



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

January 05, 2011



# ISOAG January 2011 Agenda

- |             |   |                              |
|-------------|---|------------------------------|
| <b>I.</b>   | <b>Welcome &amp; Opening Remarks</b>  | <b>John Green, VITA</b>      |
| <b>II.</b>  | <b>2010 State of Information Security<br/>In the Commonwealth of Virginia</b> | <b>Goran Gustavsson, APA</b> |
| <b>III.</b> | <b>Logical Access Control Requirements:<br/>A Short Review of SEC 501-01</b>  | <b>Bob Baskette, VITA</b>    |
| <b>IV.</b>  | <b>ISOAG Panel Update</b>   | <b>Bob Baskette, VITA</b>    |
| <b>V.</b>   | <b>Upcoming Events &amp; Other Business</b>                                   | <b>Michael Watson, VITA</b>  |
| <b>VI.</b>  | <b>Partnership Update</b>   | <b>Bob Baskette, VITA</b>    |



## CoV ISOAG Briefing

---



### 2010 State of Information Security in the Commonwealth of Virginia

---

Goran Gustavsson  
Auditor of Public Accounts



# Objectives

---

1. Provide a statewide summary of information security program compliance across agencies and institutions of higher education



### Objectives

---

2. Provide a statewide analysis of common security program compliance issues.



### Objectives

---

3. Review agency server room transformation and migration process for those agencies that participate in the Partnership.



### Scope

---

- Includes the information security findings of the most recent audit reports for 114 agencies and institutions of higher education.



### Methodology

---

- Does the Agency have an adequate Information Security Program that effectively mitigates risks to mission-critical and confidential data?



# Methodology

---

- **YES: The agency's program:**
  - Includes all risk management and contingency plans and essential components.
  - Adequately addresses the requirements of the standards or best practices the agency follows.
  - Includes communication to staff, and management has implemented and regularly monitors the plan for effectiveness.



# Methodology

---

- **NO: The agency's program:**
  - Is missing one or more of the risk management and contingency plans or any of the other essential components.
  - Does not adequately address the requirements of the standards or best practices the agency follows.
  - Has not communicated the program to staff, and management has failed to either implement or regularly monitor the program for effectiveness.

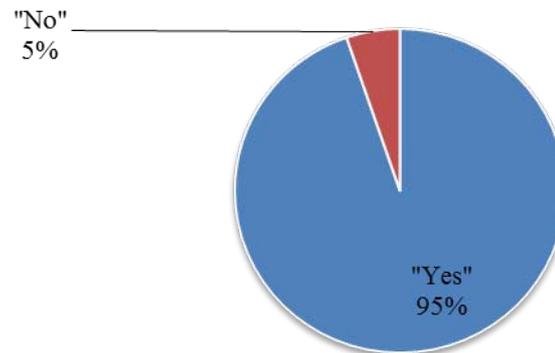


## Summary Report

---

- Six entities (5%) out of 114 do not have adequate information security programs.

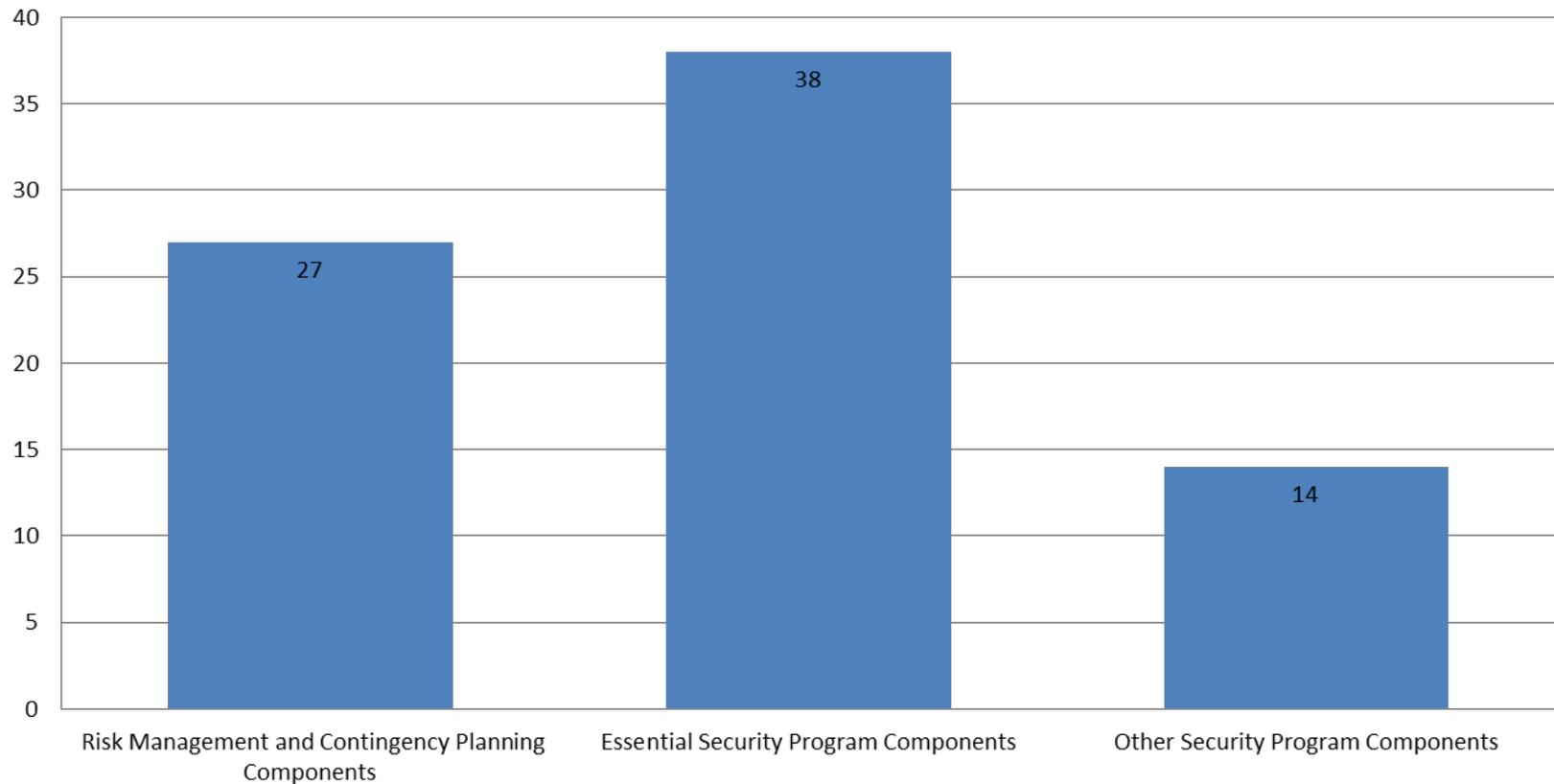
**Adequate Agency  
Information Security Programs**





## Analysis

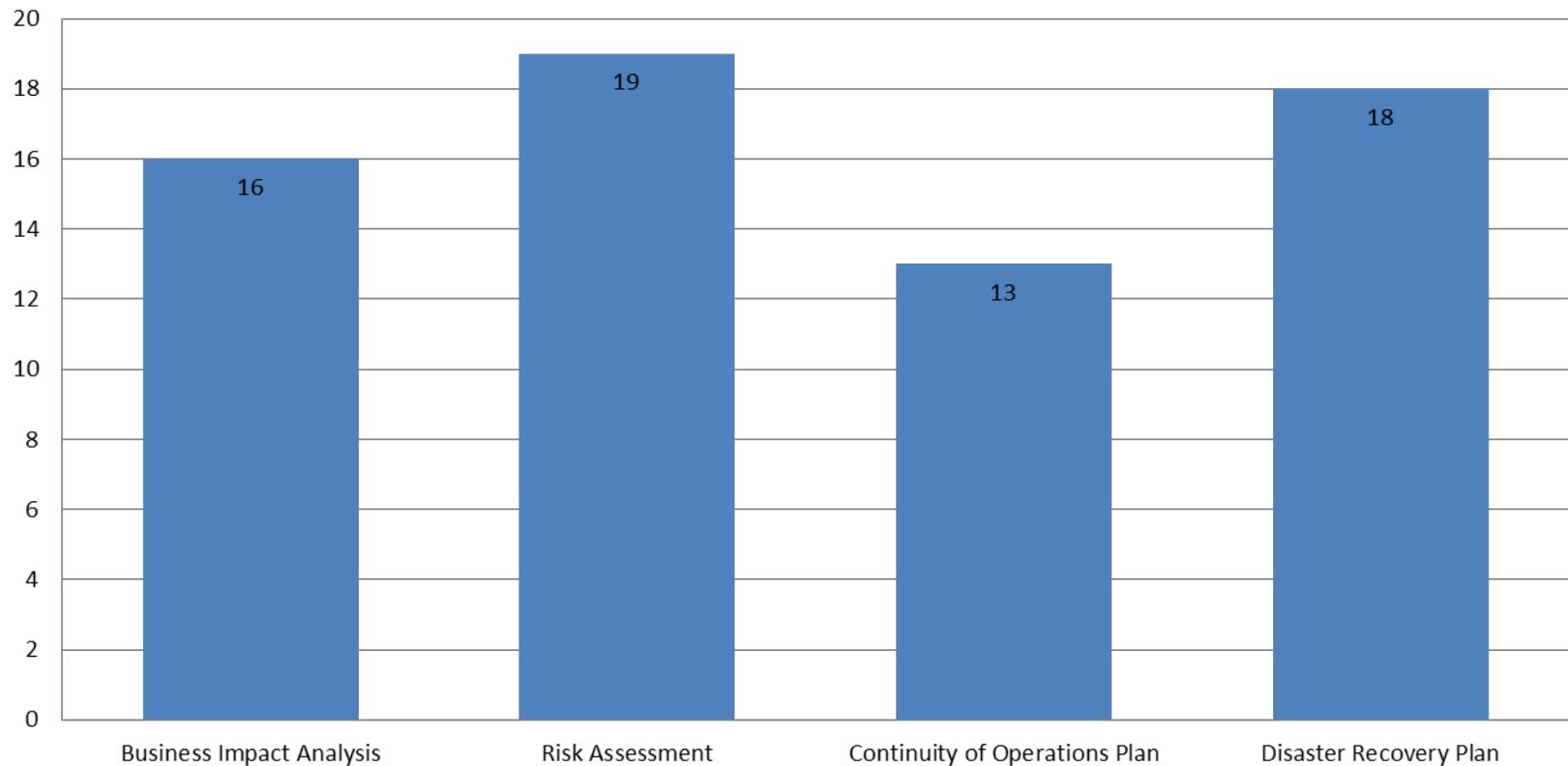
**Agencies with Compliance Issues by Major Security Category**





## Analysis

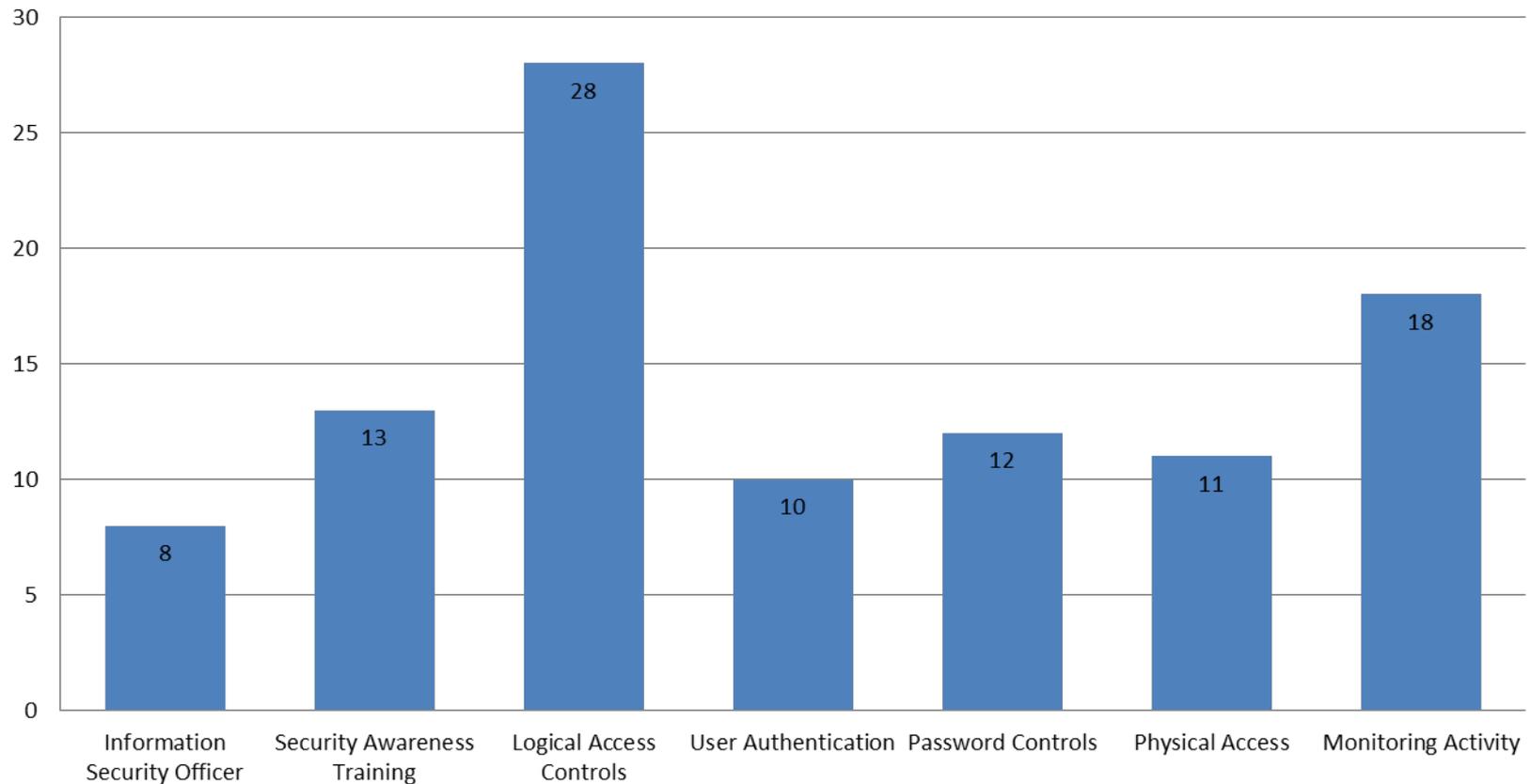
**Agencies with Risk Management and Contingency Planning Weaknesses by Security Component**





## Analysis

**Agencies with Essential Security Component Weaknesses by Component**





## Analysis

---

- 14 entities (12%) had weaknesses in “Other Security Program Requirements”

| Component                        |
|----------------------------------|
| Baseline Security Configurations |
| Data Sharing Security            |
| Encryption                       |
| Incident Response Plan           |
| Change Management                |
| Vulnerability Scanning           |
| Sanitation of Surplus Hardware   |
| Security Reviews                 |



### Finding #1

---

- *The most predominant information security issue in the Commonwealth is logical access controls, followed by risk management and contingency plans. Twenty-eight (25%) out of 114 agencies and institutions do not have logical access controls that are compliant with the Commonwealth's security standards or industry best practices. Twenty-seven (24%) do not have compliant risk management and contingency plans.*



# Agency Server Room Transformation & Migration Review

---

- **Transformation** is when all of the Partnership's servers, laptops, desktops, network, e-mail, and disaster recovery services that the agency use transfer from the agency's old network to the Partnership's new network. The Partnership's network protects and remotely maintains the infrastructure at the agency location through its central network operations center located at the Partnership's data center in Chester.



# Agency Server Room Transformation & Migration Review

---

- **Migration** is the physical relocation of an agency's server room to the Partnership's data center in Chester.



### Finding #2

---

- *Agencies should evaluate the total cost of maintaining the administrative, physical, and environmental controls for a local server room for the Partnership's servers and use this cost when evaluating the cost effectiveness of whether to maintain the Partnership's servers locally or to move the servers to the Chester data center.*



### Next report

---

- Semi-Annual reports
- April/May & October/November timeframes
- Include all 114 agencies with updates for those agencies and institutions audited since last Semi-Annual report.



# Questions?

---

- Contact

Goran Gustavsson

Audit Director

Information Systems Security Specialty Team

Auditor of Public Accounts

Commonwealth of Virginia

(804) 225-3350 ext. 306

[goran.gustavsson@apa.virginia.gov](mailto:goran.gustavsson@apa.virginia.gov)



# Logical Access Control Requirements: A short review of SEC 501-01

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## Commonwealth Audit Findings

- The Auditor of Public Accounts 2010 State of Information Security in the Commonwealth of Virginia audit report states that 28 out of 114 COV Agencies and Institutions are not providing or exercising adequate logical access controls.



## Commonwealth Audit Findings

- The logical access controls defined in the report include the processes for requesting, approving, configuring, reviewing, and removing a user's ability to view, alter, or remove sensitive or critical data.
- The report specifically comments on the lack of logical access controls related to separation of duties and least privilege.



# SEC 501 Local Access Control Requirements

## 5.1 Purpose

- Logical Access Control requirements delineate the steps necessary to protect IT systems and data by verifying and validating that users are who they say they are and that they are permitted to use the IT systems and data they are attempting to access.

# SEC 501 Local Access Control Requirements

## 5.1 Purpose

- Users are accountable for any activity on the system performed with the use of their account. This component of the COV Information Security Program defines requirements in the following three areas:
  - Account Management
  - Password Management
  - Remote Access



## Section 5.2 Account Management

- Purpose
  - Account Management requirements identify those steps necessary to formalize the process of requesting, granting, administering, and terminating accounts. Agencies should apply these Account Management practices to all accounts on IT systems, including accounts used by vendors and third parties.



## Section 5.2 Account Management

- Purpose
  - The requirements that follow distinguish between internal and external IT systems.
  - Internal IT systems are designed and intended for use only by COV employees, contractors, and business partners.
  - External IT systems are designed and intended for use by agency customers and by members of the public.
  - COV employees, contractors, and business partners may also use external IT systems.



## Section 5.2 Account Management

- Requirements
  - Each agency shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts.
  - It is strongly recommended technical controls be implemented wherever possible to fulfill the following requirements, understanding that manual processes must sometimes be implemented to compensate for technical controls that might not be feasible.



## Section 5.2 Account Management

For all internal and external IT systems

- 1. Grant IT system users' access to IT systems and data based on the principle of least privilege.
- 2. Define authentication and authorization requirements.
- 3. Establish policies and procedures for approving and terminating authorization to IT systems.

## Section 5.2 Account Management

For all internal and external IT systems

- 4. If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access that:
  - a. Are documented according to standard practice and maintained on file;
  - b. Include access attributes for the account;
  - c. Are approved by the System Owner and communicated to the ISO; and
  - d. Expire after a predetermined period, based on sensitivity and risk.



## Section 5.2 Account Management

For all internal and external IT systems

- 5. Based on risk, consider use of second-factor authentication, such as tokens and biometrics, for access to sensitive IT systems.
- 6. Review all user accounts for the user's continued need to access all IT systems.

## Section 5.2 Account Management

For all internal and external IT systems

- 7. Notify the System Administrator when IT system user accounts are no longer required, or when an IT system user's access level requirements change.
- 8. If the IT system is classified as sensitive, prohibit the use of guest accounts.



## Section 5.2 Account Management

For all internal and external IT systems

- 9. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.
- 10. Prohibit the display of the last logon user ID on multi-user systems. Desktop and laptop systems assigned to a specific user are exempt from this requirement.

## Section 5.2 Account Management

For all internal and external IT systems

- 11. Lock an account automatically if it is not used for a predefined period. Note: Agencies should strongly consider locking accounts that go unused for 90 consecutive days.
- 12. Disable unneeded accounts.
- 13. Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.

## Section 5.2 Account Management

For all internal and external IT systems

- 14. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.
- 15. Require that the System Owner and the System Administrator investigate any unusual system access activities and approve changes to access level authorizations.



## Section 5.2 Account Management

For all internal and external IT systems

- 16. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.



## Section 5.2 Account Management

For all internal and external IT systems

- 17. Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head's explicit acceptance of defined residual risks.



## Section 5.2 Account Management

For all internal and external IT systems

- 18. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.



## Section 5.2 Account Management

For all internal IT systems

- 19. Require a documented request to establish an account on any internal IT system.
- 20. Complete any agency-required background checks before establishing accounts, or as soon as practical thereafter.



## Section 5.2 Account Management

For all internal IT systems

- 21. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the System Owner or designee to establish accounts for all sensitive IT systems.
- 22. Require secure delivery of access credentials to the user based on information already on file.



## Section 5.2 Account Management

For all internal IT systems

- 23. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.
- 24. Promptly remove access when no longer required.



## Section 5.2 Account Management

For all external IT systems

- 25. Require secure delivery of access credentials to users of all external IT systems.
- 26. Require confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of all sensitive external IT systems.



## Section 5.2 Account Management

For all external IT systems

- 27. Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel (i.e., U.S. Mail).



## Section 5.2 Account Management

For all service and hardware accounts

- 28. Document account management practices for all agency created service accounts, including, but not limited to granting, administering and terminating accounts.

## Section 5.3 Password Management

### Purpose

- Password Management requirements specify the means for password use to protect IT systems and data.

- Requirements

- Each agency shall or shall require that its service provider document and implement password management practices.

## Section 5.3 Password Management

For all internal and external IT systems

- 1. Require the use of a non-shared and a unique password on each account on IT systems, including local, remote access and temporary accounts.
- 2. Require passwords on mobile devices issued by the agency such as PDAs and smart phones. For mobile phones, use a pin number with a minimum of 4 digits.

## Section 5.3 Password Management

For all internal and external IT systems

- 3. Require password complexity:
  - a. At least eight characters in length; and
  - b. Utilize at least three of the following four:
    - 1) Special characters,
    - 2) Alphabetical characters,
    - 3) Numerical characters,
    - 4) Combination of upper case and lower case letters.
  - Note: It is considered best practice not to base passwords on a single dictionary word. It is strongly recommended that system users be educated not to base passwords on a single dictionary word.



## Section 5.3 Password Management

For all internal and external IT systems

- 4. Require that default passwords be changed immediately after installation.
- 5. Prohibit the transmission of identification and authentication data (e.g., passwords) without the use of industry accepted encryption standards (see Encryption).

## Section 5.3 Password Management

For all internal and external IT systems

- 6. Require IT system users to maintain exclusive control and use of their passwords, to protect them from inadvertent disclosure to others.
- 7. Configure all sensitive IT systems to allow users to change their password at most, once per 24 hour period.

## Section 5.3 Password Management

For all internal and external IT systems

- 8. Require users of all sensitive IT systems, to include network systems, to change their passwords after a period of 90 days.
- 9. Require that IT system users immediately change their passwords and notify the ISO if they suspect their passwords have been compromised.

## Section 5.3 Password Management

For all internal and external IT systems

- 10. Configure all sensitive IT systems to maintain at least the last 24 passwords used in the password history files to prevent the reuse of the same or similar passwords.
  - Note: Reference CIS standards for Windows -
  - [http://www.cisecurity.org/tools2/windows/CIS\\_Win2003\\_DC\\_Benchmark\\_v2.0.pdf](http://www.cisecurity.org/tools2/windows/CIS_Win2003_DC_Benchmark_v2.0.pdf) .

## Section 5.3 Password Management

For all internal and external IT systems

- 11. Provide a unique initial password for each new account of sensitive IT systems and require that the IT system user changes the initial password upon the first login attempt.
- 12. For sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential manner.

## Section 5.3 Password Management

For all internal and external IT systems

- 13. Require that forgotten initial passwords be replaced rather than reissued.
- 14. Shared passwords shall not be used on any IT systems.
- 15. Prohibit the storage of passwords in clear text.

## Section 5.3 Password Management

For all internal and external IT systems

- 16. Limit access to files containing passwords to the IT system and its administrators.
- 17. Suppress the display of passwords on the screen as they are entered.



## Section 5.3 Password Management

For all internal and external IT systems

- 18. Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for COV devices. COV devices with access to sensitive systems or those devices in less physically secure environments must have a lower time out interval documented and enforced.

## Section 5.3 Password Management

For all internal and external IT systems

- 19. Require passwords to be set on device management user interfaces for all network connected devices.
- 20. Document and store hardware passwords securely.
- 21. Implement procedures to handle lost or compromised passwords and/or tokens.



## Section 5.3 Password Management

For all internal and external IT systems

- 22. Set an account lockout threshold of not greater than 10 invalid attempts and the lockout duration for at least 15 minutes.



## Section 5.4 Remote Access

### Purpose

- Remote Access requirements identify the steps necessary to provide for the secure use of remote access to resources used by the COV.

### Requirements

- Each agency shall or shall require that its service provider:

## Section 5.4 Remote Access

- 1. Protect the security of all remote access to the agency's sensitive IT systems and data by means of encryption, in a manner consistent with Section 6.3. Note: This encryption requirement applies both to session initiation (i.e., identification and authentication) and to all exchanges containing sensitive data.
- 2. Protect the security of remote file transfer of sensitive data to and from agency IT systems by means of encryption, in a manner consistent with Section 6.3.



## Section 5.4 Remote Access

- 3. Document requirements for use of remote access and for remote access to sensitive data, based on agency and COV policies, standards, guidelines, and procedures.
- 4. Require that IT system users obtain authorization and a unique user ID and password prior to using the agency's remote access capabilities.



## Section 5.4 Remote Access

- 5. Document requirements for the physical and logical hardening of remote access devices.
- 6. Require maintenance of auditable records of all remote access.

## Section 5.4 Remote Access

- 7. Where supported by features of the system, session timeouts shall be implemented after a period of not longer than 30 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented.



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



# ISOAG Panel Update

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## Replies to Questions from Dec. ISOAG Panel

- How does an Agency receive Iron Port logs for agency email?
  - Iron Port logs cannot be generated for a specific Agency.
  - The Iron Port logs record activity for the virginia.gov and state.va.us domain levels.



## Replies to Questions from Dec. ISOAG Panel

- How does an agency receive Bluecoat/ISG reports?
  - The ISO and their representatives can access the reports using their COV domain credentials.
  - The URLs for the BC Reporters:
    - [Http://bcreporter2.vita.virginia.gov:8081](http://bcreporter2.vita.virginia.gov:8081)
    - [Http://bcreporter3.vita.virginia.gov:8081](http://bcreporter3.vita.virginia.gov:8081)



## Replies to Questions from Dec. ISOAG Panel

- Why is the email digital certificate not set to be exportable (Blackberry configuration for signed email)?
  - The ITP Messaging team has produced a procedural document that provides information on how to use the Blackberry Desktop Manger software to transfer the individual's digital signature.



## Replies to Questions from Dec. ISOAG Panel

- How are COV users provisioned for VPN access?
  - Single Factor VPN is provisioned when the COV-AD account is created.
  - Dual factor VPN is requested through the eVA process.



## Replies to Questions from Dec. ISOAG Panel

- Does the Agency provide a list of approved users or does ITP simply enable all Agency users for VPN access?
  - All COV accounts receive single factor VPN.



## Replies to Questions from Dec. ISOAG Panel

- How are Agencies informed when a user is provisioned for VPN access to their systems?
  - During transformation it was communicated to the AITR.
  - Once the agency is transformed, the VCCC issues accounts per request.
  - The Manager of the new user is notified that the accounts are set up and to contact the VCCC for initial password.



## Replies to Questions from Dec. ISOAG Panel

- How will an Agency be notified when an ITP employee that supports the Agency is removed from the Partnership?
  - VCCC will terminate all partnership accounts and notify the Agency when the ITP employee is terminated.
  - This will allow the Agency to terminate any agency applications and/or building access.



## Replies to Questions from Dec. ISOAG Panel

- How can an Agency review and approve users allowed to connect to the network and VPN?
  - ITP Security Operations can a run report by agency on who has VPN access.
  - Please create VCCC ticket to initiate the process.



## Replies to Questions from Dec. ISOAG Panel

- How can an Agency review the list of users authorized to access their systems?
  - The ITP Program Security Office will coordinate with all of the different application owners to gather a list of the uses accounts: Messaging, Unix and Mainframe.
  - There is no single place to gather all users access to all applications. Agency applications would be handled by the agency.



## Open Questions from ISOAG Panel

- What should an Agency do if Partnership support staff use non-COV/non-ITP devices for support services?



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



*Virginia Information Technologies Agency*

# Upcoming Events





## General Assembly

# General Assembly convenes January 12, 2011

(Odd number year = short session)



## Future ISOAG's

From 1:00 – 4:00 pm at CESC

*ISOAG will be held the 1<sup>st</sup> Wednesday of each month in 2011*

Wednesday - February 2, 2011

Wednesday - March 2, 2011



# Future IS Orientation Sessions

**Tuesday - January 11, 2011**  
**(CESC)**

**9:00 – 11:30a**

**Tuesday - March 8, 2011**  
**(CESC)**

**1:00 – 3:30p**

**IS Orientation is now available via webinar!**



# AITR Meeting

## AITR Meeting:

**Wednesday, February 9th**

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

**Location:** TBD



# Information Security System Association

## ISSA

**DATE:** Wednesday, January 19, 2011

**LOCATION:** Maggiano's Little Italy, 11800 W. Broad St.,  
#2204, Richmond/Short Pump Mall

**TIME:** 11:30 - 1:30pm. Presentation starts at 11:45 &  
Lunch served at 12.

**COST:** ISSA Members: \$10 & Non-Members: \$20

**SPEAKER:** Sam Brothers, Digital Forensics Analyst

**TOPIC:** *"A review of ALL Cell Phone Forensics tools  
and HOW they work"*



## Identity Theft Red Flags Rules Extended Until December 31, 2010

- **UPDATE:** On December 18, 2010, President Obama signed legislation that exempts certain businesses, including physician practices and apparently most hospitals, from the Identity Theft Red Flags Rule.
- The Red Flags exemption law more narrowly defines the term "creditor" so that, in effect, far fewer organizations must comply with the rule.

The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until December 31, 2010.

**Read the FAQ at:**

<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



Virginia Information Technologies Agency

Any Other Business ???????



# ADJOURN

## THANK YOU FOR ATTENDING

