



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

February 02, 2011



ISOAG February 2011 Agenda

- | | | |
|-------|---|-------------------------|
| I. | Welcome & Opening Remarks | John Green, VITA |
| II. | Checkmate: How Legitimate Web Sites Have Become Unwilling Pawns For Attackers | Michael Sutton, Zscaler |
| III. | Threat Management:
A Short Review of SEC 501-01 | Bob Baskette, VITA |
| IV. | Open ISOAG Operational Questions | Bob Baskette, VITA |
| V. | Agency-Level Application Support | Bob Baskette, VITA |
| VI. | General Assembly Bills | John Green, VITA |
| VII. | Upcoming Events & Other Business | John Green, VITA |
| VIII. | Partnership Update | Bob Baskette, VITA |



February ISOAG Guest Speaker

**Checkmate:
How legitimate web sites have become unwilling
pawns for attackers**



Michael Sutton
VP Security Research, Zscaler

Keynote slides not available until later. Please check back.



Threat Management: 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 18 out of 114 COV Agencies and Institutions do not comply with the SEC 501 requirements for monitoring system activity.



Commonwealth Audit Findings

- The system monitoring activities listed in the report include the tracking events such as access attempts, alterations to critical data, and actions deemed as malicious activity.
- The report specifically comments on the need to routinely review logs and respond to appropriately suspicious activity.



SEC 501 Threat Management

- Purpose
 - Threat Management delineates the steps necessary to protect IT systems and data by preparing for and responding to information security incidents. This component area defines requirements for the following:
 - Threat Detection
 - Information Security Monitoring and Logging
 - Information Security Incident Handling
 - Data Breach Notification



SEC 501 9.2 Threat Detection

- Purpose
 - Threat Detection requirements identify the practices for implementing intrusion detection and prevention.



SEC 501 9.2 Threat Detection

- Requirements
 - 1. Designate an individual responsible for the agency's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.
 - 2. Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).



SEC 501 9.2 Threat Detection

- Requirements
 - 3. Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.
 - 4. Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.



SEC 501 9.2 Threat Detection

- Requirements
 - 5. Maintain regular communication with security research and coordination organizations, such as US CERT, to obtain information about new attack types, vulnerabilities, and mitigation measures.



SEC 501 9.3

Information Security Monitoring and Logging

- Purpose
 - Information Security Monitoring and Logging requirements identify the steps necessary to monitor and record IT system activity.



SEC 501 9.3

Information Security Monitoring and Logging

- Requirements
 - 1. Designate individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs.



SEC 501 9.3

Information Security Monitoring and Logging

- Requirements
 - 2. Enable event logging on all IT systems. At a minimum, logs will include:
 - a. The event;
 - b. The user ID associated with the event; and
 - c. The time the event occurred
 - Note: Examples of events might include logons, invalid access attempts or data deleted, changed or added.



SEC 501 9.3

Information Security Monitoring and Logging

- Requirements
 - 3. Routinely monitor IT system event logs, correlate information with other automated tools, identify suspicious activities, and provide alert notifications.
 - 4. Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.



SEC 501 9.3

Information Security Monitoring and Logging

- Example: Possible actions include stopping the event, shutting down the IT system, and alerting appropriate staff.
- Note: Multiple actions may be warranted and advisable, based on sensitivity and risk.



SEC 501 9.3

Information Security Monitoring and Logging

- Requirements
 - 5. Prohibit the installation or use of unauthorized monitoring devices.
 - 6. Prohibit the use of keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the Agency Head.



SEC 501 9.4

Information Security Incident Handling

- Purpose
 - Information Security Incident Handling requirements identify the steps necessary to respond to suspected or known breaches to information security safeguards.



SEC 501 9.4

Information Security Incident Handling

- Requirements
 - 1. Designate an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.
 - 2. Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.



SEC 501 9.4

Information Security Incident Handling

- Requirements
 - 3. Implement proactive measures to defend against new forms of cyber attacks and zero-day exploits.
 - 4. Establish information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.



SEC 501 9.4

Information Security Incident Handling

- Requirements
 - 5. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems.



SEC 501 9.4

Information Security Incident Handling

- Requirements
 - 6. Establish a process for reporting information security incidents to the CISO. All COV agencies are encouraged to report security incidents; however, Executive branch agencies must establish a reporting process for information security incidents in accordance with §2.2-603(F) of the Code of Virginia



SEC 501 9.4

Information Security Incident Handling

- so as to report “to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence,” “all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities.”



SEC 501 9.4

Information Security Incident Handling

- Requirements
 - 7. Establish requirements for internal agency information security incident recording and reporting requirements, including a template for the incident report.
 - 8. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.



SEC 501 9.4

Information Security Incident Handling

- 9. Report information security incidents only through channels that have not been compromised. Note: The CISO, in conjunction with the Agency Head through the agency ISO or other Administration authorities as necessitated by circumstances, may authorize the confiscation and removal of any IT resource suspected to be the object of inappropriate use or violation of laws, regulations, policies or standards in order to preserve evidence that might be utilized in forensic analysis of a security incident.



SEC 501 9.5

Data Breach Notification

- Purpose
 - To specify the notification requirements for agencies by identifying the triggering factors and necessary responses to unauthorized release of unencrypted sensitive information.



SEC 501 9.5

Data Breach Notification

- Requirements
 - All of the following are industry best practices. Where electronic records or IT infrastructure are involved, the following are requirements that each agency shall adhere to. Based on their business requirements, some agencies may need to comply with regulatory and/or industry requirements that are more restrictive. Where non-electronic records are involved or implied, the following are advisory in nature, but are strongly recommended:



SEC 501 9.5

Data Breach Notification

- Requirements
 - 1. Identify and document all agency systems, processes, and logical or physical data storage locations (whether held by the agency or a third party) that contain Personal Information which means the first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the data elements are neither encrypted nor redacted:



SEC 501 9.5

Data Breach Notification

- Requirements
 - 1.
 - a. Social security number;
 - b. Drivers license number or state identification card number issued in lieu of a driver's license number; and
 - c. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.



SEC 501 9.5

Data Breach Notification

- Requirements
 - 1.
 - “Redact” means alteration or truncation of data such that no more than the following are accessible as part of the information:
 - a. Five digits of a social security number; or
 - b. The last four digits of a driver’s license number, state identification card number, or account number.



SEC 501 9.5

Data Breach Notification

- Requirements
 - 2. Include provisions in any third party contracts requiring that the third party and third party subcontractors:
 - a. Provide immediate notification to the agency of suspected breaches; and
 - b. Allow the agency both to participate in the investigation of incidents and exercise control over decisions regarding external reporting.



SEC 501 9.5

Data Breach Notification

- Requirements
 - 3. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted Personal Information by any mechanism, including, but not limited to:



SEC 501 9.5

Data Breach Notification

- Requirements
 - 3.
 - a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
 - b. Theft or loss of physical hardcopy; and
 - c. Security compromise of any system.
 - An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.



SEC 501 9.5

Data Breach Notification

- Requirements
 - 3.
 - If a Data Custodian is the entity involved in the data breach, they must alert the Data Owner so that the Data Owner can notify the affected individuals.
 - The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #7, below.



SEC 501 9.5

Data Breach Notification

- Requirements
 - 4. In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules. Agencies shall notify the CISO when notification of affected individuals has been completed.



SEC 501 9.5

Data Breach Notification

- Requirements
 - 5. Provide notification that consists of:
 - a. A general description of what occurred and when;
 - b. The type of Personal Information that was involved;
 - c. What actions have been taken to protect the individual's Personal Information from further unauthorized access;



SEC 501 9.5

Data Breach Notification

- Requirements
 - 5.
 - d. A telephone number that the person may call for further information and assistance, if one exists; and
 - e. What actions the agency recommends that the individual take. The actions recommended should include monitoring their credit report and reviewing their account statements.



SEC 501 9.5

Data Breach Notification

- Requirements
 - 6. Provide this notification by one or more of the following methodologies, listed in order of preference:
 - a. Written notice to the last known postal address in the records of the individual or entity;
 - b. Telephone Notice;
 - c. Electronic notice; or



SEC 501 9.5

Data Breach Notification

- d. Substitute Notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:



SEC 501 9.5

Data Breach Notification

- 1) Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
- 2) Conspicuous posting of the notice on the web site of the individual or the entity if the individual or the entity maintains a web site; and



SEC 501 9.5

Data Breach Notification

- 3) Notice to major statewide media.
- Note: Section C. of Code of Virginia, §18.2-186.6: An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.



SEC 501 9.5

Data Breach Notification

- Note: Section E. of Code of Virginia, §18.2-186.6: In the event an individual or entity provides notice to more than 1,000 persons at one time the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. §1681(a)(p), of the timing, distribution, and content of the notice.



SEC 501 9.5

Data Breach Notification

- 7. Hold the release of notification immediately following verification of unauthorized data disclosure only if law-enforcement is notified and the law-enforcement agency determines and advises the individual or entity that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.



Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov



Thank You!



Open ISOAG Operational Questions

Bob Baskette
Senior Manager, Security Operations
and Architect





Open Questions from December ISOAG Meeting

- How to get a list of NG Contractors who are in the agencies area.
 - We do not plan to have the AOMs compile the list. We need to create a back end process to compile that information and provide it to the AOM to use to ensure he can advise the ISO on who has access to the Agency.



Open Questions from December ISOAG Meeting

- Who is notified of when a NG Contractor leaves
 - We do not plan to have the AOMs compile the list. We need to create a back end process to compile that information and provide it to the AOM to use to ensure he can advise the ISO on who has access to the Agency.



Open Questions from December ISOAG Meeting

- We heard on the ISOAG meeting today that someone in our agency is supposed to be getting a list of the ITB support techs who are supporting our agency.
 - We do not plan to have the AOMs compile the list. We need to create a back end process to compile that information and provide it to the AOM to use to ensure he can advise the ISO on who has access to the Agency.



New Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov



Thank You!



Agency-Level Application Support

Bob Baskette
Senior Manager, Security Operations
and Architect



Agency-Level Application Support

- SEC 501-01 Section 4.5.2.13 allows a COV Agency to define what software packages can be installed on an Agency system.
- ITP End-User Services only supports Level-0 and Level-1 software.
- Level-0 software is the base OS and Level-1 software is common use software (Office, Adobe Reader).



Agency-Level Application Support

- All Agency-specific software is designated as Level-2 software and the Agency is responsible for performing all software maintenance and patching for Level-2 software.
- The Agency should request an AA-account for the Agency Authorized IT Staff to provide support for the Level-2 software.



Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov



Thank You!



General Assembly Legislation Session 2011

John Green
Chief Information Security Officer



HB2189

Information Technologies Agency; assist in determining rules for distribution of electronic records.

Virginia Information Technologies Agency; electronic government services. Provides for the Virginia Information Technologies Agency to assist public bodies of the Commonwealth to determine the rules and standards applicable to the acceptance and distribution of electronic records and electronic signatures. ***Patron: Roxann L. Robinson***

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11102248D

01/12/11 House: Referred to Committee on Science and Technology

01/26/11 House: Stricken from docket by Science and Technology by voice vote



HB2259

Uniform Computer Information Transactions Act; identity credentials.

Provides for the liability or immunity of both providers and licensees of digital identity credentials in the provisioning, providing, and commercially reasonable reliance upon digital identity credentials. The bill also includes technical amendments. ***Patron: Joe T. May***

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11102239D

01/12/11 House: Referred to Committee on Science and Technology



HB2271

Computer and digital forensic services; exempt from regulation as private security service business.

Exempts from regulation as a private security service business any individual engaged in (i) computer or digital forensic services or in the acquisition, review, or analysis of digital or computer-based information, whether for purposes of obtaining or furnishing information for evidentiary or other purposes or for providing expert testimony before a court, or (ii) network or system vulnerability testing, including network scans and risk assessment and analysis of computers connected to a network. **Patron: Mark L. Keam**

Status:

- 01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11102595D
- 01/12/11 House: Referred to Committee on Science and Technology
- 01/26/11 House: Reported from Science and Technology with substitute (21-Y 0-N)
- 01/26/11 House: Committee substitute printed 11104665D-H1
- 01/27/11 House: Read first time
- 01/28/11 House: Read second time
- 01/28/11 House: Committee substitute agreed to 11104665D-H1
- 01/28/11 House: Engrossed by House - committee substitute HB2271H1
- 01/31/11 House: Read third time and passed House BLOCK VOTE (98-Y 0-N)
- 01/31/11 House: VOTE: BLOCK VOTE PASSAGE (98-Y 0-N)



HB2315

Breach of medical information; adds private entities are required to provide notice.

Notification of breach of medical information. Adds private entities to the list of those entities that are required to provide notice of a database breach involving medical information. Current law applies to state and local governmental entities only. Any entity, public or private, that is required to provide similar notice pursuant to federal law would be exempt from the state requirement. *Patron: Kathy J. Byron*

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11103065D

01/12/11 House: Referred to Committee on Science and Technology

01/26/11 House: Reported from Science and Technology (17-Y 3-N)

01/27/11 House: Read first time

01/28/11 House: Read second time and engrossed

01/31/11 House: Read third time and passed House (94-Y 4-N)

01/31/11 House: VOTE: PASSAGE (94-Y 4-N)



HB2317

Information Technology Advisory Council; advise CIO on creation of technology application framework.

Requires the ITAC to advise the Chief Information Officer on the creation of a technology application governance framework through which executive branch agencies can address agency business needs with potential information technology solutions. Agency leaders and information technology managers shall participate with the ITAC in the design of this framework.

Patron: Kathy J. Byron

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11103592D

01/12/11 House: Referred to Committee on Science and Technology



SB943

Information Technology Advisory Council; advise CIO on creation of technology application framework.

Requires the ITAC to advise the Chief Information Officer on the creation of a technology application governance framework through which executive branch agencies can address agency business needs with potential information technology solutions. Agency leaders and information technology managers shall participate with the ITAC in the design of this framework.

Patron: Janet D. Howell

Status:

01/10/11 Senate: Prefiled and ordered printed; offered 01/12/11 11103591D

01/10/11 Senate: Referred to Committee on General Laws and Technology

01/19/11 Senate: Reported from General Laws and Technology (15-Y 0-N)

01/21/11 Senate: Constitutional reading dispensed (35-Y 0-N)

01/24/11 Senate: Read second time and engrossed

01/25/11 Senate: Read third time and passed Senate (39-Y 0-N)



HJ577

Internet; urging Congress to recognize importance of unfettered access and limit regulation by FCC.

Memorializes Congress to recognize the importance of unfettered access to the Internet. Urges Congress to limit the Federal Communications Commission's authority over regulation of the Internet.

Patron: John M. O'Bannon, III

Status:

01/10/11 House: Prefiled and ordered printed; offered 01/12/11 11103326D

01/10/11 House: Referred to Committee on Rules

01/25/11 House: Reported from Rules (15-Y 0-N)

01/28/11 House: Passed by for the day

01/31/11 House: Taken up

01/31/11 House: Pending question ordered

01/31/11 House: Engrossed by House

01/31/11 House: Agreed to by House (63-Y 33-N 3-A)

01/31/11 House: VOTE: ADOPTION (63-Y 33-N 3-A)



HJ645

Local governments; procurement and sharing of technology applications, report.

Study; procurement and sharing of technology applications for local governments; report. Requests the Secretary of Technology to study opportunities to facilitate cooperative procurement and sharing of custom technology applications to leverage buying power and create efficiencies for local government. *Patron: Charles D. Poindexter*

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11103712D

01/12/11 House: Referred to Committee on Rules

01/18/11 House: Assigned Rules sub: #3 Studies

01/27/11 House: Subcommittee recommends reporting with amendment(s) (4-Y 0-N)



Virginia Information Technologies Agency

Upcoming Events





AITR Meeting

Cathilea Robinett, Executive Director for Digital Government & Center for Digital Education will be Guest speaking on “The Latest Trends in Digital Government”

Wednesday, February 9th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: CESC



Information Security System Association

ISSA

DATE: Wednesday, February 9, 2011

NEW LOCATION: The Place At Innsbrook,
4036 Cox Road, Glen Allen, VA 23060

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

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

SPEAKER: Randy Grubb, Executive Director
Cyber Security Research Institute at Armstrong Atlantic State University

TOPIC: *"Hiding Data in Plain Sight, The Covert Channel Threat"*



Future ISOAG's

From 1:00 – 4:00 pm at CESC

ISOAG will be held the 1st Wednesday of each month in 2011

Wednesday - March 2, 2011

Wednesday - April 6, 2011



Future IS Orientation Sessions

Tuesday - March 8, 2011
(CESC)

1:00 – 3:30p

Tuesday - May 10, 2011
(CESC)

9:00 – 11:30a

IS Orientation is now available via webinar!



Virginia Information Technologies Agency

Any Other Business ???????





ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

February 2, 2011



NORTHROP GRUMMAN



ADJOURN

THANK YOU FOR ATTENDING

