



# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

March 19, 2008



# St. Patrick's Day!

## 1<sup>st</sup> Day of Spring!



## March Winds!





# ISOAG March 2008 Agenda

- |       |   |   |
|-------|---|---|
| I.    | Welcome and Opening Remarks   | Peggy Ward, (VITA)  |
| II.   | CAM/APM Roles   | Debbie Secor, (VITA)  |
| III.  |   |   |
| V.    | FRAC/FIPS 501   | Mike McAllister, (OCP)  |
| VI.   | VEAP  | Peggy Feldmann, (GOV)   |
| III.  | Commonwealth IS Council Survey <ul style="list-style-type: none"><li>• Identity and Access Management</li><li>• Encryption</li><li>• Small Agency Outreach</li><li>• Executive Management</li></ul> | Michael McDaniel, (VRS)<br>John Willinger (DHMRSAS)<br>Steve Werby (VADOC)<br>Rob Jenkins (DJJ)<br>John Karabaic (DMAS) |
| V.    | VITA Compliance Management Tool   | Ed Miller, (VITA)   |
| VI.   | VITA IS Annual Report/Audit Language  | Cathie Brown, (VITA)  |
| VIII. | VITA Web App Hacking Demo   | Tripp Sims, (VITA)  |
| IX.   | 2008 Legislation Related to Security  | Peggy Ward, (VITA)  |
| X.    | Upcoming Events & Other Business  | Peggy Ward (VITA)   |



# CAM/APM Roles

**Debbie Secor**

---

ISOAG Meeting



# ISOAG Meeting

- Customer Account Management
- Agency Performance Management

Who are we and what do we do?



# Customer Account Managers

- Aligned by Secretariat
- Liaison with the customer at all levels
- Key customer advocate
- Serve as an escalation point
- Proactively work with customers to determine and qualify requests for service (strategic planning/forecasting)
- Monitor and align key communications to our customers
- Understand the customers' business



## Agency Performance Managers

- Serve as the conduit and oversight for the Request for Service process
- Proactively monitor, troubleshoot and resolve Agency procurement issues
- Manage the tactical and operational components of the IT Partnership
- Monitor and measure service delivery performance



## How do we interact with our customers?

- Customer Account Teams
- Cabinet Technology Team meetings
- Regular customer service meetings
- Strategic planning sessions
- Check in regularly with customers if no formal meetings are planned
- Communication, responsiveness and follow-through are KEY!!



# Customer Account Managers

Health and Human Resources	Anne Wingfield
Administration, Finance, Technology	Mary Davis-Barton
Public Safety and Agriculture/Forestry	Bobby Keener
Commerce and Trade and Education	Linda Smithson
Transportation	Zeta Wade
Natural Resources/VITA	Dee Piscicella
Governor's office, localities, out-of-scope customers	Hal Hughey



# Agency Performance Managers

Health and Human Resources	Ken Golaszewski
Administration, Finance, Technology	John Kissel
Public Safety and Agriculture/Forestry	Cathy Nott
Commerce and Trade and Education	Norm Hill
Transportation	Chris Brown
Natural Resources	Chris Brown
Technology (VITA)	John Kissel



# QUESTIONS?

# Information Security Officers Advisory Group

March 2008

Mike McAllister

Critical Infrastructure Protection Coordinator

Office of Commonwealth Preparedness



**The Governor's Office of  
Commonwealth Preparedness**

During incidents such as natural and man-made disasters, there is a need to expeditiously authenticate and validate the Emergency Response Community (public and private)

Need to have a standard credential for Emergency Response Officials (not associated with the REAL ID Act)

Credential needs to verify the identity and other pertinent information of Emergency Responders at incident scenes

Credential needs to allow access into and out of secured areas and across multi-jurisdictions

Need to identify a person's status within Sectors, Agency, or Emergency Support Function (ESF) which supports the National Response Framework (NRF)

H.R. 1 (9/11 Commission) Act – Requires Federal Government provide model standards and guidelines for credentialing critical infrastructure workers that may be used by a State to credential critical infrastructure workers that may respond to a natural disaster, act of terrorism, or other manmade disaster.

Need a standard process and requirements to obtain the credential (trust model)

Trust Model is established when all participants agree upon credentialing and eligibility rules and therefore trust credentials issued through a partner



Signed by President Bush in August, 2004

Mandatory for all Executive Branches of Government

Established a mandatory Federal Government-wide interoperable standard for secure and reliable forms of identification that:

- Can verify an individual's identity
- Are strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Are issued through an official accreditation process



# Federal Credentialing Standard: FIPS 201 (Federal Information Processing Standards)

Created by the National Institute of Standards and Technology  
(NIST)

Response to HSPD-12

Specifies the architecture, technical and administrative  
requirements

Defines requirements for:

- Identity proofing
- Registration
- Issuance of identification credentials



**The Governor's Office of  
Commonwealth Preparedness**

# Needed Standards

States, locals, and private sectors need to agree upon common credentialing standards for Emergency Response Community

In many high profile incidents, the lack of identity trust between jurisdictions resulted in the inability of Emergency Responders to reach incident scenes, and response and recovery activities were significantly delayed because incident scene commanders could not rapidly verify the person's identity



**The Governor's Office of  
Commonwealth Preparedness**

# Commonwealth FRAC Mission

To develop a FIPS 201 interoperable personal identification verification standard for Virginia Emergency Responders (federal, state, local, private and volunteer groups) that will be used to identify and categorize Emergency Responders, to support access processing for critical incident areas.



**The Governor's Office of  
Commonwealth Preparedness**

# First Responder Authentication Credential (FRAC)

The FRAC is a standards-based smart card that is issued to the Emergency Response Community in the NCR which will be recognized and accepted as a true representation of their identity and other pertinent data

The FRAC provides an interoperable identity credential platform for all Federal, State, local and private sector Emergency Responders

Facilitates quick identity verification

Supports NCR preparedness objectives

Supports EO 44 (culture of preparedness)

COOP/COG

Response and recovery efforts



**The Governor's Office of  
Commonwealth Preparedness**

# Commonwealth FRAC Partners

- Office of Commonwealth Preparedness
- Department of Homeland Security
- Virginia Department of Transportation
- Arlington County
- City of Alexandria
- Virginia State Police
- Virginia Department of Health
- Virginia Department of Fire Programs
- Virginia Department of Emergency Management
- Local Governments
- Private Sector Critical Infrastructure



**The Governor's Office of  
Commonwealth Preparedness**

# The Commonwealth's Progress

The Commonwealth has developed a FRAC Program using NCR UASI grant funding

Virginia is the first nationally

Issued over 2,300 FRACs to Arlington County and the City of Alexandria Emergency Response Community



**The Governor's Office of  
Commonwealth Preparedness**

# The Commonwealth of Virginia FRAC

**Arlington County**



Affiliation  
**Employee**  
Agency  
**Police Dept**  
Issued  
**2005DEC31**  
Expires  
**2008DEC31**

**LAST,  
FIRST, MI**



Employee ID  
**123456**

Rank or ESF  
**Lieutenant**



**Emergency Response Official**

This credential is the property of the Commonwealth of Virginia. The counterfeit, alteration, or misuse of this credential constitutes a violation of 18.2-204.2 of the Code of Virginia and section 499, Title 18 of the U.S. Code.

The bearer of this card is a designated Emergency Responder. After credential verification, bearer may be given access to controlled areas.



Return to: Lost Card Returns Commonwealth of Virginia FRAC  
Bay O 4262 Entre Court Chantilly, VA 20151

**000000006010** **00050150025**



The Governor's Office of  
Commonwealth Preparedness

## The Commonwealth FRAC is designed to:

- Securely establish emergency responders' identities at the scene of an incident.
- Confirm first responders' qualifications and expertise, allowing incident commanders to dispatch them quickly and appropriately.
- Enhance cooperation and efficiency between federal, state and local first responders.
  - Nationally
  - Regionally
  - Locally



**The Governor's Office of  
Commonwealth Preparedness**



# Next Steps

The Commonwealth has organized a Hampton Roads Regional Credentialing Working Group

Continue to educate State and local officials on the FRAC program and it's interoperability with partners

Continue to work with state agencies to implement FIPS 201 compliant FRAC programs

Continue to support state and local agencies adoption of FIPS 201 compliant credentials for employee identification and physical access control



**The Governor's Office of  
Commonwealth Preparedness**

# State and Local Efforts

The following are voluntarily choosing to adopt the HSPD 12 and FIPS 201 standards, following Virginia's lead, thereby achieving multi-jurisdictional interoperability between the Emergency Response Community, all levels of government, and the private sector:

**Maryland** has developed a standard FRAC for Emergency Responders which is interoperable with Virginia's FRAC

**Illinois** is currently developing a FRAC program

**Pennsylvania** is in the early stages of developing a FRAC program

The **San Antonio, Texas** region is beginning the first steps toward full FIPS 201 compliance for their next generation unified ID badge for all Fire/EMS personnel and physicians

**Denver, Colorado** is developing a FIPS 201 compliant credential and wants to implement statewide



**The Governor's Office of  
Commonwealth Preparedness**

# National Efforts

The National Fire Academy released a report recommending a FIPS 201 compliant National Fire Service Responder Credentialing System

National Incident Management System is developing a consensus on job requirements within each Emergency Support Function.

Transportation Worker Identification Card (TWIC) now follows FIPS 201 standards

DHS anticipates rolling out the FRAC program first in FEMA Region 3 and then the entire East Coast

Pentagon Force Protection Agency (PFPA) has identified the FRAC as it's preferred identification for response to the Pentagon and other leased DOD facilities within the NCR



**The Governor's Office of  
Commonwealth Preparedness**



# VEAP

## Virginia Enterprise Applications Program

*Visibility – Efficiency – Accountability – Progress*

# ISOAG Meeting

Peggy Feldmann  
[Peggy.Feldmann@VEAP.Virginia.com](mailto:Peggy.Feldmann@VEAP.Virginia.com)

# Agenda

---

- Present
  - History
  - Current Projects
  - IT Governance Issue



**VEAP**

Virginia Enterprise Applications Program

# VEAP History

Mar '07

Sep '07

Dec '07

Feb '08

**Financial Mgmt ERP**

**Financial Mgmt ERP  
Performance Budgeting  
Business Intelligence**

**Governor's Budget  
APA Report**

**Financial Mgmt  
Performance Budgeting  
Business Intelligence  
Document Management  
Mainframe Modernization Efforts  
Citizen Facing Portals  
Customer Relations Management  
HR Initiatives  
Electronic signature  
Licensing initiatives  
IT governance plans**

# Performance Budgeting

---

- Separated from Financial Management
  - Speed to Production
  - Focus on Budget requirements / market offerings
- Phased Development
  - Initial focus on central agency needs
  - All executive agencies in a later phase
- Planning currently underway
  - Requirements complete
  - Request for Proposals is out

# Business Intelligence (BI)

---

- Separated from Financial Management
  - Speed to Production
  - Capability lacking or disparate throughout the agencies
    - Currently 9 different tools
- Enterprise Umbrella
  - Procure an executive agency standard BI tool
  - Staff a Center of Excellence to support and consolidate agency requirements for BI
    - Provide services for small agencies
    - Provide consultation/collaboration services for large agencies
- Software - Spring 2008

# Financial Management

---

- Financial Management ERP RFP is officially delayed
  - “On hold, 30 days notice will be provided before posting”
- Analysis of Alternatives
  - Single state-wide system (complexity of VDOT requirements)
  - Number of agencies deployed within a phase
  - “As is” migration to existing ERPs
  - Technology upgrade of central financial system (CARS)
- Currently evaluating alternatives and strategies

# Document Management

---

- Software contract awarded in Summer 2007
- Integration Services contracts awarded in November 2007
- Shared Services (SS) study completed December 2007
  - Currently 22 small agencies in need of capability
  - Library of Virginia would be functional manager
  - Leverage TAX's world class scanning capability
  - Would be focused at small agencies, but would provide large agencies with "outsourced" capabilities (like scanning)
- Coordinating with DEQ on large ECM implementation



VEAP

Virginia Enterprise Applications Program

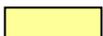
# BACKGROUND

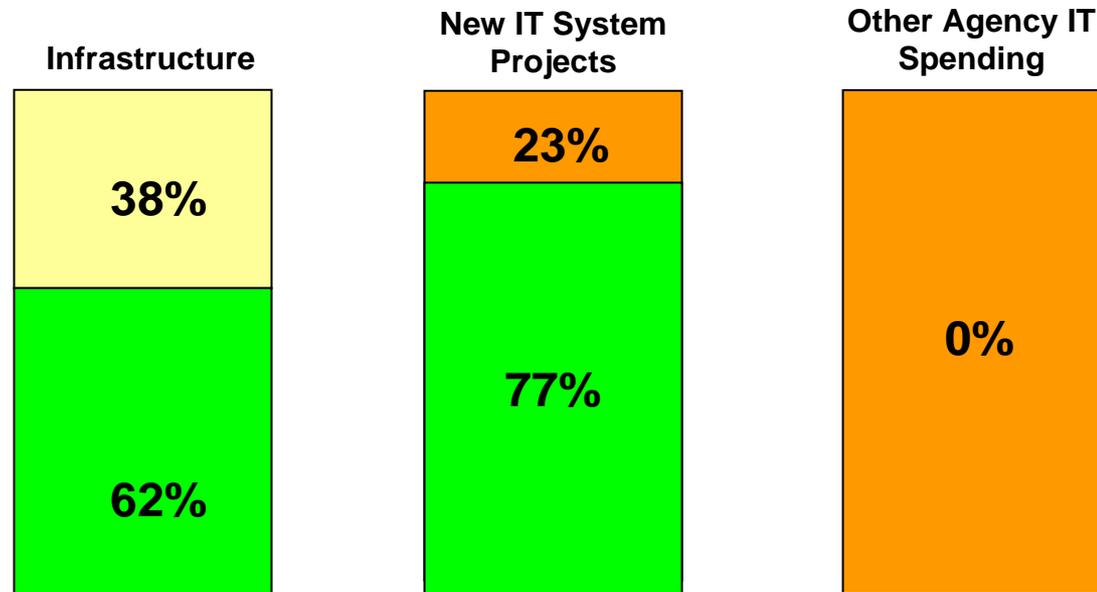
- 
- APA IT Governance report asked “Who has control?”
    - VITA - - infrastructure
    - CIO & ITIB - - new systems development
    - Agencies - - maintenance and operations of legacy
  - APA report revealed problem areas:
    - CIO’s responsibilities broader than just VITA, e.g.
      - Project Management oversight
      - Standard setting
      - Budget resource recommendations
    - Agencies
      - Do not understand the Commonwealth’s Business Model
      - Plan for maintenance differently and at varying levels
      - Not working jointly to implement an enterprise system
      - Try to avoid IT governance by using M&O budgets
    - The lack of data standards is resulting in disparate systems
    - New system development projects lack a sound return on investment



# APA ASSESSMENT OF IT GOVERNANCE "AS IS"

Virginia Enterprise Applications Program

Key: Best Practice...  
 exists  
 evolving  
 does not exist  
at the enterprise level



- **Infrastructure Services:** "IT governance over the infrastructure is transforming"
- **New Projects:** "IT governance over new systems development projects is maturing"
- **Maintenance and Operations:** "IT governance over agency maintenance and operations is non-existent"



VEAP

Virginia Enterprise Applications Program

# PROBLEM

---

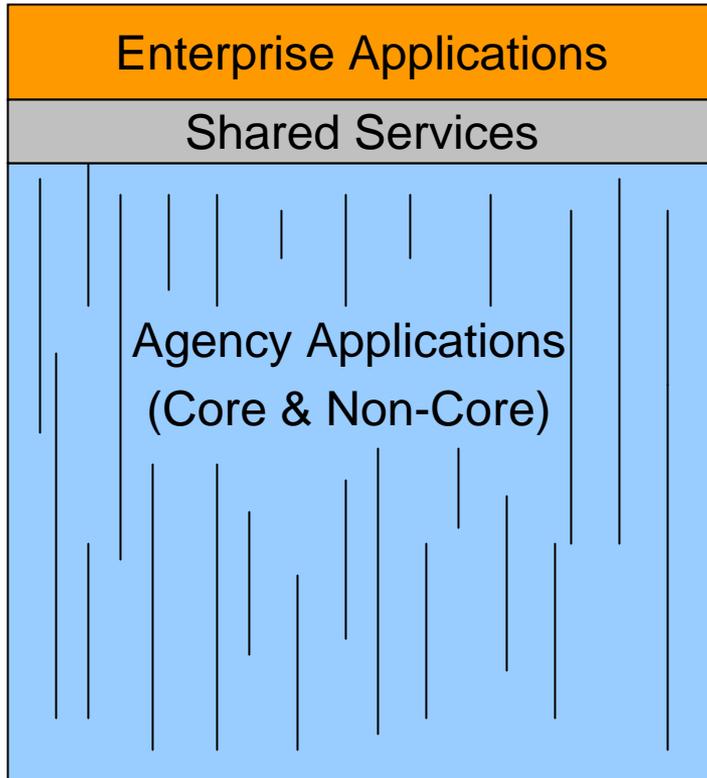
The Commonwealth lacks of an effective enterprise governance and investment management program over total IT spend.

Knowing this, how do we ensure that all Commonwealth IT investments-- new projects, infrastructure services, and operations/maintenance:

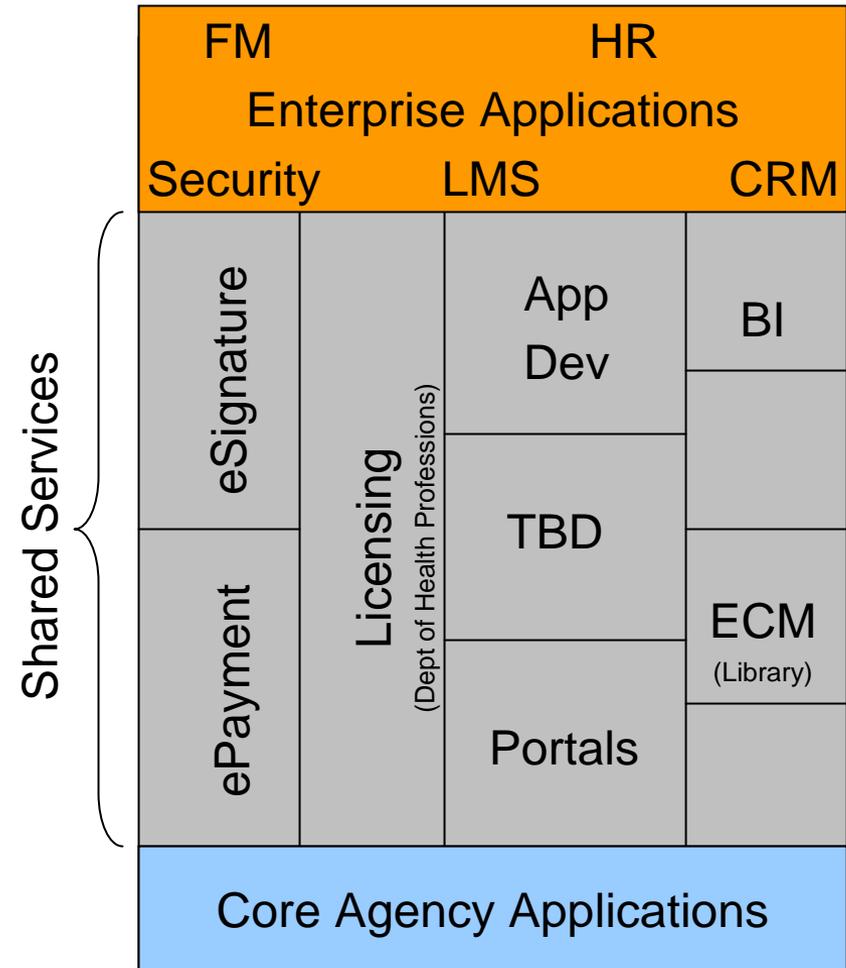
- Meet our strategic business objectives in a cost- effective manner;
- Are in line with other business investments and contribute to improved portfolio management;
- Are effectively managed to deliver the intended business results;
- Provide the business value we expect;
- And ensure progress is real and visible?

# Application Architecture

## “As-Is”



## “To-Be”





VEAP

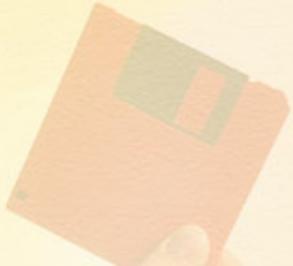
Virginia Enterprise Applications Program

# Future Vision

---

- Comprehensive IT Governance Model
  - Aligned to business strategy
  - Encompassing the entire portfolio
- Portfolio of on-demand and hosted solutions
- Data-centric environment where information is recognized as an asset
- Shared Service Centers delivering business capability
- Centers of Excellence delivering focused support
- Virginia Government acting as a single, unified enterprise when its in their best interest

# COV Information Security Council Survey 2008



# COV Information Security Council Survey 2008

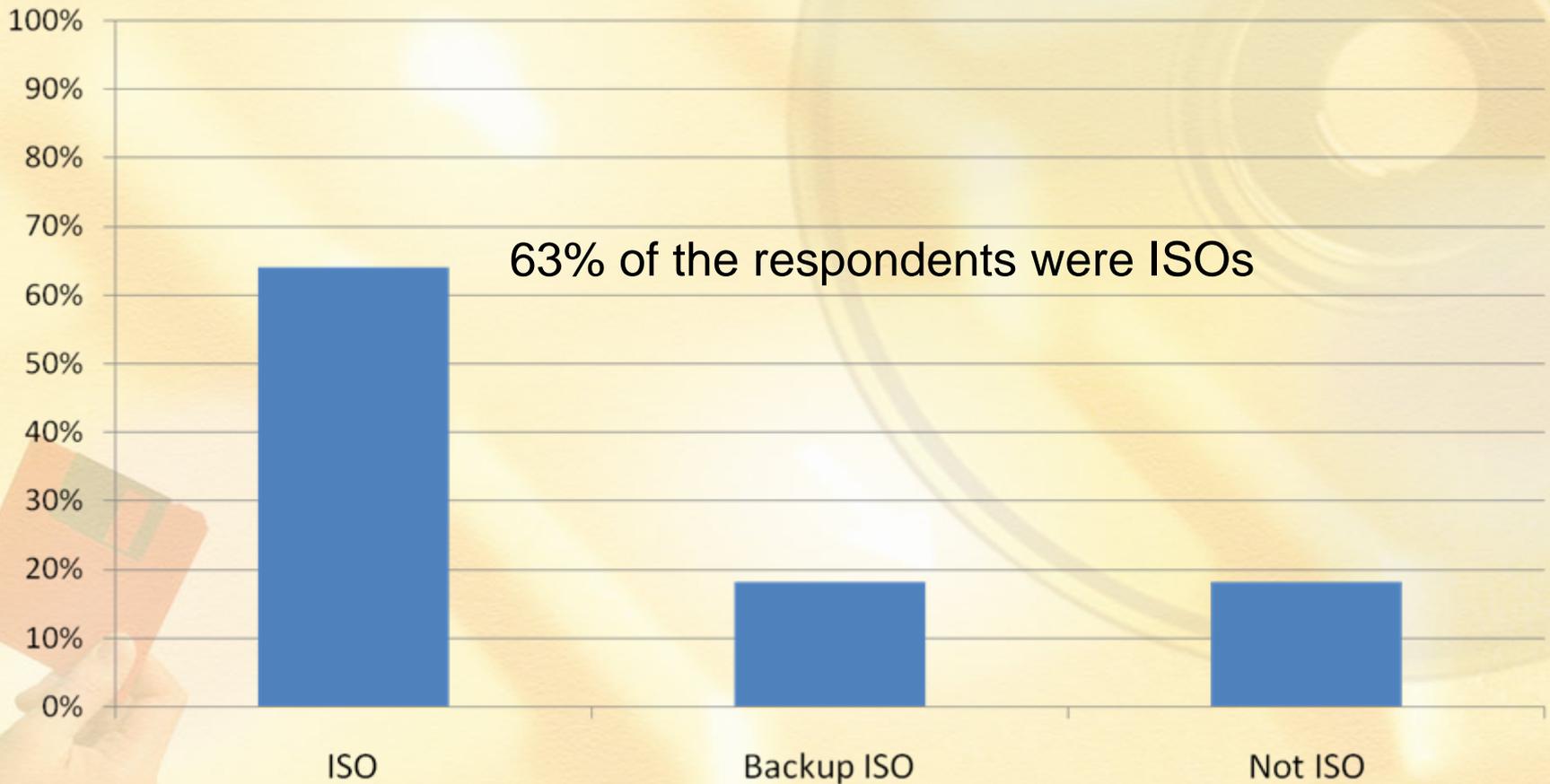
## Security Council Committee Surveys

- Encryption
- Making Information Security an Executive Management Priority
- Identity and Access Management
- Small Agency

# COV Information Security Council Survey 2008

- Survey sent to all ISO's, their backups, and AITRs
- 72 respondents
- Large and small agencies were represented

# COV Information Security Council Survey 2008



2/3 of the ISO's considered themselves to be knowledgeable or an expert in the security field

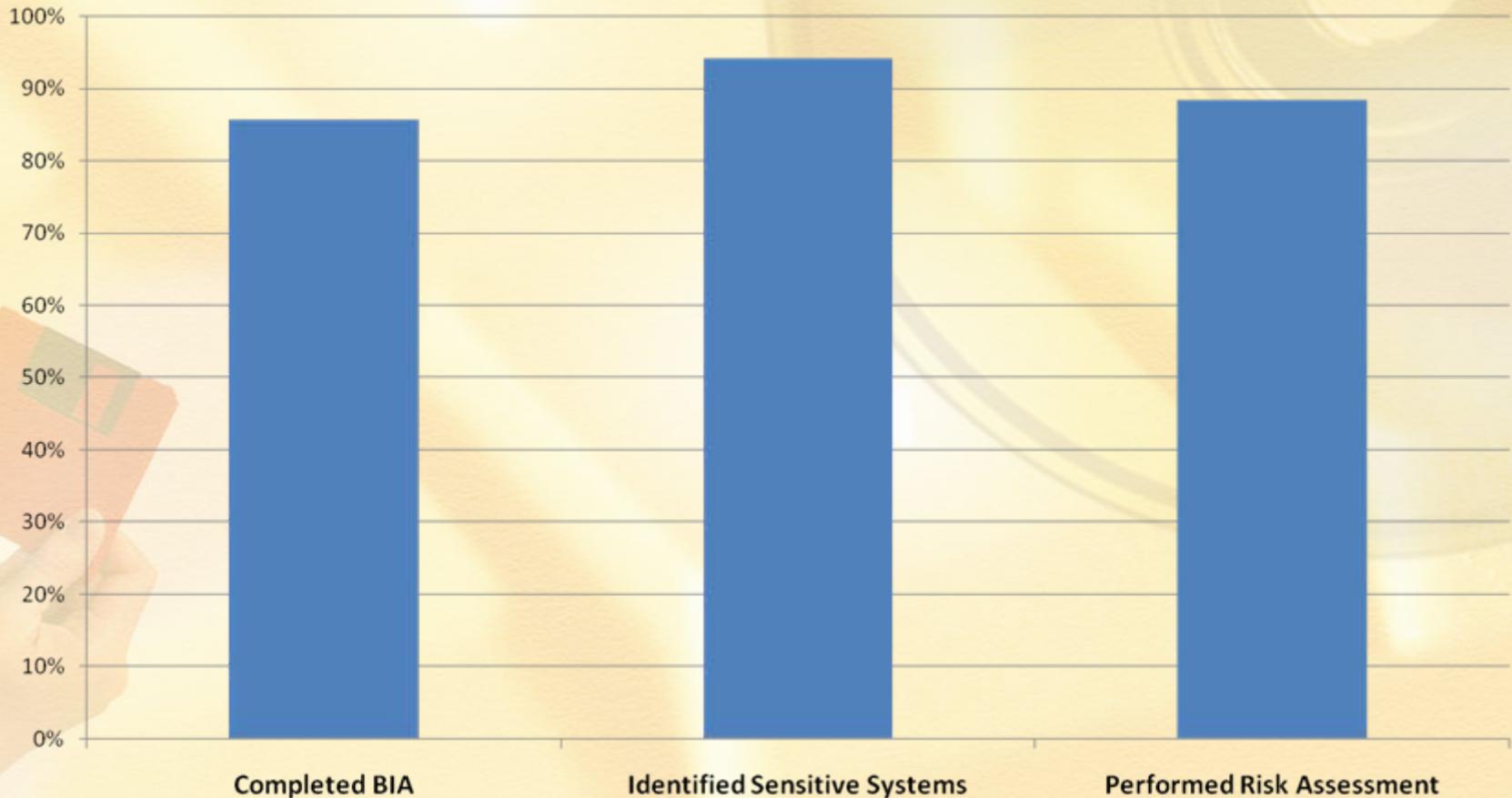
# COV Information Security Council Survey 2008

## 53 individual agencies represented

- APA
- Arlington County Gov.
- Board of Medicine
- CIT
- DBA
- DCJS
- DCR
- DEQ
- DFS
- DGIF
- DHP
- DHR
- DHRM
- DJJ
- DMA
- DMAS
- DMBE
- DMHMRSAS
- DMME
- DOC
- DOE
- DOF
- DOLI
- DPOR
- DRS
- DSS
- EDR
- George Mason University
- John Tyler Community College
- Library of Virginia
- Longwood University
- Marine Resources Commission
- MRC
- NSU
- OAG
- Old Dominion University
- Richard Bland College
- SBE
- SCC
- Lottery Department
- Supreme Court
- TAXATION
- Treasury
- VCU
- VDA
- VDACS
- VDEM
- VEC
- Virginia Museum of Natural History
- VITA
- VRC
- VRS

# COV Information Security Council Survey 2008

Most agencies have completed a BIA, Identified their Sensitive Systems, and Performed a Risk Assessment



# COV Information Security Council Survey 2008

## • High level topics of requested information security training:

- COV Security Policy & Standards training and compliance (including non-technical training)
- Cyber Security
- Encryption – implementation & policy
- Security training & awareness (Including Certifications)
- Use Online training methods
- Target end users (including faculty)
- Risk Assessments
- Contingency planning
- Facility security
- VITA/NG/Agency Roles
- Information sharing
- Incident handling
- Regulatory Compliance (e.g. HIPAA)
- Record retention

# IAM

## Identity and Access Management And Account Management Survey Results

# IAM Committee Members

## Co-Chairs:

Mike Garner – TAX, [mike.garner@tax.virginia.gov](mailto:mike.garner@tax.virginia.gov)

Marie Greenberg – SCC, [marie.greenberg@scc.virginia.gov](mailto:marie.greenberg@scc.virginia.gov)

John Willinger – DMHMRSAS,  
[John.Willinger@co.dmhmrsas.virginia.gov](mailto:John.Willinger@co.dmhmrsas.virginia.gov)

## Members:

Jim Austin, VDOT, [james.austin@vdot.virginia.gov](mailto:james.austin@vdot.virginia.gov)

Maria Batista, DMV, [maria.batista@dmv.virginia.gov](mailto:maria.batista@dmv.virginia.gov)

David Hines, SCV, [dhines@courts.states.va.us](mailto:dhines@courts.states.va.us)

Joel McPherson, DSS, [joel.mcpherson@dss.virginia.gov](mailto:joel.mcpherson@dss.virginia.gov)

Chris Nicholl, VEC, [christopher.nicholl@vec.virginia.gov](mailto:christopher.nicholl@vec.virginia.gov)

Easton Rhodd, VITA, [easton.rhodd@vita.virginia.gov](mailto:easton.rhodd@vita.virginia.gov)

**Is there a documented process in place at your agency to establish/change/terminate user accounts?**

**85% of respondents said they had a documented process in place**

**Some said that procedures exist, but there was no policy.**

Is the process for creating/changing/  
terminating user account automated or  
manual?

60 % said they use manual methods.

10 % have an automated process

30 % use a combination

Many used automated features such as  
setting expiration dates on accounts  
and having accounts disabled due to  
inactivity.

# How long does it take on average to establish access for new users?

62% said new accounts were processed in 1 day or less.

37% said going through the VCCC takes 2-5 days

When users change positions or roles, is system access modified to match the new role?

94% said yes, but comments were that:

It is not an automated process and needs to be better enforced

Roles are not clearly defined

MIS is not always notified by management

Changes are not always communicated

# How long does it take to disable or remove inactive and terminated accounts?

23 % said 2-5 days

71 % said 1 day

However, accounts have been discovered weeks and even months after an employee has left.

# How many user accounts are issued to the average user?

50 % said 2-3 accounts per user

43% said 1 account per user

7% said 4 or more accounts per user

Many said the average user only has a single Windows account.

Has your agency documented the various job functions (roles) within the agency?

56 % said yes

44 % said no

Access is typically determined by another user with a similar job

# Do you periodically review accounts and access?

44 % said periodic reviews are performed but there is no documented process.

38 % said they perform periodic reviews and have a documented process

18 % said they do not perform periodic reviews

Is there any type of “single sign on” technology in use at your agency?

28 % said yes

72 % said no

Some used AD login for email and application access using the partnership network.

Several commented that they would like to have SSO implemented.

Some said due to not having control, they do not want SSO.

Does your agency have any automated identity management tools such as “smart cards” in place?

7 % said yes

93% said no

Some use access cards for physical access to the building

Some said they are interested in using the technology and would like to have something.

# Are there any current or planned projects that will utilize IAM technologies?

29% said yes

71 % said no

Some said the need exists for web customers but not agency users

Lack of funding

Transformation

# Can you audit and report on account activity and access?

71 % said yes

29 % said no.

Limited storage capacity for logs

VITA/NG does this

# Next steps

Create requirements list for COV Agencies based on survey responses

Meet with VEAP to discuss Enterprise solutions

Review available solutions from the Partnership

Provide recommendations based on good practices to the CISO

# InfoSec Council Survey

## Encryption Committee

### Co-Chairs:

Michael McDaniel, VRS

John Palese, DSS

Steve Werby, DOC

### Members:

Cameron Caffee, VDOT

Jesse Crim, VCU

Craig Goeller, DMAS

Tripp Sims, VITA

# InfoSec Council Survey - Encryption

## Goals:

- Determine agencies' needs and implemented solutions

## Conclusions:

- Large percentage of device storing sensitive data unencrypted
- Sensitive data transmitted via Internet with wide variety of recipients
- Most respondents have not implemented an email encryption solution
- Wide variety of solutions implemented; some inadequate
- User training is an area of concern
- Agencies feel they need help to determine encryption needs and implement solutions

# InfoSec Council Survey - Encryption

A measurement of adverse affect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled that comprise of IT systems and data with respect to confidentiality, integrity, and/or availability could cause. IT systems and data are sensitive in direct proportion to the materiality of the adverse effect caused by their compromise.

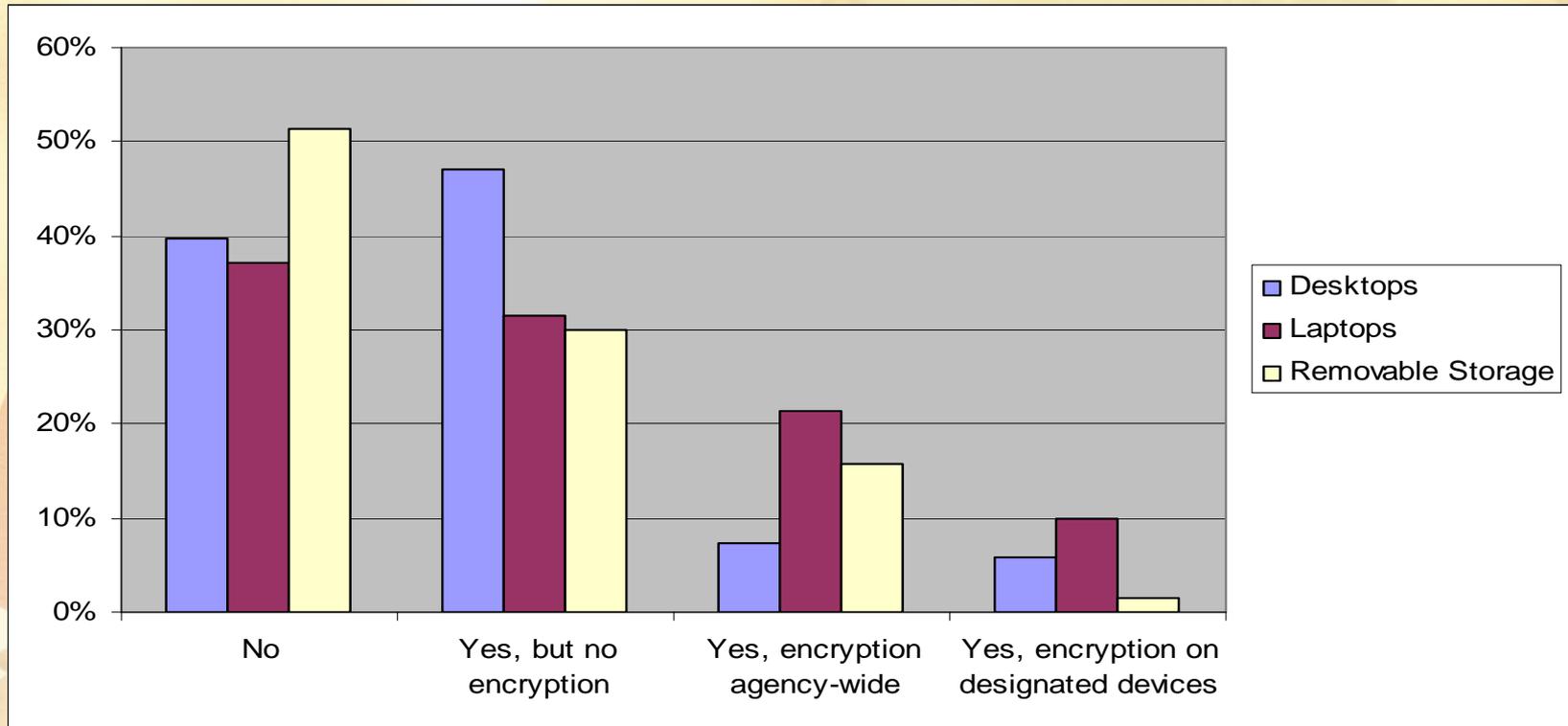
## Sensitivity

### Examples of sensitive data:

- PII (name and SSN/DL/DOB/CC #/etc.)
- Federally protected data (HIPAA, FERPA)
- Proprietary data
- Agency restricted data
- Passwords
- Network diagrams, server names, IP addresses, usernames

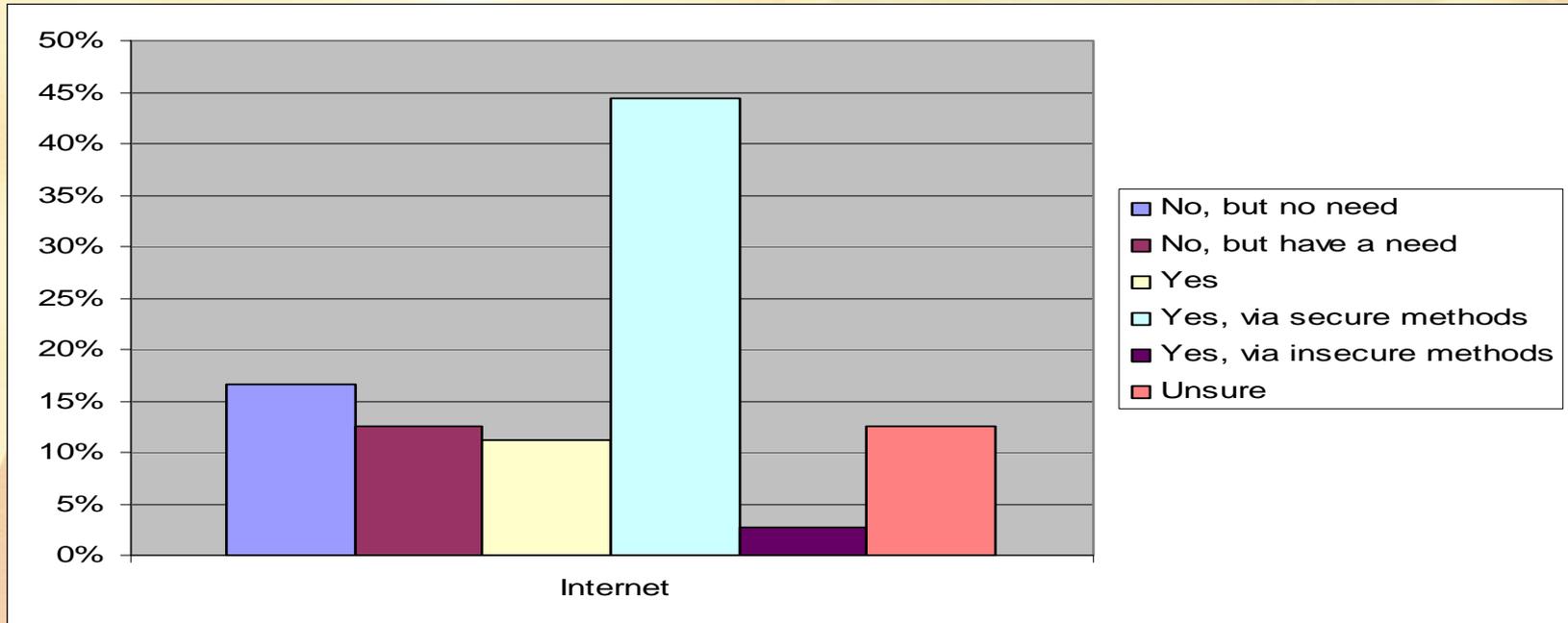
# InfoSec Council Survey - Encryption

Do employees store sensitive or confidential data on workstations or removable storage?



# InfoSec Council Survey - Encryption

Do employees transmit sensitive data via the Internet?



With whom?

State agencies, in-scope – 36%

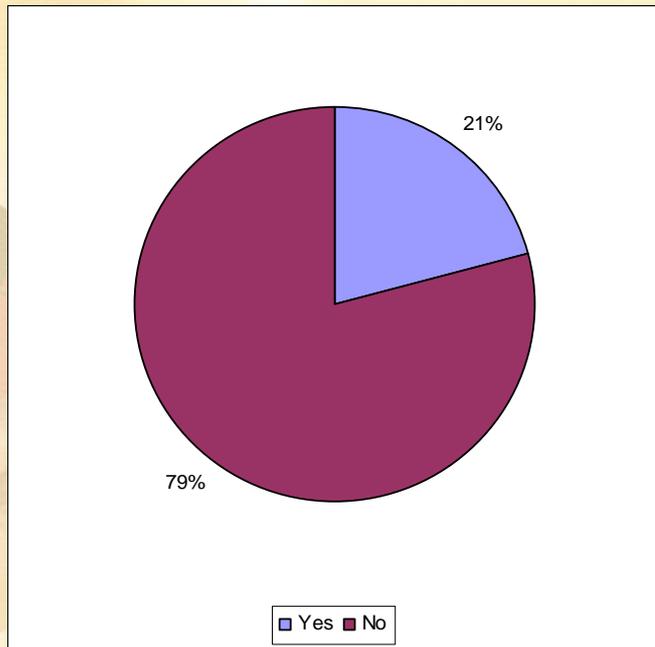
State agencies, out of scope – 23%

Other agencies – 28%

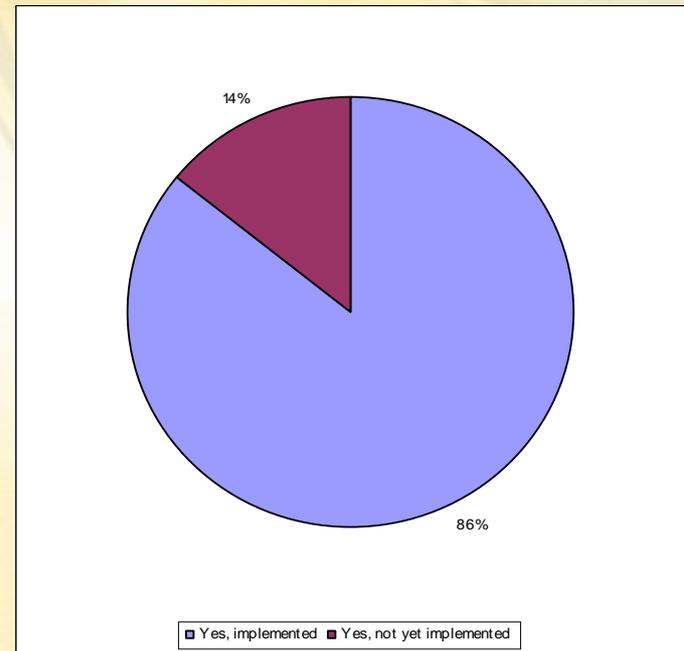
Citizens – 13%

# InfoSec Council Survey - Encryption

Have you implemented an email encryption solution?

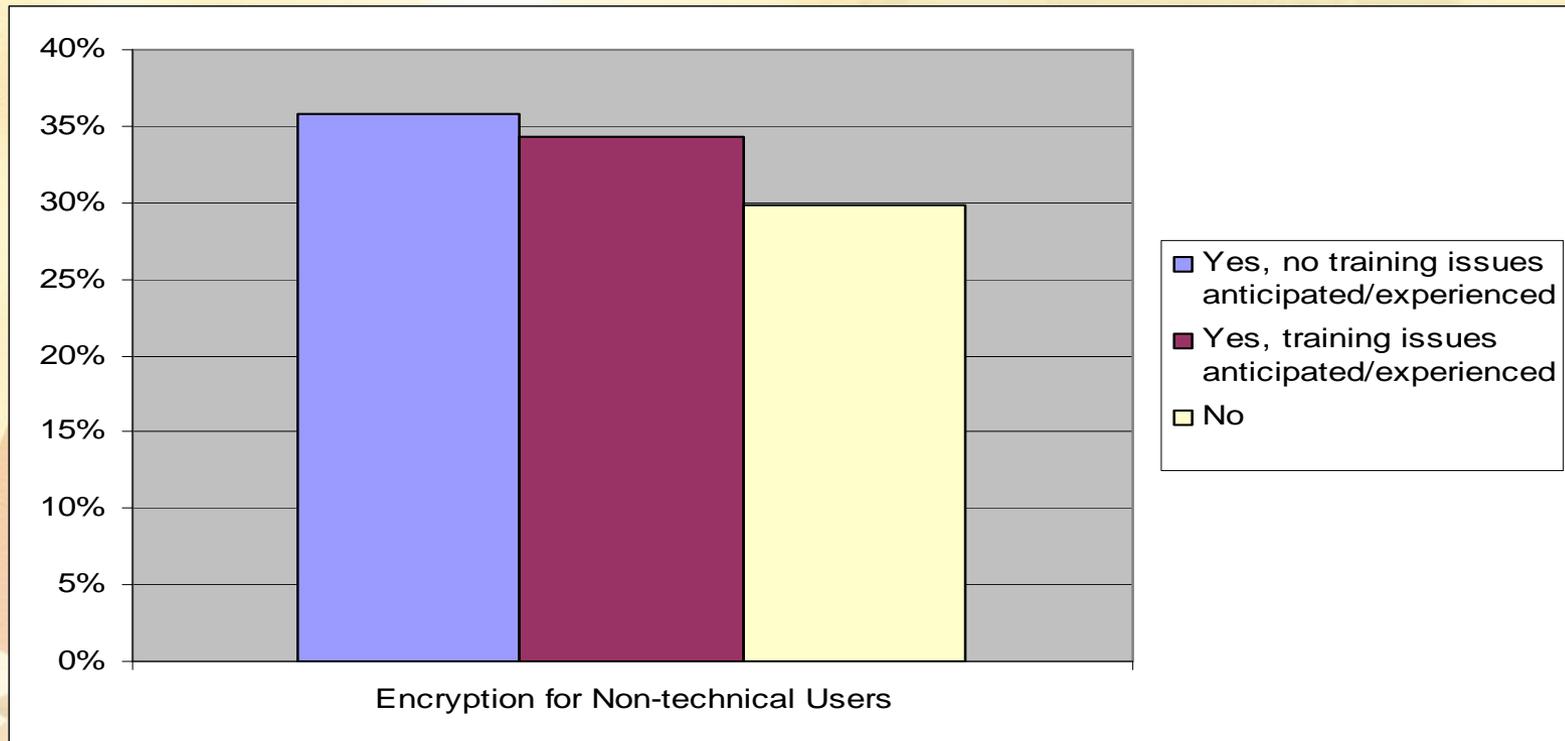


Is inbound remote access needed for employees and business partners?



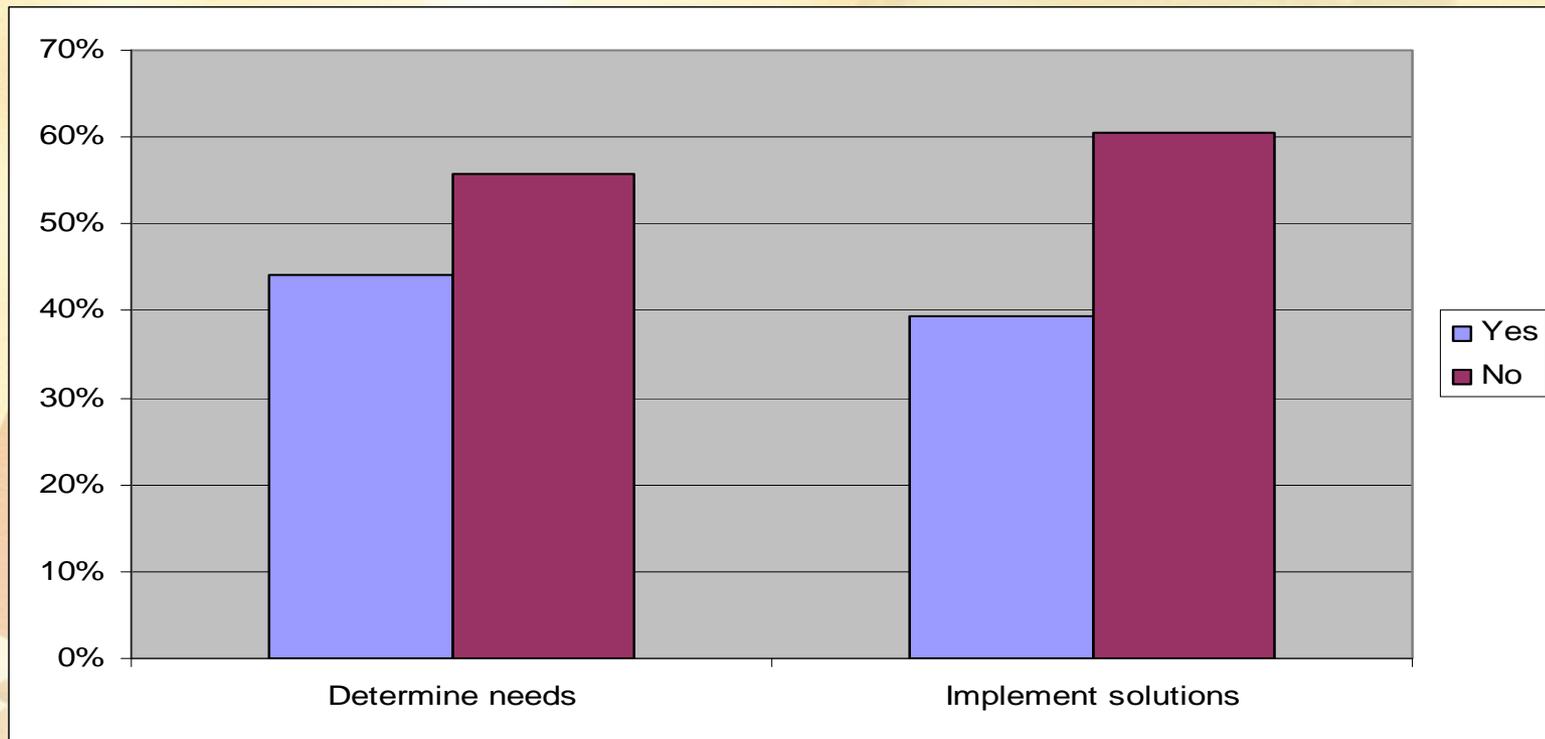
# InfoSec Council Survey - Encryption

Will encryption be used by non-technical users and are training issues expected?



# InfoSec Council Survey - Encryption

Do you have adequate staff to determine encryption needs and to implement related solutions?



# InfoSec Council Survey - Encryption

A sampling of comments from the survey:

Do employees transmit sensitive data via the Internet?

- We have policies against doing so but we know that it happens anyway.
- No good way of knowing but I have to assume they do.
- Don't know.

Will encryption be used by non-technical users and are training issues expected?

- Many of our users do not have strong computer skills.
- Given the option, users find such software too troublesome and avoid using it as it slows down system.

# InfoSec Council Survey - Encryption

What are the committee's next steps?

1. Develop best practices
2. Develop plan for educating users and ISOs
3. Recommend feature sets for enterprise solutions



Considering from a broad COV perspective



# **Small Agency Security State of the Union – 1<sup>st</sup> Cut**

Small Agency Outreach  
Sub-Committee

March 2008



# Small Agency Outreach Committee

## Co-Chairs

Goran Gustavsson, APA

Rob Jenkins, DJJ

Aaron Mathes, OAG

## Members

Bob Auton, DSS

Don Gray, VDEM

Ross McDonald, DSS

Ron Necessary, DOA

Jack Spooner, DOA

# Executive Branch Small Agencies

- Secretariat of Administration
  - DHRM (97 MEL) \*
  - State Board of Elections (38 MEL) \*
  - Dept. of Minority Business Enterprise (29 MEL) \*
  - Compensation Board (26 MEL)
  - Dept. of Employment Dispute Resolution (18 MEL) \*
  - Human Rights Council (6 MEL)
    - **214 Small Agency MEL**

# Executive Branch Small Agencies

- Secretariat of Commerce & Trade
  - Dept. of Business Assistance (50 MEL) \*
  - Virginia Racing Commission (10 MEL) \*
  - Virginia Board of Accountancy (8 MEL) \*
    - **68 Small Agency MEL**
- Secretariat of Education
  - The Science Museum of Virginia (102 MEL)
  - Frontier Culture Museum of VA (40.5 MEL)
  - Gunston Hall (11 MEL)
  - VA Commission for the Arts (5 MEL)
    - **158.5 Small Agency MEL**

# Executive Branch Small Agencies

- Office of the Governor
  - Governor's Office (41 MEL)
  - Sec. of Administration (12 MEL)
  - Sec. of Commerce and Trade (8 MEL)
  - Sec. of Public Safety (7 MEL)
  - Sec. of Education (6 MEL)
  - Sec. of Health and Human Resources (6 MEL)
  - Sec. of Transportation (6 MEL)
  - Sec. of Natural Resources (5 MEL)
  - Sec. of Finance (5 MEL)
  - Sec. of Technology (5 MEL)
  - VA Enterprise Application Program Office (3 MEL)
    - **104 Small Agency MEL**

# Executive Branch Small Agencies

- Secretariat of Finance
  - Dept. of Planning and Budget (70 MEL)
- Secretariat of Technology
  - Center for Innovative Technology (35 MEL) \*
- Secretariat of Health & Human Resources
  - Dept. for the Aging (27 MEL) \*
  - VA Rehab Center for the Blind & Vision Impaired (26 MEL)
    - Dept. for the Deaf and Hard-of-Hearing (14 MEL)
    - VA Board for People with Disabilities (10 MEL)
    - **77 Small Agency MEL**

# Executive Branch Small Agencies

- Secretariat of Natural Resources
  - Virginia Museum of Natural History (52.5 MEL) \*
  - Dept. of Historic Resources (52 MEL) \*
    - **104.5 Small Agency MEL**
- Secretariat of Public Safety
  - Dept. of Fire Programs (37 MEL)
  - Commonwealth's Attorneys' Service Council (7 MEL)
    - **44 Small Agency MEL**

# Executive Branch Small Agencies

- Secretariat of Transportation
  - Dept. of Rail & Public Transportation (55 MEL)
  - Dept. of Aviation (33 MEL)
  - Motor Vehicle Dealer Board (22 MEL)
    - **110 Small Agency MEL**
- **Small Agency Totals**
  - 25 Small Agencies (100 MEL or Less)
  - 985 Total Small Agency MEL
  - Small Agencies (985 MEL) > DEQ (957 MEL)

# Executive Branch Small Agency – State of the Union

- Of the 11 agencies that responded to the survey (44%), the results were encouraging
- Strong awareness of security needs
- Implementation of many key security practices
- 87% did not have an internal auditor

# Executive Branch Small Agency – State of the Union

- Networked computers:
  - 20% <10
  - 7% 10 to 20
  - 40% 21 to 50
  - 33% >50
- Need areas:
  - Awareness Program,
  - Classification of data and systems,
  - Performing risk assessment
  - Security policy templates.

# Executive Branch Small Agency – State of the Union

- Audit resources used:
  - 29% Internal Resources
  - 14% Consultants
  - 14% Partnership
  - 21% APA
  - 21% internal Audit
- 93% were interested in a shared services program

# Executive Branch Small Agency – Potential Options

- Train Internal Resources
- Consulting – SMSA, CAI
- ISO at the Secretariat Level
- Informal Shared Service Center Network
- Creation of positions to meet security needs of small agencies



# **Security Awareness Executive Priority**

---

Making Information Security an  
Executive Management Priority

*Survey Results*



# Committee Members

---

**Joe Hubbell** Virginia Lottery,  
[jHubbell@vaLottery.com](mailto:jHubbell@vaLottery.com)

**John Karabaic, Co-Chair**, Department of Medical Assistance Services,  
[john.karabaic@dmas.virginia.gov](mailto:john.karabaic@dmas.virginia.gov)

**Judy Napier**, Secretary of Technology Office,  
[judy.napier@governor.virginia.gov](mailto:judy.napier@governor.virginia.gov)

**Shirley Payne**, Co-Chair, University of Virginia.  
[payne@virginia.edu](mailto:payne@virginia.edu)

# Is there a documented security awareness program?

---

Yes: 78%

No: 22%

# Is the program based upon an assessment of need?

---

Yes: 64%

No: 36%



# Is the program aligned with the business?

---

Yes: 73%

No: 27%



# Are all employees required to complete general security awareness training?

---

Yes: 83%

No: 17%

# Are supervisors, managers, and executives required to complete general security awareness training?

---

Yes: 44%

No: 56%



## Does the security awareness program also target non-staff, e.g. contractors?

---

Yes: 61%

No: 39%



# Does the organization have a security awareness coordinator or manager?

---

Yes: 57%

No: 43%

# Are lessons learned from security incidents incorporated into the security awareness program?

---

Yes: 60%

No: 40%

# Would security awareness tools be useful to your agency?

---

Need: 27%

Somewhat Needed: 60%

Not Needed: 13%



## Next steps

---

- Working to ensure IT security is well covered in executive and management training programs, e.g. CMI, VEI, and DHRM
- Writing monthly security articles for inclusion in Leadership Communiqués
- Developing “canned” security awareness presentation aimed at executive audience



# Compliance Management Tools

**Ed Miller**  
Information Security Assurance Manager

---

ISOAG Meeting



# Compliance Management Tools

- **Purpose**

- To fulfill our responsibilities for providing a secure infrastructure commensurate with system sensitivity and risk and allow us to provide assurance of this to our customer agencies.

- **Function**

- Identify the security requirements of systems that are considered sensitive, high risk or that process data with specific security needs.
- Evaluate the security controls in place for the infrastructure where the sensitive system resides.
- Identify gaps in the security requirements and controls to determine whether corrective action is appropriate or acceptance of risk is necessary.



# Compliance Management Tools

- In order to meet the goals and objectives set out for VITA's Commonwealth Security & Risk Management Directorate (CS & RM), the need exists to collect information from Customer Agencies about "sensitive" IT systems and existing security controls. CS & RM distributed a Security Template in Excel for agencies to use to provide this information back in March 2006. The intent was to aggregate this information in a format that would allow us to evaluate the systems and controls against policy and recommended best practices.



# Compliance Management Tools

- To facilitate the collection of this information and its evaluation, we have been developing a number of software tools. The first “tool” we have developed is a web-based form that will be used by agency ISO’s to update the information collected in March 2006 and add new information as needed. Users (ISO’s) will need a secure Login ID and password.
- This particular tool should be ready on a test basis in April and available for other users in May.
- The next tool to be developed will require IT Partnership engineers and staff to evaluate the controls in place for the device and infrastructure where the sensitive system resides so that gaps can be identified and remediated.



- Home
- Resource Directory
- System Profiles
- Change Agency
- Administration
- Reports

## Compliance Management Tool

Home Page

**Current Agency:**  
Virginia Information Technologies Agency

# Commonwealth Security & Risk Management



### System Profiles

Entity used by agencies to document the security requirements of sensitive systems.

- Home
- Resource Directory
- System Profiles
- Change Agency Administration
- Reports
- System Profile
- Example
- Information/Screening
- Information
- Resources
- User Interface
- Instructions
- Administration
- IT Strategy Planning
- Change Management
- Support

## Compliance Management Tool

### System Profile

**System Name:** ISOAG Example

**Mode:** Read/Write

*Current Agency:*

Virginia Information Technologies Agency

System Name: ISOAG Example

Describe the system function or purpose: Example system for IS Council, ISOAG, and Screenshots

Device Name that stores the systems data: Device #1

Who hosts this device? VITA

Physical Street Address of the Device Listed Above

Address 1: 11751 Meadowville Lane

Address 2:

City: Chester

State: VA

Zip: 23836

Select how the system was developed: CUSTOM DEVELOPED IN-HOUSE STAFF

Platform: WINDOWS SERVER

If other, please specify:

Database: ORACLE

Version: 10g

Next

The **System Profile** screen asks you to identify basic profile information about the sensitive system: Name of system, description of system, location, platform, etc.

## Compliance Management Tool

### System Profile

System Name: ISOAG Example

Current Agency:

Mode: Read/Write

Virginia Information Technologies Agency

#### System Profile

##### People

Training/Screening

Risk Information

Metrics

Interface

Additional resources that support the sensitive system application may include: System Owners, System Administrators, Data Owners, and Data Custodians. There will be a Primary and Secondary person for each title.

#### Support People:

View/Edit	Remove	Name	Support Type	Office Phone	Title
		Joe Snuffy	DATA OWNER - PRIMARY	1115551212	Security Manager

#### Supporting Person

Support Type:

First Name:

Middle Initial:

Last Name:

Title:

 Office Phone:  
 (###) ###-####

Email:

 -- Select One --  
 -- Select One --  
 DATA CUSTODIAN - BACKUP  
 DATA CUSTODIAN - PRIMARY  
 DATA OWNER - BACKUP  
 SYSTEM ADMINISTRATOR - BACKUP  
 SYSTEM ADMINISTRATOR - PRIMARY  
 SYSTEM OWNER - BACKUP  
 SYSTEM OWNER - PRIMARY

Save

Clear

Previous

Next

**People:** This screen is used to identify the responsible people as they relate to this particular sensitive system. ITRM SEC502-00 describes four major roles:

- **Data Custodian:** Individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for: protecting data from unauthorized access, alteration, destruction or usage.
- **System Administrator:** An analyst, engineer or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner and/or Data Custodian.
- **System Owner:** The agency manager responsible for operation and maintenance of this agency IT system.
- **Data Owner:** The agency manager responsible for the policy and practice decisions regarding data.

## Compliance Management Tool

### System Profile

System Name: ISOAG Example

Current Agency:

Virginia Information Technologies Agency

Mode: Read/Write

System Profile

People

Training/Screening

Risk Information

Manages

User Interface

Interconnections

Access Control

Contingency Planning

Change Management

Reporting Documents

Help

Define specific groups or divisions that do have access to the data:

Security Personnel

Are personnel with significant system security and administration responsibilities required to complete specific role based training?

Yes  No

Provide any additional information for Technical Staff Training:

Users with elevated rights are required to take role based training.

Are all users required to take Security Awareness Training?

Yes  No

Provide any additional information for Security Training:

Is background screening required for Technical Staff?

Yes  No

Provide any additional information for Technical Staff screening:

Background screenings are conducted according to organization policy.

Is background screening required for users?

Yes  No

Provide any additional information about background screening:

Previous

Next

Use this screen to identify any security related **training or background screening** being performed for system users or technical staff.

- System Profile
- People
- Training/Screening
- Risk Information**
- Mandates
- User Interface
- Interconnections
- Access Control
- IT Contingency Planning
- Change Management
- Supporting Documents
- Finish

**Describe this system in terms of its sensitivity to the following criteria:**

Confidentiality  Justification

Integrity  Justification

Availability  Justification

Evaluate this system in terms of its sensitivity to the criteria of:  
**CONFIDENTIALITY, INTEGRITY and AVAILABILITY.**

**What Personal identification information does the system contain? (Select all that apply):**

<input type="checkbox"/> ACCOUNT NUMBERS	<input type="checkbox"/> FEDERAL TAX INFORMATION	<input checked="" type="checkbox"/> NAME
<input type="checkbox"/> BIOMETRICS	<input type="checkbox"/> HOME ADDRESSES	<input type="checkbox"/> NATIONAL ID NUMB
<input type="checkbox"/> BIRTH DATES	<input type="checkbox"/> ID CODES/CHARACTERISTICS	<input type="checkbox"/> OTHER
<input type="checkbox"/> CERTIFICATION AND LICENSE NUMBERS	<input type="checkbox"/> INSURANCE POLICY NUMBERS	<input type="checkbox"/> PASSPORT NUMBERS
<input type="checkbox"/> CREDIT CARD NUMBERS	<input checked="" type="checkbox"/> IP ADDRESSES	<input type="checkbox"/> SOCIAL SECURITY NUMBERS
<input type="checkbox"/> DRIVERS LICENSE NUMBERS	<input type="checkbox"/> LICENSE PLATE NUMBERS	<input checked="" type="checkbox"/> TELEPHONE NUMBERS
<input checked="" type="checkbox"/> EMAIL ACCOUNTS	<input type="checkbox"/> MEDICAL DATA	<input type="checkbox"/> VEHICLE IDENTIFICATION NUMBERS
<input type="checkbox"/> FAX NUMBERS	<input type="checkbox"/> MOTHER'S MAIDEN NAMES	

Indicate whether the system contains any **Personally Identifiable Information (PII)**.

If other, Please specify:

Describe any security related incidents that occurred:

any other security

[Previous](#) [Next](#)

Also identify any security related **incidents** or other security concerns that CS&RM should be aware of.



- Home
- Resource Directory
- System Profiles
- Change Agency
- Administration
- Reports

## Compliance Management Tool

### System Profile

**System Name:** ..... ISOAG Example

*Current Agency:*

Virginia Information Technologies Agency

**Mode:** ..... Read/Write

- System Profile
- People
- Training/Screening
- Risk Information
- Mandates**
- User Interface
- Connections
- Access Control
- Contingency Planning
- Change Management
- Documents

Is any data within the system subject to legal mandates relative to security?  Yes  No

Mandate Name	Legal Reference	Mandate Description	Edit	Delete
SEC 501-01	STATE: COV	System is required to comply with SEC 501-01		

Mandate Name: ..... -- Select One --

Description: .....

Is encryption required to meet specific requirements?  Yes  No

If yes, provide details of the encryption:

Add Mandate

Cancel

Previous

Next

Use this screen to identify any **legal or business mandates**, such as HIPAA or PCI, that require compliance for the security of the data maintained in this sensitive system.

- Home
- Resource Directory
- System Profiles
- Change Agency Administration
- Reports

### Compliance Management Tool

#### System Profile

System Name: ISOAG Example

Mode: Read/Write

- System Profile
- People
- Training/Screening
- Risk Information
- Mandates
- User Interface
- Interconnections
- Access Control
- IT Contingency Planning
- Change Management
- Supporting Documents

Common data entry methods include: keyed, batch upload, scanned data (i.e. OCR), etc.

Current Agency:  
Virginia Information Technologies Agency

Use this section to describe how **data is entered** into the sensitive system and how data may be **accessed** through the system.

How is the data entered? (Check all that apply)

- BATCH  
Describe Selected Method
- KEYED  
Describe Selected Method
- OTHER  
Describe Selected Method
- REAL-TIME PROCESSING  
Describe Selected Method
- SCANNED/OCR  
Describe Selected Method

How is the application accessed by the user? (Check all that apply)

- CLIENT/SERVER  
Describe Selected Method
- OTHER  
Describe Selected Method
- REMOTE  
Describe Selected Method
- THIN CLIENT  
Describe Selected Method
- WEB - INTERNET  
Describe Selected Method  
Data must be available to all agencies over the internet. Utilization of VPN provides
- WEB - INTRANET  
Describe Selected Method

Data may be accessed through a client/server interface, thin client interface, web or browser interfaces, remote access, etc.

[Previous](#) [Next](#)

## Compliance Management Tool

### System Profile

**System Name:** ISOAG Example

*Current Agency:*

Virginia Information Technologies Agency

**Mode:** Read/Write

- System Profile
- People
- Training/Screening
- Risk Information
- Mandates
- User Interface
- Interconnections**
- Access Control
- IT Contingency Planning
- Change Management
- Support Documents
- Financial

Is data shared with entities or other programs?  Yes  No

What is the name of the external entities/Agencies that electronic data is shared with?

-- Select One --

If other entity, please specify:

What is the external entities/Agencies system name?

Provide a detailed list of interfaces and system methods of sharing:

What type(s) of data are shared?

Do you have an interoperability agreement/memorandum of understanding?  Yes  No

- Select the type(s) of connection:
- BATCH
  - RECEIVES DATA
  - FTP
  - SENDS DATA
  - OTHER
  - WEB SERVICES
  - REAL-TIME INTERFACE

If other, Please Specify

Add Cancel

Previous Next

If data from this sensitive system is **shared** with other agencies or entities, use this screen to describe the relationship in terms of what data is shared, who it is shared with and how it is shared and documented.

- Home
- Resource Directory
- System Profiles
- Change Agency Administration
- Reports

### Compliance Management Tool

#### System Profile

System Name: ISOAG Example

Mode: Read/Write

Current Agency:

Virginia Information Technologies Agency

- System Profile
- People
- Training/Screening
- Risk Information
- Mandates
- User Interface
- Interconnections
- Access Control**
- IT Contingency Planning
- Change Management
- Supporting Documents
- Finish

Provide a detailed description of the logical access controls in place for this sensitive system:

System utilizes Active Directory and requires VPN connection from external users

Provide a detailed description of the physical access controls in place for this sensitive system:

System is housed in the CESC Datacenter.

Previous

Next

Provide a detailed description of the **logical access controls** in place for this application

Provide a detailed description of the **physical access controls** in place for this application.



## Compliance Management Tool

### System Profile

**System Name:** ISOAG Example

*Current Agency:*

**Mode:** Read/Write

Virginia Information Technologies Agency

#### System Profile

People

Training/Screening

Risk Information

Mandates

User Interface

Interconnections

Access Control

**IT Contingency Planning**

Change Management

Supporting Documents

Finish

Does the data have specific retention requirements?  Yes  No

If yes, provide a description:

Is there an existing contingency plan for this sensitive system?  Yes  No

Is there an alternative site for this sensitive system?  Yes  No

Are backups conducted in a method to restore the sensitive system data meeting the business requirements for the sensitive system?  Yes  No

Is the backup equipment tested on a regular predefined basis?  Yes  No

Excluding backups, is the data stored on a non-network storage device?  Yes  No

If yes, is there approval from the agency head?  Yes  No

Is the data encrypted?  Yes  No

Previous

Next

Use this screen to indicate whether this system has an existing **contingency plan** including any backup requirements. In addition, indicate any specific retention requirements for the data including any that may be mandated by other standards or regulations, such as IRS 1075 or HIPAA.



- Home
- Resource Directory
- System Profiles
- Change Agency
- Administration
- Reports

## Compliance Management Tool

### System Profile

**System Name:** ..... ISOAG Example

**Current Agency:**

Virginia Information Technologies Agency

**Mode:** ..... Read/Write

#### System Profile

People

Training/Screening

Risk Information

Mandates

User Interface

Interconnections

Access Control

IT Contingency Planning

**Change Management**

Supporting Documents

Finish

Are there planned changes for this sensitive system?  Yes  No

Target Date:   
*MM/YYYY*

Short Description:

Change Description:

Has the change been reviewed and approved?  Yes  No

If yes, by whom?

Has a backup/rollback plan been completed?  Yes  No

Has a test plan been created?  Yes  No

Have the proposed changes been tested?  Yes  No

Previous

Next

Indicate any **planned changes** anticipated for this sensitive system including a description, timetable and test plan.



- Home
- Resource Directory
- System Profiles
- Change Agency
- Administration
- Reports

## Compliance Management Tool

### System Profile

**System Name:** ..... ISOAG Example

**Current Agency:**

Virginia Information Technologies Agency

**Mode:** ..... Read/Write

System Profile

People

Training/Screening

Risk Information

Mandates

User Interface

Interconnections

Access Control

IT Contingency Planning

Change Management

**Supporting Documents**

Finish

Please use this area to upload any supporting documents (i.e. Network Diagrams, IT Contingency Planning documents, System Security Plans, Training Documents, Access Control Documents etc...) that will assist Commonwealth Security Services with providing assurance of your sensitive systems security posture.

File upload: .....

Title: .....

Description: .....

File Type: .....

File Name	Friendly Name	Description	Doc Type	Delete	View
PCI Datasheet.pdf		Compliance requirements	OTHER		

Please upload any **supporting documents** that you feel will help VITA to understand the security requirements of your sensitive system. You may wish to upload: MOU's; Interoperability Agreements; Risk Assessments; System Diagrams; Network Diagrams, Policies/Procedures; etc.



# Compliance Management Tools

- Next Tool:
  - Assessments of Infrastructure and Devices
  - Gap Analysis
  - Remediation Tracking
- Down the road:
  - Audit Plans for Sensitive Systems
  - Audit Finding Tracking
  - Corrective Action Reporting



# Compliance Management Tools

- Questions?



# Update: §2.2-2009 Information Security Annual Report

Cathie Brown, CISM, CISSP

---

Deputy, Chief Information Security Officer



## §2.2-2009 Requirement

- C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those ***executive branch and independent agencies and institutions of higher education*** that have ***not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats***. For any executive branch and independent agency or institution of higher education whose ***security audit results and plans for corrective action are unacceptable***, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.



## Our Approach

- Provide Information Security guidance to agencies and institutions of higher education:
  - Published Policy, Standards, and Guidelines
  - Provide awareness and training to meet compliance
  - Provide templates and instructions for planning and reporting IT Security Audits and Corrective Action Plans (CAP's)
  - Monitoring compliance on required submissions
  - Follow up for late or incomplete information



## Our Plan

- Verify the list of agencies and institutions
- Draft data points for assessment
- Vet our plan with COV IS Council
- Vet our plan with APA
- Finalize data points for assessment
- Assess and analyze data
- Work with agency ISO's on inadequate findings
- Draft report
- Finalize report changes
- Submit to CIO



# Verify Agencies and Institutions

- Executive Branch including Higher Education and Independent Agencies
- Excludes:
  - UVA
  - W&M
  - VT
  - VCU
- To Be Determined:
  - VA Baseball Stadium Authority
  - Hampton Roads Sanitation District
  - Hampton Roads Sports Facility Authority
  - VA Coalfield Economic Development Authority
  - VA Resource Authority
  - Roanoke Higher Education Authority
  - VA Business Education Partnership



## Vet Plan with APA & COV IS Council

- COV IS Council – November 19<sup>th</sup>, 2007
- APA - January 31<sup>st</sup>
- Reviewed Requirements of the Code
- Reviewed Data Points
- Verified Data Points



# Data Points For Assessment

- Official ISO Designation
  - Official ISO Designation as submitted to CS&RM and required in IT Security Policy and Standard to include Primary and Backup Designations
- ISO Attendance at ISO Orientation
  - Agency ISO and non-ISO attendance at ISO Orientation
- IT Security Audit Plan
  - IT Security Audit Plan Submission as required by IT Security Audit Standard (to include agencies with no sensitive systems)
- Results of audits including 3<sup>rd</sup> Party and APA Audits
  - Results of SAS 70 Audits, D&T IT Security Audits, Agency Security Audits and APA Audits
- Corrective Action Plans (CAP's)



## Data Points For Assessment (Continued)

- IT Security Policy & Std Exceptions on file
  - Types
  - Pending transformation
- IT Security Incidents and Resolutions
  - Type and Severity
  - Timeliness of reporting (within 24 hrs)
  - Data Breach (number of citizens)
  - Reported and discovered and remediated
- IT Disaster Recovery Plans
  - Approach for Higher Education and Independents
  - Existence vs. viability



## Data Points For Assessment (Continued)

- Results of Information Assurance efforts due in August
- APA Update on SJR51 due in August
- NG Vulnerability Assessments as available
- IT Partnership progress
  - Transformation of Infrastructure



# Additional Considerations

- IT Security Policy and Standards
  - CS&RM Policy, Standard and Guidelines roadmap
- Security Awareness Efforts
  - ISOAG topics and attendance
  - Presentations at other events
  - Cyber Security Toolkit
  - Computer Security Resource Center
- Security Architecture
  - Security Architectural Standards documented
  - Projects Reviewed and Approved
    - VITA Architectural Review (VAR)
    - Commonwealth Architectural Review (CART)
- Information Security Council activities
- Coming Events and Opportunities



# Comments and/or Questions





# Update: IT Security Audit Standard

Cathie Brown, CISM, CISSP

---

Deputy, Chief Information Security Officer



## IT Security Audit Standard - change

Under 2.1 Planning for IT Security Audits:

Annually, each Agency shall develop an IT security audit plan **or review and as necessary, update an existing one** for the government databases for which it is the Data Owner. The IT security audit plan shall be based on the Business Impact Analysis (BIA) **and data classification** performed by the Agency. Each Agency Head shall submit the Agency IT security audit plan to the CISO. However, the initial IT security audit plan shall be submitted to the CISO at the Agency's earliest convenience, but not later than 7 months after the effective date of this standard.



Virginia Information Technologies Agency

# Web Application Hacking

**Tripp Sims**

Commonwealth of Virginia Security Architect

---

ISOAG

March, 2008

Comments: [tripp.sims@vita.virginia.gov](mailto:tripp.sims@vita.virginia.gov)



## A Sample of 2007 Website Hack Headlines

**California State Internet services shut down over website intrusion.**

**Bank of India Distributes Malware due to website hack.**

**Chinese Internet Security Response Team website distributing malware.**

**US State Dept. Russian Consulate website distributes malware due to hack.**

**Hacker Defaces Nuclear Website with Exploding Bomb Photos**

**New Dept. of State Website Accidentally Hosts Loan Documents with SSNs**

**Indiana State Website Hacked, exposing 5,600 credit cards and 71,000 SSNs**



# Cyber Security Toolkit

CYBER SECURITY AWARENESS MONTH



## Cyber Security Awareness Toolkit

<http://www.vita.virginia.gov/security/default.aspx?id=5146>

Banner

Bookmarks

Brochures

Calendar

Posters

Citizen Guide to Online Protection



# Content

- Web Application Hacking
- The Demos
  - Code Quality
  - Parameter Validation
  - Javascript Bypass
  - Access Control
  - Session Management
  - Cross Site Scripting
  - Injection Attacks
  - Improper Error Handling
  - "Googledorks"
- Questions



# Web Application Hacking

- Why target a web application?
  - Efficient and effective
  - Easy anonymity
  - “That’s where the money is.”
- What is a web application?
  - Almost all of it.
  - Anything with logic.



## Q & A

# Questions?



# 2008 Legislation Related to Security

**Peggy Ward**

---

Chief Information Security & Internal Audit  
Officer



## Bills Failed or Continued to 2009\*

- **HB 345** *Credit reports; authorizes an individual to freeze access thereto*
- **HB 384** *Computer trespass; alters elements of crime*
- **HB 385** *Computer invasion of privacy; personal information*
- **HB 390** *Compromised Data Notification Act; created*
- **HB 554** *Computer crimes; website redirection, penalty*
- **HB 971** *Identity theft; database breach notification*
- **HB 1019** *Telecommuting; state agencies to keep savings*
- **HB 1052** *Identity theft; notice of database breach*
- **HB 1087** *Social security numbers; public access, exceptions*
- **HB 1096** *Protection of Social Security Numbers Act; created*
- **SB 492\*** *Vital Records, Office of, et al.; development of alternative verification system*



## Bills Passed

- **HB 633** *Personal Information Privacy Act; prohibits dissemination of another's social security number*
- **HB 634** *Government Data Collection and Dissemination Practices Act; disclosure of personal information*
- **HB 1007** *Fusion Intelligence Center; confidentiality, immunity*
- **HB 1017** *Telework Promotion and Broadband Assistance, Office of; established, report*
- **HB 1311/SB 576** *Credit reports; authorizes consumer to freeze access thereto*
- **HB 1469** *Identity theft; notice of database breach*
- **SB 336** *Temporary detention orders; encryption of medical records not required*



## HB 633

**Personal Information Privacy Act; prohibits dissemination of another's social security number**

<http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb633>

**Personal Information Privacy Act; social security numbers.** Prohibits the dissemination of another person's social security number, regardless of whether such number is obtained from a public or private record. Currently, the prohibition against dissemination only applies to social security numbers obtained from private sources. This bill is a recommendation of the Freedom of Information Advisory Council and the Joint Commission on Technology and Science. *Patrons: May, Athey, Carrico, Cole, Cosgrove, Crockett-Stark, Gilbert, Lingamfelter, Massie, Merricks, Morgan, Poindexter, Rust and Sherwood*

**STATUS:** 03/10/08 House: Impact statement from DPB (HB633ER)



# HB 634

Government Data Collection and Dissemination Practices Act; disclosure of personal information

<http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb634>

Government Data Collection and Dissemination Practices Act (GDCDPA); personal information; definition; collection of same; penalty for violation; jurisdiction of district courts. Provides that no agency shall require an individual to furnish or disclose his social security number (SSN) or driver's license number unless the furnishing or disclosure of such number is (i) expressly authorized by state or federal law and (ii) essential for the performance of that agency's duties. The bill also strengthens the remedies provisions of the GDCDPA by adding civil penalties matching those in FOIA, and grants general district courts the authority to hear GDCDPA cases. Additionally, the bill has enactment clauses giving it a delayed effective date of July 1, 2009, and requires state agencies to study their own collection and use of SSNs and report to the FOIA Council and JCOTS on such collection and use by October 1, 2008. The bill also contains a fourth enactment clause providing for the gathering of similar information about the use and collection of SSNs by cities, counties and towns with a population greater than 15,000. The bill is a recommendation of the Freedom of Information Advisory Council and JCOTS. *Patrons: May, Athey, Carrico, Cole, Cosgrove, Crockett-Stark, Hugo, Morgan, Rust and Sherwood*

**STATUS:** 03/09/08 Senate: Signed by President



## HB 1007

### Fusion Intelligence Center; confidentiality, immunity

<http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1007>

**Virginia Fusion Intelligence Center; confidentiality; immunity.** Provides that papers, evidence, information, etc., and databases or other information in the possession of the State Police are confidential and not subject to the Virginia Freedom of Information Act or the Government Data Collections and Disseminations Practices Act. The bill also provides that employees of the Department are not subject to subpoena in any civil action concerning criminal intelligence information or terrorism investigation. The bill restricts the release or dissemination of information without prior authorization from the Virginia Fusion Intelligence Center and punishes any person who knowingly disseminates information with a Class 1 misdemeanor. If such unauthorized release or dissemination results in death or serious bodily injury, such person is guilty of a Class 4 felony. *Patron: Jones, D.C.*

**STATUS:** [03/08/08 Senate: Conference report agreed to by Senate \(38-Y 0-N\)](#)



## HB 1017

Telework Promotion and Broadband Assistance, Office of;  
established, report

<http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1017>

Office of Telework Promotion and Broadband Assistance; codified; sunset. Codifies Executive Order 35 (2006) creating the Office of Telework Promotion and Broadband Assistance under the Secretary of Technology. The goals of the Office are to encourage telework as a family-friendly, business-friendly public policy that promotes workplace efficiency and reduces strain on transportation infrastructure. In conjunction with efforts to promote telework, the Office shall work with public and private entities to develop widespread access to broadband services. The provisions of this act expire on July 1, 2018. *Patrons: Hugo, Carrico and Lingamfelter; Senator: Puckett*

**Status:** 03/07/08 Governor: Approved by Governor-Chapter 444 (effective 7/1/08)



## HB 1311 / SB 576

### Credit reports; authorizes consumer to freeze access thereto

<http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1311>

**Freezing access to credit reports.** Authorizes any consumer to freeze access to his credit report. If a consumer has placed a freeze on his credit report, a consumer reporting agency is prohibited from releasing the credit report, or any information in it, without the consumer's express authorization. The measure provides a means by which a consumer can release his report, permanently, temporarily, or to a specific third party. Certain disclosures are exempt from the freeze. A fee of up to \$10 may be charged for establishing or lifting a freeze, except identity theft victims are not required to pay a fee except for a temporary lifting of the freeze within 15 minutes of receipt of certain electronic requests. A person who willfully fails to comply with the requirements is liable to a consumer for actual damages of between \$100 and \$1,000, punitive damages, and reasonable attorney fees. A person who negligently fails to comply with the requirements is liable to a consumer for actual damages and reasonable attorney fees. *Patron: Byron*

**Status:** 03/08/08 House: Reenrolled bill text (HB1311ER2)



# HB 1469

## Identity theft; notice of database breach

<http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1469>

**Database breach notification.** Requires an individual or entity that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery or notification of the breach to any resident of the Commonwealth whose unencrypted and unredacted personal information was, or is reasonably believed to have been accessed and acquired by an unauthorized person. A breach is defined as the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Violations by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator. All other violations shall be enforced by the Office of the Attorney General, which may obtain either actual damages or a civil penalty not to exceed \$150,000 per breach or series of breaches of a similar nature that are discovered in a single investigation. *Patron: Byron*

**Status:** 03/10/08 House: Impact statement from DPB (HB1469ER)



## SB 336

Temporary detention orders; encryption of medical records not required

<http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=sb336>

Temporary detention orders; encryption of medical records not required. Provides that a health care provider or designee of a local community services board or behavioral health authority shall not be required to encrypt any email containing information or medical records provided to a magistrate unless there is reason to believe that a third party will attempt to intercept the email. *Patron: Cuccinelli*

**Status:** 03/11/08 Senate: Signed by President



# QUESTIONS?





# Upcoming Events

---





## UPCOMING EVENTS

**Monday, March 24, 1:00 – 3:30 p.m.** ISO Orientation  
CESC ISO orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV IT Security Policy and Standards and is open to all Commonwealth ISO's and interested IT persons!

To register email [VITASecurityService@VITA.Virginia.gov](mailto:VITASecurityService@VITA.Virginia.gov)

**Tuesday, March 25, 8:30 - 11:00 a.m.** AITR Meeting  
Virginia Economic Development Partnership  
901 E. Byrd Street 20<sup>th</sup> floor presentation room



# UPCOMING EVENTS

## COOP TRAINING

**Tuesday, April 1<sup>st</sup>**, 9:00 am – 12:00 pm AND 1:00 – 4:00 pm

**Wednesday, April 2<sup>nd</sup>**, 9:00 am – 12:00 pm AND 1:00 – 4:00 pm

**Location:** Virginia Department of Emergency Management  
Richmond, Virginia

**REGISTRATION DEADLINE:** Friday, March 28<sup>th</sup>, 2008 at 12:00pm

**Tuesday, April 8<sup>th</sup>**, 9:00 am – 12:00 pm AND 1:00 – 4:00 pm

**Wednesday, April 9<sup>th</sup>**, 9:00 am – 12:00 pm AND 1:00 – 4:00 pm

**Location:** George Mason University's Prince William Campus  
Northern Virginia

**REGISTRATION DEADLINE:** Friday, April 4<sup>th</sup>, 2008 at 12:00 pm

**Register at:**

<http://www.vaemergency.com/library/coop/resources/training.cfm>



## UPCOMING EVENTS

The US Department of Homeland Security's National Cyber Security Division and the Multi-State Information Sharing and Analysis Center invite you to participate in the next session of the National Webcast Initiative:

~ Application Security ~

Wednesday, April 23rd, 2008  
2:00pm - 3:00pm (Eastern)

<http://www.msisac.org/webcast/2008-04/>



## UPCOMING EVENTS!

### NEXT ISOAG MEETING

Tuesday, April 8th 1:00 – 4:00

@ CESC

Draft Agenda:

SEC 501 – 01 – Roles and Responsibilities

Messaging in Transformation



Any Other Business ???????

---





**ADJOURN**

**THANK YOU FOR ATTENDING!!**

