



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

July 11, 2012

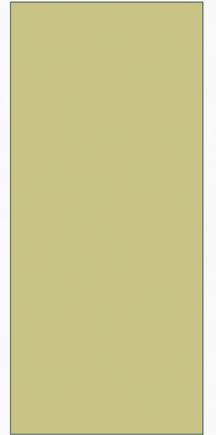


# ISOAG July 2012 Agenda

- |      |                                  |  |
|------|----------------------------------|--|
| I.   | Welcome & Opening Remarks        | Michael Watson, VITA                                 |
| II.  | PCI Compliance                   | Andrew Hallberg, ABC & Shirley Payne, UVA            |
| III. | ISO Family Feud                  | Ed Miller, VITA                                      |
| IV.  | VITA MITA Program Overview       | Rich Barnes, VITA                                    |
| V.   | Upcoming Events & Other Business | Michael Watson, VITA                                 |
| VI.  | Partnership Update               | Bob Baskette, VITA<br>Adenike Lucas & Mike Clark, NG |

# PCI COMPLIANCE

ANDREW HALLBERG, ABC  
SHIRLEY PAYNE, UVA





# WHERE DOES IT COME FROM?



# WHAT'S IT FOR?



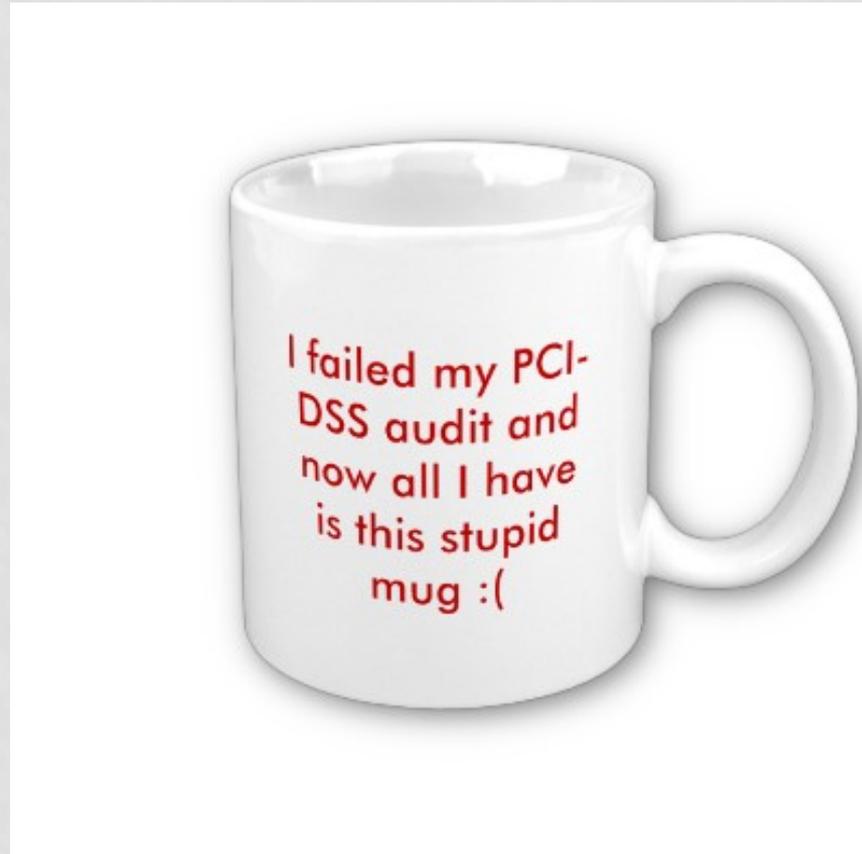
# WHO NEEDS IT?

- All merchants, small or large, that accept credit cards, need to be PCI compliant.
- Sell a product?
  - Liquor
  - License
  - Gifts
- Charge for events?
  - Classes
  - Registrations
  - Events
- Fees/Penalties

# WHO NEEDS IT?

Level	Merchant Criteria
1	Process over 6,000,000 transactions annually <u>or has suffered a breach</u>
2	Process between 1,000,000 and 6,000,000 transactions annually
3	Process between 20,000 - 1,000,000 transactions annually
4	Process under 20,000 transaction annually

# HOW IS IT CHECKED?



# HOW IS IT CHECKED?

Level	Merchant Criteria
1	3rd party PCI approved Qualified Security Assessor(QSA) to perform a yearly onsite assessment, yearly penetration tests and quarterly security scans by an approved PCI scanning vendor
2 and 3	complete a yearly self assessment questionnaire(SAQ) and quarterly security scans by an approved PCI scanning vendor
4	Recommended to perform level 2 and 3 requirements but not enforced

# WHAT ARE THE COMPONENTS?

1. Install and maintain a firewall
2. Do not use vendor default passwords
3. Protect stored data
4. Encrypt transmissions of cardholder data

# WHAT ARE THE COMPONENTS?

5. Use and update antivirus software
6. Develop and maintain secure systems and applications
7. Restrict access by need-to-know
8. Assign unique IDs to all users

# WHAT ARE THE COMPONENTS?

9. Restrict physical access to cardholder data
10. Track and monitor access to cardholder data
11. Regularly test security systems and processes
12. Maintain an information security policy

# IMPLEMENTATION DETAILS...

We use Trustwave for

- SAQ
- QSA
- Quarterly vulnerability scans
- Internal and External Penetration testing



Powered By **SpiderLabs**®

# WHAT IF I DON'T?

- Starts with fines
- Removal credit card acceptance privileges
- Reporting requirements
  - COV reputation at stake
- If found non-compliant and a breach occurs, additional charges levied per account compromised

# A PROGRAM FOR PCI COMPLIANCE

# GETTING TO COMPLIANCE



1. ORGANIZE



2. ASSESS



3. PLAN &  
REMEDiate



4. EDUCATE



5. VERIFY

# STEP 1: ORGANIZE

## Determine Who Leads

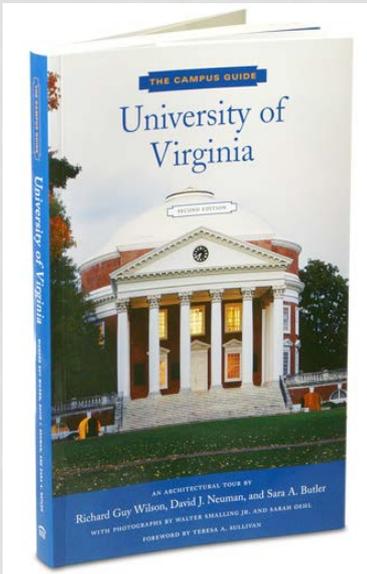


# STEP 1: ORGANIZE

## Involve All Appropriate Parties



# LOTS TO CONSIDER IN HIGHER ED ENVIRONMENT



# STEP 2: ASSESS

- Determine Scope
  - Merchant level (based on card transaction volume)
  - Processes where CHD stored, processed, or transmitted
  - PCI regulations applicable to each process
- Conduct Gap Analysis

# STEP 2: ASSESS

- Determine Scope
  - Merchant level (based on card transaction volume)
  - Processes where CHD stored, processed, or transmitted
  - PCI regulations applicable to each process
- Conduct Gap Analysis
- Investigate Scope Reduction Options

# STEP 3: PLAN & REMEDIATE

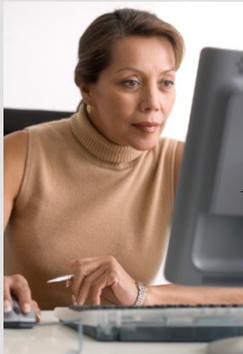
Top five vulnerabilities according to VISA:

1. Storing prohibited data, e.g. card verification values
2. Unpatched systems
3. Use of vendor default settings and passwords
4. Poorly coded web applications
5. Unnecessary and vulnerable services on servers

# STEP 3: PLAN & REMEDIATE



**Ensure sensitive data collected only when essential**



**Ensure sensitive data access authorized to least # of people**



**Business Processes & Supporting Technology**



**Ensure sensitive data stored or transmitted only when essential**



**Ensure sensitive data handled only by highly secured devices and networks**

**Enhance data protection policies/procedures as needed**  
**Strengthen data protection provisions in 3<sup>rd</sup> party contracts**

# REDUCE SCOPE

- Eliminate storage of data
  - If you don't need to keep the card data for
    1. Returns
    2. Affinity Programs
    3. Return purchases
  - Don't!
- Outsource payment processing
- Segment network

# STEP 4: EDUCATE

- Training program for managers and staff covering:
  - PCI compliance overview
  - Applicable policies and procedures
  - Incident reporting guidance
  - Consequences of non-compliance
- Central repository of resources
- Periodic updates to executives

# EDUCATE TO ERADICATE



False front (Skimmer) placed over the face of an ATM in Texas.



Camera hidden inside pamphlet holder next to ATM at the University of Texas campus

# NEED TO IDENTIFY...



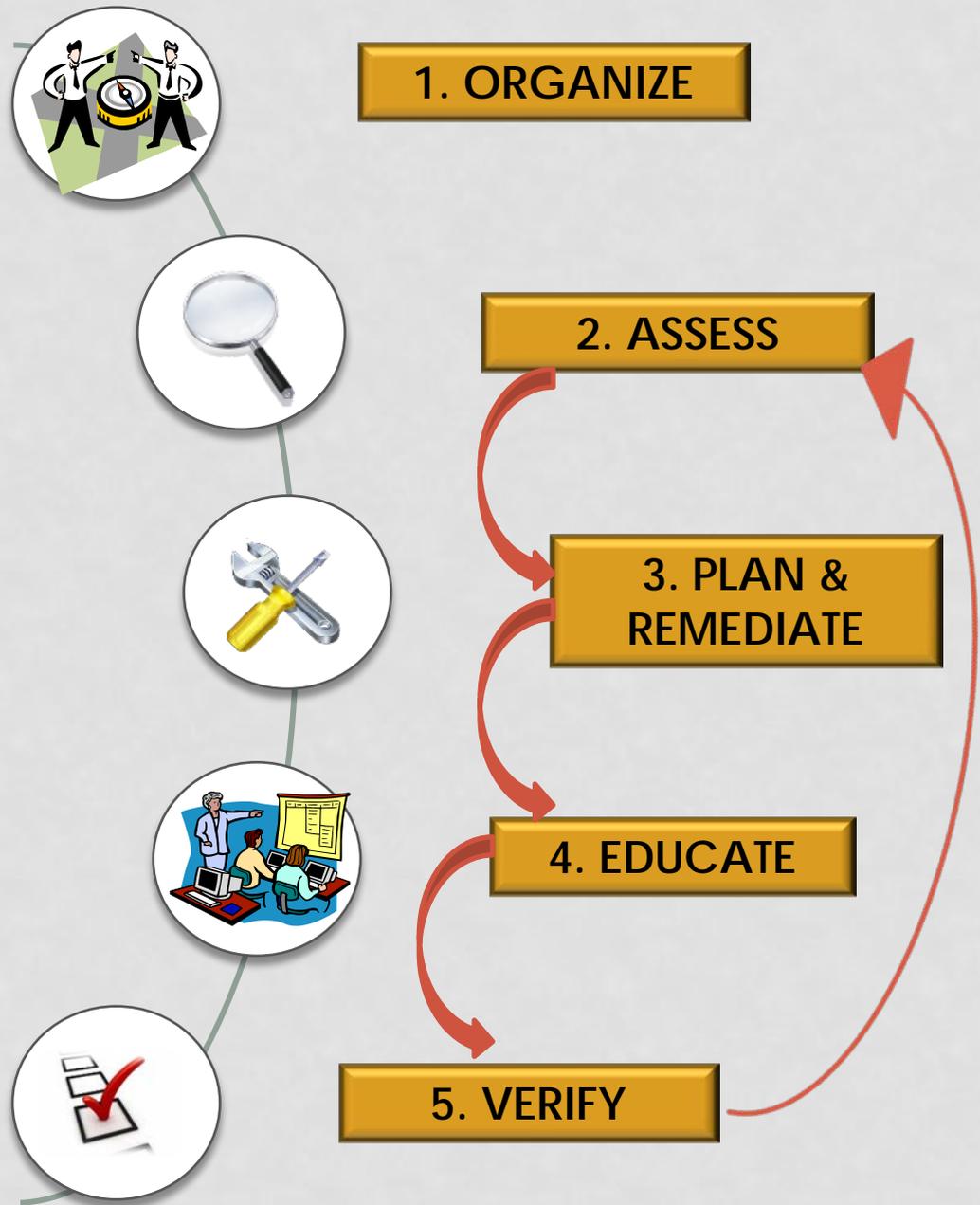
- Pwn Plug Elite
- \$800, available to the public
- Has everything needed to sniff/steal/send pre-installed

# STEP 5: VERIFY

- Annual self-assessment questionnaire
- Quarterly\* vulnerability scans of Internet-facing, in-scope IP addresses
- Annual\* penetration tests
- Attestation of compliance form

\* and after significant change occurs

# COMPLIANCE IS AN ONGOING PROCESS



# SOME PCI MYTHS

- Outsourcing card processing makes us compliant
- PCI compliance is an IT project
- PCI will make us secure
- PCI requires us to hire a QSA
- PCI requirements are unreasonable
- We don't take enough credit cards
- We completed a SAQ so we're compliant

# MORE INFO

- <https://www.pcisecuritystandards.org/>
- Andy Hallberg
  - [Andrew.Hallberg@abc.virginia.gov](mailto:Andrew.Hallberg@abc.virginia.gov)
- Shirley Payne
  - [scp8b@virginia.edu](mailto:scp8b@virginia.edu)



# ISO FAMILY FEUD



Ed Miller

Commonwealth Security & Risk Management

---

ISOAG Meeting

## OBJECT

Teams try to provide all of the answers to a question that has multiple correct answers before getting 3 strikes (for providing wrong answers)

## FACEOFF

Each round starts with a Faceoff

One player from each family comes to the podium.

Each player takes a buzzer

Reveal the game board (each game board is a round)

I'll read the question

First person to buzz gets to answer

If it's a right answer the family can decide to pass or play.

## GAME PLAY

If the family decides to play, each team member gets to answer in sequence.

For game play, family members stay at the table.

I'll ask the next family member in sequence to give their answer

Each right answer scores 10 points for the team

Each wrong answer gets a STRIKE (X).

If the team reveals all answers before they get 3 strikes, they win the round, and 10 points for each revealed answer.

If the team gets 3 strikes before all answers are revealed, the other team gets to "steal" the round and all the points if they can come up with one of the remaining answers.

Points awarded each round are added to each team's cumulative score.

Highest cumulative score at the end wins the game.

**FACE  
OFF**

**150 FAMILY FEUD**

# Name a castaway on Gilligan's Island:

1) X X X X X X

2) X X X X X X

3) X X X X X X

4) X X X X X X

5) X X X X X X

6) X X X X X X

7) X X X X X X



Time

Yes!

No

# Name a castaway on Gilligan's Island:

Gilligan

Ginger

the Skipper

Mary Ann

Professor

Thurston Howell, III

Lovie Howell



Time

Yes!

No

# Commonwealth ISO Family Feud



Thanks for playing!



# VITA MITA Program Overview

Rich Barnes  
Acting Program Manager



# VITA MITA Overview

1. Opening Remarks & Program Background – *Rich Barnes, VITA Program Manager*
2. Overview of Enterprise Data Management (EDM) – *Sean Weir, EDM Project Manager*
3. *Data Sharing Challenges* – *Joe Grubbs, Enterprise Data Governance Lead*
4. Commonwealth Authentication Service (CAS) – *Mike Farnsworth, CAS Project Manager*
5. Service Oriented Architecture Overview – *Todd Kissam, VITA Enterprise Architect*
6. Competency Centers, Wrap-up, and Q & A – *Rich Barnes*



## Program Background

- The Patient Protection and Affordable Care Act of 2010 (PPACA) mandates an expansion of Medicaid enrollment that is predicted to increase Virginia's Medicaid membership by 35% to 45%.
- PPACA and the American Recovery and Reinvestment Act (ARRA) provide federal funding for States to modernize Health Information Technology (HIT) systems.
- Medicaid Information Technology Architecture (MITA) is intended to foster integrated business and IT transformation across the national Medicaid enterprise that will enable successful administration of the expanded Medicaid program under PPACA.
- Leverages federal funding to provide services that can eventually be used by all state agencies
- HHR Secretary requested that VITA provide Enterprise-level services in support of the MITA Program.



## Enterprise-Level Services

- Historically, these tools have been too expensive for agencies to procure themselves.
- Sharing allows the Commonwealth to leverage the HHR investment and results in significant value. Examples:
  - Reusability of services among agencies
  - Decoupling legacy applications
  - Shared testing & development environments
  - Shared expertise and support



## Active VITA MITA Projects

- **Enterprise Data Management (EDM)**  
Is “John Smith” the same person as “Jonny Smyth?” EDM’s sophisticated logic can be used in bringing together data from multiple sources to provide a single, “trusted” view of data entities for any user or application.
- **Commonwealth Authentication Service (CAS) – DMV and VITA**  
CAS will provide improved verification of identity, expediting citizens’ access to services while protecting against identity theft and fraudulent activities.
- **Service Oriented Architecture Platform (SOA)**  
A suite of several tools that will expedite connecting legacy applications to new services, support sharing and reuse of Web services across agencies, facilitate the automation of business rules and much more.



## EDM – Where's the Value?

- Greatly reduced error rates in enrollment
  - Improved fraud prevention and detection
  - Reduced rework
  - Automated services can accurately retrieve information
  - Provides a composite view of person data (Golden Record) from existing systems
  - Delivers functionality as a web service to authorized subscribers
- Single trusted view of person allows an agency to see a customer's complete relationship with the Commonwealth (participating agencies) leading to better service, improved customer satisfaction and more informed decision making.

# EDM Solution

## Major Capabilities

### Initiate<sup>®</sup> MASTER DATA SERVICE<sup>®</sup> PLATFORM

#### Initiate<sup>®</sup> INSPECTOR<sup>™</sup>



Issue Resolution



Hierarchy/  
Relationship  
Management



Central Data Store

#### Initiate<sup>®</sup> DATA HUBS



Provider



Organization



Person

#### Initiate<sup>®</sup> WORKBENCH<sup>®</sup>



Master Data  
Engine



Configuration &  
Administration

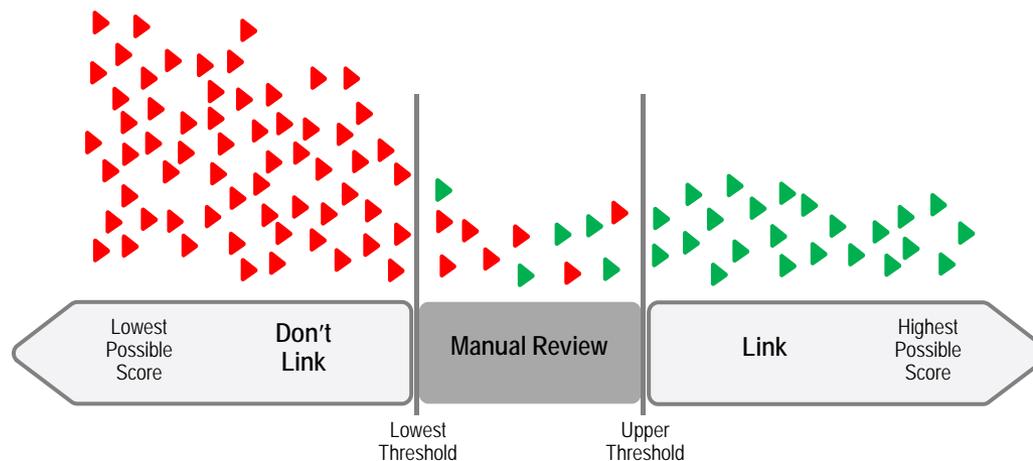


Integration

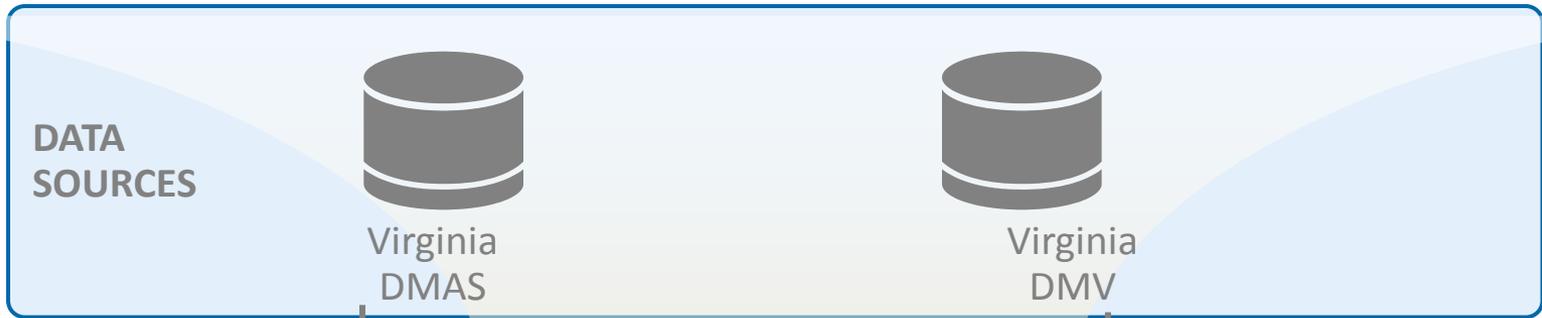
- Stores/Manages data from multiple sources
- Uses statistical probability theory/matching algorithms to compare and link records
- Enables data stewardship – supports issue resolution (e.g. duplicates, overlays, etc.)
- Receives updates in real-time or batch
- Data integration
- High performance

# EDM – Creating the Golden Record

- Bases weights on actual data
- Determines how ‘close’ two values are
- Looks for incorrectly used and ‘overloaded’ columns
- Assigns thresholds for clerical review
- ‘Learns’ from human input
- Enables data stewardship
- Recognizes equivalencies



# EDM – the Golden Record



Name	NPI	DOB	SSN	Sex	Address 1	Zip Code	Phone	IRS TIN#
Deborah Becker		06021964	491-86-4511	Female	43776 Maison Blanc Square	60054	312-334-1012	
Dr. Debbie Becker	1821125661	02-06-64	491-86-4511	Female	19456 Madison, Suite 207	60606	312-334-1012	454-76-1211
Deborah Becker	1821125661	06-02-1964	491-86-4511	Female	43776 Maison Blanc Square	60054	312-334-1012	454-76-1211



## Data Sharing - What is a DURSA?

- Data Use and Reciprocal Support Agreement
- Multi-party trust agreement among Participants in the information exchange
- Scalable alternative to multiple “point-to-point” agreements
- Common set of terms and conditions that establish obligations, responsibilities and expectations for information exchange
- Framework for safe and secure information exchange, designed to promote trust and protect the privacy and security of shared data

# Data Sharing - DURSA Elements



Source: Gravely, Steven D. 2011.  
[http://www.vita.virginia.gov/uploadedFiles/VITA\\_Main\\_Public/EAD/Enterprise\\_Data\\_Management/AppendixC\\_DURSA\\_overview.pdf](http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/EAD/Enterprise_Data_Management/AppendixC_DURSA_overview.pdf)



## Data Sharing - Major Challenges

- Statutory authority to promulgate a Commonwealth DURSA and governance framework
  - DURSA “Owned” by Secretary of HHR
  - SoTech, CIO and VITA in Technology and Data Governance Support Role



## Data Sharing - Major Challenges

- Statutory authority to allow interagency data-sharing
  - Clear, affirmative statement of legal authority before DURSA can be executed
  - Informed consent and notification

# CAS – Houston, We Have A Problem



*"On the Internet, nobody knows you're a dog."*

The above cartoon by Peter Steiner has been reproduced from page 61 of July 5, 1993 issue of [The New Yorker](#), (Vol.69 (LXIX) no. 20) only for academic discussion, evaluation, research and complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.

## CAS – the Problem(s)

- Feds (HHS) estimates 16% of Virginia Medicaid Eligibility records are in an “error” status
  - > Represents hundreds of millions of dollars
  - > Pressure on states by Feds to correct the problem
  - > Eligibility fraud continues to grow
- Duplicative Processes
  - > Eligibility processes performed by multiple agencies
  - > Budget deficit can no longer support duplication
- No fully automated Commonwealth level communication exists between agencies for authenticating a citizen’s identity



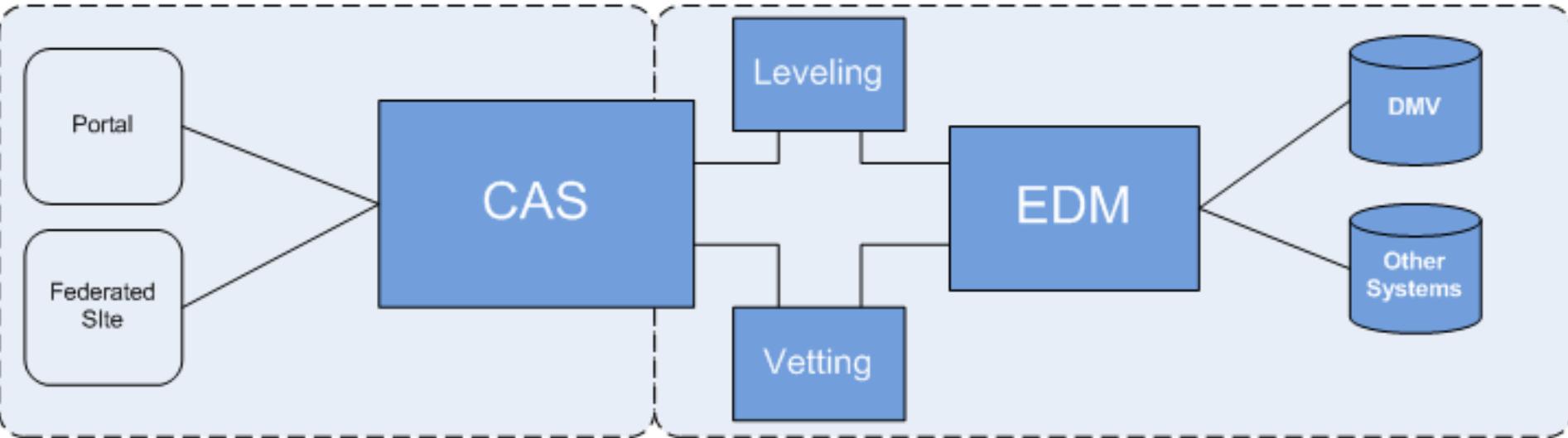
# CAS – What Are We Doing About It?

- Collaborative effort between VITA and DMV
- CAS will offer
  - NIST Level 1-3 compliant credentials
  - Enterprise Identity Service
  - Competency Center for on-boarding
- CAS Services
  - Identity Proofing
  - Identity Credential
  - Multi-Factor (Strong) Authentication
  - Identity Binding

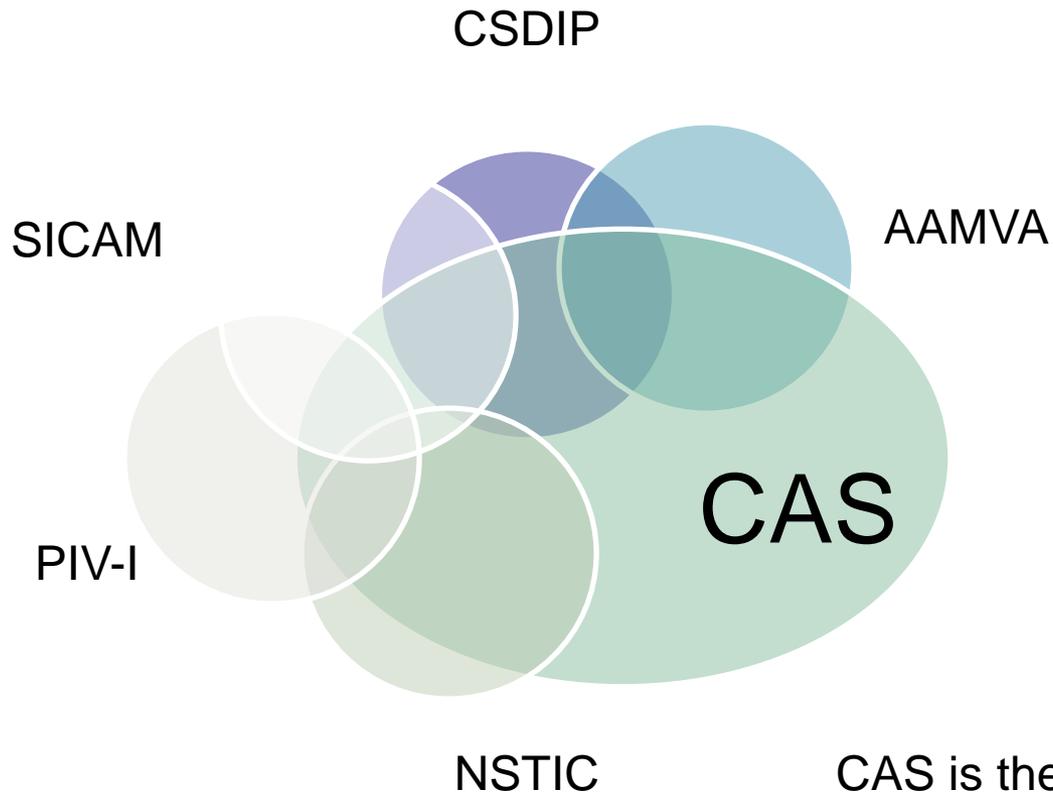
# CAS – What are we doing?

CAS Registers, Stores,  
and Manages Users along  
with notifications and help  
desk activities

EDM maintains common  
entities



# CAS – Initiative Relationships



CAS is the glue for other strategic initiatives



## Rationale for Shared Service Platform

- Historically, these tools have been too expensive for the agencies to procure themselves.
- Sharing allows the Commonwealth to leverage the HHR investment and results in significant value. Examples:
  - Reusability of services among agencies
  - Decoupling legacy applications
  - Shared testing & development environments
  - Shared expertise and support

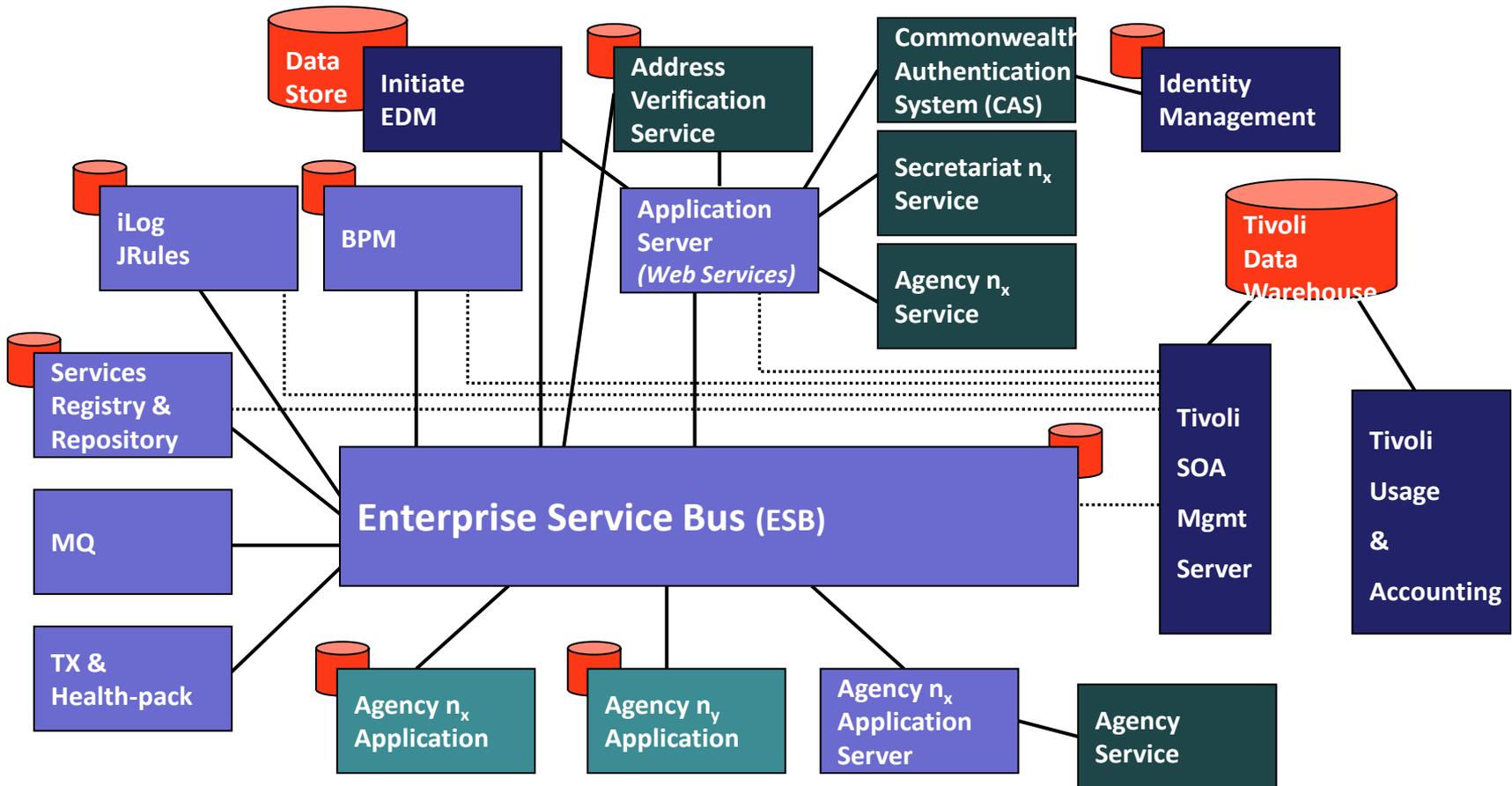
# SOA Platform - components

- WebSphere ESB (Enterprise Service Bus)
  - Connects legacy applications to newly developed applications and services
  - Manages data exchanges between agencies and to/from external organizations
- WebSphere MQ (Robust Asynchronous Messaging)
  - Guarantees persistence of messages and supports publish/subscribe model (ex. VDH publishes death notice once on queue, agencies subscribe as needed (daily, weekly, etc.))

## SOA Platform - components

- WebSphere ILOG Jrules (Business Rules Management System (BRMS))
  - Targeted use by Business Analysts: reduced reliance on programmers
  - The ability to express decision logic using a business vocabulary and graphical representations (decision tables, trees, scorecards and flows)
  - Improved efficiency of processes through increased decision automation

# Commonwealth SOA Platform Components





## Competency Centers

- On-boarding Business Process
- Standards, Policies & Guidelines
- Help Desk Plan
- Education/Training Plan
- Staffing Plan
- Change Management
- Cost Model



# VITA MITA Q&A





Virginia Information Technologies Agency

# Commonwealth Business Impact Analysis

**Mike Watson**

Chief Information Security Officer

---



# COV Business Impact Analysis

- Under the provisions of § 2.2-2009, additional duties of the CIO, the CIO is required to develop a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps
- To enhance the development of the risk program we are requesting Business Impact Analysis, (BIA) information for agency functions that use IT systems. The collected BIA data will assist in identifying COV risks.



# BIA Survey Procedure

Step 1 : An e-mail with a list of BIA related questions will be sent to all Information Security Officer's (ISO's) to assist in preparing for the BIA survey.

Step 2: In a phased approach sometime after the first e-mail, a second e-mail will be sent providing instructions on how to complete the BIA survey. Partnership and non-partnership agencies will receive two different sets of instructions.

Step 3: Once the survey is completed and/or you have any questions, please send an e-mail to Commonwealth Security at [CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)



## BIA Survey Procedure continued

Step 4: Commonwealth Security and Risk Management will perform an analysis of the information and release it with the annual report.



Virginia Information Technologies Agency

# Upcoming Events





## Proposed Revision to the *Information Security Standard* (ITRM SEC501-07)

- The proposed revision to the *Information Security Standard* is posted on the VITA Online Review and Comment Application (ORCA) for your review and comments.
- The draft revision broadens the requirements of the *Information Security Standard* to include security best practices in line with the National Institute of Standards and Technology (NIST) specifically NIST 800-53. The revised standard will define the minimum information security management requirements for Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education. The standard was developed in partnership with the Information Security Council and discussed in Information Security Officers Advisory Group (ISOAG) meetings over the past year.



## Proposed Revision to the *Information Security Standard (ITRM SEC501-07)*

- The 30-day comment period will run until August 1, 2012. As always, all comments received will be considered for inclusion in the final document.
- ORCA is an interest-group participation tool that offers a convenient on-line means of providing specific comments on a document on a line-by-line basis. Use of ORCA will help assure that all comments and suggestions specific to any portion of the text are accurately recorded in their intended context.



## Proposed Revision to the *Information Security Standard (ITRM SEC501-07)*

- To use ORCA, access the log-in page at <http://apps.vita.virginia.gov/publicORCA/>. Next, enter a self-determined user name and password by clicking the hyperlink labeled "Request a Password." For more detailed instructions, please click the hyperlink labeled "ORCA Help Page." If you have comments or questions of a more general nature not specific to the text, you may send them to Eric B. Perkins, Enterprise Architect, at [eric.perkins@vita.virginia.gov](mailto:eric.perkins@vita.virginia.gov).
- Please ensure that all appropriate management and technical staff in your agency associated with information technology are aware of, understand and have an opportunity to comment on this document. Your assistance is greatly appreciated..



# NEW SECURITY AWARENESS CONTRACT

- A statewide contract, that includes all public bodies, has been awarded to **Awareity for Managed Ongoing Awareness and Trust, (MOAT)**.
- MOAT provides a comprehensive platform of proven and award winning policy and procedure management and training tools.



## The MOAT platform provides tools for:

- Annual Security Awareness Training (SEC-501, ISO-27001, FERPA, HIPAA and PCI-DSS)
- Organizations to upload customized policies, procedures, organization specific training, etc.
- Role-based assignment of individual responsibilities
- All training and all policy acknowledgements to be tracked, time-stamped and documented
- Improving compliance with audits and examinations
- Ongoing reminders and notifications to staff and third-parties
- On-demand progress reporting and certifications



## Old VI Contract Expires Aug 31, 2012

- This new state contract provides an option for organizations who license MOAT through Virginia Interactive as well as all other Virginia entities to take advantage of MOAT's innovative offerings and benefits.
- Simply contact Awareity or review the link on the VITA website;  
[http://www.vita2.virginia.gov/procurement/contractDetail.cfm?contract\\_id=1000734](http://www.vita2.virginia.gov/procurement/contractDetail.cfm?contract_id=1000734) for more information



## SANS On Demand Training Reminder

- The MS-ISAC SANS Training purchasing Window is open until 07/31/2012.
- On Demand Classes are heavily discounted.
- Order link: <http://www.sans.org/ondemand/partnership/msisac>
- Classes must be activated within 1 year and completed 4 months after activation.
- For more information please contact:
  - [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



## Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - Aug 1, 2012

*Topic: FBI – Mobile Devices Overseas*

Wednesday - Sept 5, 2012

*Topic: RSA – Advanced Persistent Threat*

*ISOAG will be held the 1<sup>st</sup> Wednesday of each month in 2012*



# IS Orientation Sessions

Tuesday - Aug 7, 2012 1:00 – 3:30p  
(CESC)

Email [CommonwealthSecurity@VITA.virginia.gov](mailto:CommonwealthSecurity@VITA.virginia.gov) if you are interested in attending.

**IS Orientation also available via webinar!**



## COV IS Council

**IS Council accepting nominations for new members.**

**Send your nomination to:**

**[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)**



# MS-ISAC Announces BEST of the WEB Contest

## 4<sup>th</sup> Annual

### MS-ISAC BEST of the WEB Contest!

State & Local government's cyber security websites will be reviewed by MS-ISACs Education & Awareness Workgroup to be judged on content, usability, accessibility and appearance.

The criteria for the contest can be found at:

<http://msisac.cisecurity.org/resources/toolkit/2011-best-of-the-web-contest.cfm>

All state government cyber security websites are automatically entered. If a local government wishes to participate, email a link and contact info to: [contest@msisac.org](mailto:contest@msisac.org) by 7/31.



## Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# ISOAG-Partnership Update

*IT Infrastructure Partnership Team  
Bob Baskette*

July 11, 2012



**NORTHROP GRUMMAN**

# ADJOURN

