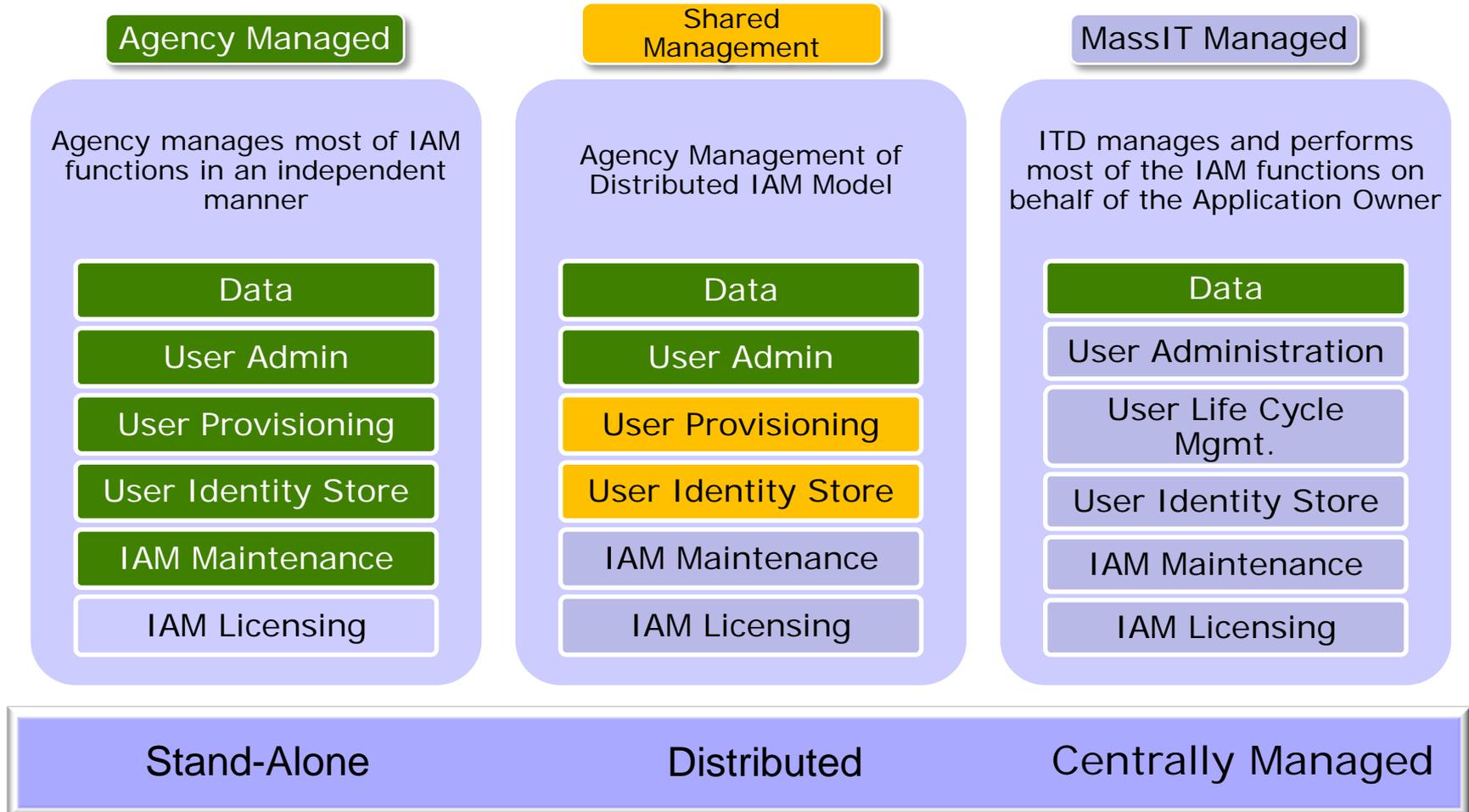
Contractors





IAM Operating Models

Given the diversity of Commonwealth's environments, the IAM Solution will need to support multiple concurrent IAM Operating models.





Questions?



Appendix



IAM Program Benefits

An improved enterprise IAM environment enables these benefits



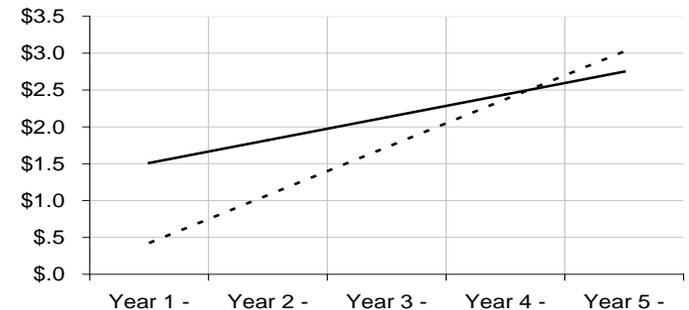
Benefit	Typical Metric
Decreased time to provision accounts	Reduce from weeks to 1h or less
Automated auditing and reporting	Decreased reporting labor through more automated processes
Simplify system architecture	Reduce development costs by 2-5% per system
Standardized login processes that simplify access	Single consolidated login process
Simplify account management & improve accuracy	Reduce labor by 50% or more
Automated password reset function	Reduce help desk calls by 75%+
De-provision accounts quickly	Decrease from days to minutes
Automated provisioning improves accuracy assignment and permissions	Decrease errors by 90% or more
Improved understanding of who has access to speed investigation	# Of Risks avoided
Enforce standardized IAM policies and procedures	Improve compliance scores, decrease risk scores
Fewer passwords or other access credentials	Reduce from dozens to a few or one

Which result in a strong, industry demonstrated return on investment



Typical Financial ROI Model

- ROI ranges from 40% to over 100%
- 100% recapture of capital investment in three years or less
- Reduced ongoing operating costs of 20% or greater



———— Total Cost - - - - - Quantifiable Benefits

*Typical Metrics and ROI Model



DAN FRISOLI

Security Administrator
Department Assistance Bureau
Office of the Comptroller



THE FINAL DFISC



DFISC Security Role

- DFISC is a MMARS role that allows the assignee to submit most MMARS Financial transactions.
- DAB Security Unit will remove DFISC from the last 298 users and replace it with 9 roles that amount to the same access as DFISC. Starting in April.
- Departments are encouraged to remove some of the 9 roles if they are not needed.



DFISC will be replaced with these roles

Security Role ID	Description
ACTPL_EDIT	Accounting Template Edit (Edit ACTPL page)
DAPA	Accounts Payable Administrator (Submit: GAX, INP, PRC)
DARA	Accounts Receivable Administrator (Submit: CR and RE)
DBGA	Budget Administrator (Submit: BGTS, BGCN, BGCS)
DFAA	Fixed Asset Administrator (Submit: FA)
DPROA	Procurement Administrator (Encumbrances)(Submit: CT, GAE, PC, RPO)
DTRSA	Trust Administrator (Mostly for Schools) (Submit: TV and RT)
DVCA	Vendor Customer Administrator (Submit: VCC, VCM)
SIGENTRY	SIG UI Page Entry - Non DFISC Departmental Users (Edit DISRQ and SIG pages)



Review Enterprise System Security Reports

Security Reports in Doc Direct are run monthly

- SECCIW – CIW Security Report
- SECHRCMS – HR/CMS Security Report
- SECINTEM – InTempo Security Report
- **SECMMARS – MMARS Security Report**
- MISRVE10 – UAID Report by UAID Report
- MISRVE20 – UAID Report by Name Report
- VPNUSSL – VPN Usage Report
- Security Reports in PartnerNet

DSOs can run an Updated PartnerNet security report at any time.



MMARS WORKFLOW

FOR DEPARTMENTS



MMARS Workflow

- MMARS transactions that meet certain parameters are submitted to a **Pending** state instead of a Final state
- Example: U05 Object code and Dept Code AGR
- Pending transactions are then routed to a shared worklist
- Department approvers access the shared worklist to review the **Pending** transactions
- Department approvers either **Approve** (submit to **Final**) or reject the **Pending** transactions
- Some transactions may move to a secondary worklist for review by control agency



Current Use of MMARS Workflow

- 29 departments currently utilize departmental level workflow
- 23 Transaction codes
- AR, BGDN, BGDS, BGTS, CEC, CT, EA, EAV, ER, EX, GAE, GAEC, GAP, GAX, IE, INP, ITA, PC, PRC, RA, RE, RPO, TV



Workflow Examples

- Many executive branch departments currently workflow UU object codes (IT related).
- Workflow setup is very flexible and can be tailored to fit the needs of your department. (Subject to CTR Bureau approval)
- Possible examples include
 - Doc Code. Have ALL CTs for your department go to workflow.
 - Thresholds. Set specific dollar amount thresholds. CT over \$50,000.00 would workflow to an approver. PRCs over \$10,000.00 would workflow.
 - Appropriations. Payments using specific appropriations could be set to workflow.
 - Combinations. Payments over \$10,000.00 and using a specific appropriation would workflow.



Benefits

- Ensure accuracy of MMARS transactions before submitting them to Final
- Monitor use of restricted appropriations or federal grants
- Reduce paper and storage costs
 - MMARS is the Official Record of Fiscal Activity. If department approvers have proper department head signature authorization then no wet signature is needed for the submission of MMARS transactions. The record is stored in MMARS.
- Remotely approve transactions via VPN



How To Get Started

- Contact The Comptroller's Office 617-973-2468
- Questions?



Webcasts for UDOCs



April 2015





Lenny Montone

Security Analyst
Department Assistance Bureau
Office of the Comptroller



Do Not Clone HR/CMS Access

User Information ViewDirect HR/CMS Warehouse

HR/CMS Information

Enter UAID to clone HR/CMS access from another UAID?

Hierarchy Tree Node:

Available Roles for User

ADDITIONAL PAY CORRECTION	<input type="checkbox"/>
ADDLPAY A/U/D	
CONFIGURATION TABLE DISPLAY	
CTR PAYROLL DISPLAY	
CTR PAYROLL VERIFICATION	
CTR PY FULL CORRECTION	



SSTA Security Enhancements

-Change or View Security Question

The screenshot shows a web application interface with a left-hand menu and a main content area. The menu is titled "Menu" and contains the following items: "Self Service", "Change My Password", "My Personalizations", and "My System Profile". The main content area is titled "General Profile Information" and contains two input fields: "Enter your DOB (MM/DD/YYYY):" and "Last four digits of your SSN:". Below these fields are "Submit" and "Return" buttons. A "Save" button is located at the bottom left of the main content area. A "Message" dialog box is open in the bottom right corner, displaying the text "To proceed, please answer your security question(s). (20001,1050)" and an "OK" button.

Menu

- Self Service
- Change My Password
- My Personalizations
- My System Profile

General Profile Information

Enter your DOB (MM/DD/YYYY):

Last four digits of your SSN#

Submit [Return](#)

Save

Message

To proceed, please answer your security question(s). (20001,1050)

OK



View W2 Form

- Menu
- Self Service
 - Time Reporting
 - Personal Information
 - Payroll and Compensation
 - View Paycheck
 - Direct Deposit
 - W-4 Tax Information
 - View W-2/W-2c Forms**
 - W-2/W-2c Consent
 - Change My Password
 - My Personalizations
 - My System Profile

View W-2/W-2c Forms

Security Question What is you favorite food?

Response

Submit

Message

To proceed, please answer your security question(s). (20001,1050)

OK



Change Direct Deposit

Menu

- Self Service
 - Change My Password
 - My Personalizations
 - My System Profile

General Profile Information

Enter your DOB (MM/DD/YYYY):

Last four digits of your SSN#

Submit

[Return](#)

Save

Message

To proceed, please answer your security question(s). (20001,1050)

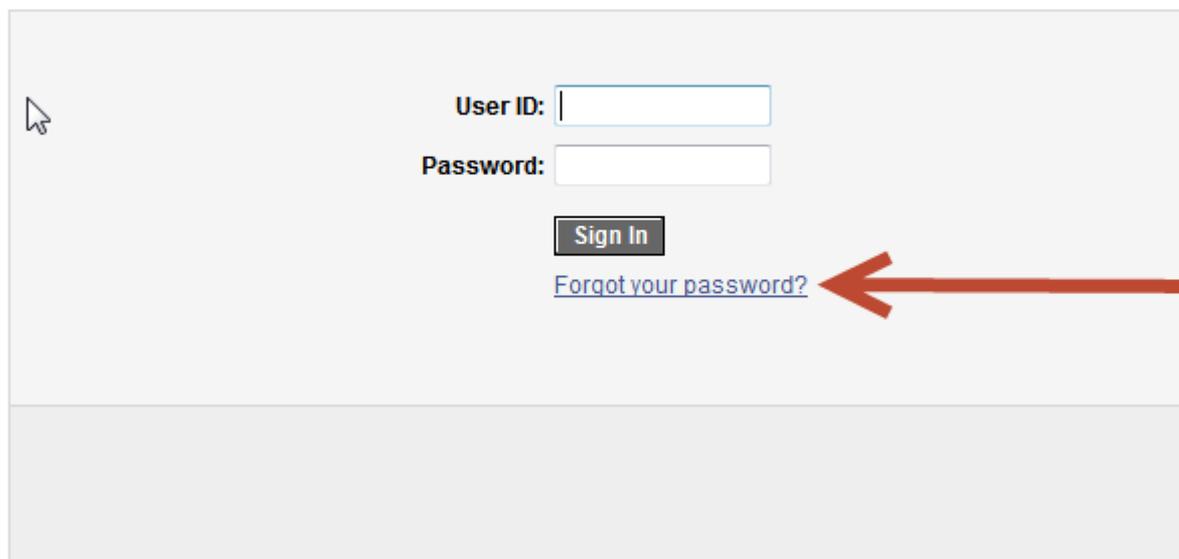
OK



Self Service Password Reset

- Numerical Employee ID's Only

ORACLE
PEOPLESOFT ENTERPRISE



User ID:

Password:

[Forgot your password?](#)



Forgot My Password

✓ If you have forgotten your password, or your password has expired, you can have a new password emailed to you.

Enter your User ID below. This will be used to find your profile, in order to authenticate you.

Enter Your User ID to find your profile:

Continue

 Refresh



Forgot My Password

User ID: XXXXXX

Email ID: Peter.T.Steele@ton.net

Please answer the following question below for user validation.

Question: What is you favorite food?

Response:

[Email New Password](#)



New HR/CMS v9.2 Add On Role:

Time and Labor Administrator

- This role will not appear in the InTempo list of available roles
- When CTR Security adds Time and Labor A/U/D or SS_TA_Admin to a profile the system will automatically add this role
- Role has NO permissions.
- Security Guide updated before v9.2 launch



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
 - Comptroller.Info@State.MA.US



Follow us
on Twitter
@MA_Comptroller