



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

May 2, 2012



ISOAG May 2012 Agenda

- | | | |
|------|----------------------------------|--|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Air Force Cyber Operations | Lt. Col. DeLange, Commander
83 NOS |
| III. | Jeopardy Game on IT Ethics | Ed Miller, VITA |
| IV. | 2012 COV Security Annual Report | Michael Watson, VITA |
| V. | Upcoming Events & Other Business | Michael Watson, VITA |
| VI. | Partnership Update | Bob Baskette, VITA, Eric Taylor,
Dennis Brink, Mike Clark, NG |



Air Force Cyber Operations



*Lt Col Eric DeLange
Commander, 83 NOS*



Presentation Intentionally Omitted

Virginia Information Technologies Agency



IT SECURITY ETHICS

Ethics –
is doing the
right thing.

What is the Importance of Ethics in IT Security

Information Security professionals in the Commonwealth are entrusted with the most sensitive and confidential information belonging to an agency.

Ethical behavior, both on and off-the-job, is the assurance that we are worthy of that trust.

Ethical Challenges in Info Security

- Misrepresentation of skills
- Abuse of privileges
- Inappropriate monitoring
- Withholding information
- Divulging information inappropriately
- Overstating issues
- Conflicts of interest
- Management / employee / client issues

Rules and Ethics

Some things we do are required.

- Those are generally laws and regulations and policies.

And some things we do simply because it's the right thing to do.

- Those are ethics.

▲ CAUTION



SLIPPERY
SLOPE

The Slippery Slope

- The “slippery slope” is the theory that sometimes A leads to B which might lead to C which could lead to D. D would be bad.
- There is an Arabic saying that “if you let the camel put his nose in the tent, the rest of the camel will soon follow”.
- Sometimes, even the “appearance” that A could lead to B, is enough to “suggest” that there is an impropriety, a conflict of interest, or other ethical problem.
- COV employees should try to avoid both the slippery slope₁₀ and even the appearance of being on the slippery slope.

Code of Ethics (based on ISSA)

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles.
- Promote generally accepted information security current best practices and standards.
- Maintain appropriate confidentiality of sensitive information encountered in the course of professional activities.
- Discharge professional responsibilities with diligence and honesty.
- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of the agency or the COV.

Let's Play a Game

We're going to play
a Jeopardy style
Quiz Game.

IT Security Ethics Jeopardy

Rules

1. We're not playing for real money
2. You do not have to phrase your "answer" in the form of a "question" like on the real Jeopardy
3. We'll use 3 teams of 2 people per team and everyone has a buzzer.
4. Anyone can buzz in on a question
5. First to buzz, gets to answer
6. You can buzz at any time, but I'll finish reading the question before I call on you to answer.
7. Answer right, you win that many points and can choose the next question.
8. Answer wrong, you lose that many points.
9. If you answer wrong, someone from another team can buzz to answer, but not your teammate.
10. We're not playing for real money!

IT Security Ethics Jeopardy

Rules

1. Some questions deal with specific laws, rules or policies or other topics and therefore have specific answers.
2. However, many questions are asking about “ethics” (i.e. the right thing to do) and not what is specifically allowed or not allowed under the law or by COV policies.
3. Some of the answers to some questions are therefore debatable or open to interpretation.
4. I chose what I think is the “best” answer under the circumstances posed by the question.

IT Security Ethics Jeopardy

COV Policies	Survey Says	Myth Busters	Ethics	Situations
<u>\$100</u>	<u>\$100</u>	<u>\$100</u>	<u>\$100</u>	<u>\$100</u>
<u>\$200</u>	<u>\$200</u>	<u>\$200</u>	<u>\$200</u>	<u>\$200</u>
<u>\$300</u>	<u>\$300</u>	<u>\$300</u>	<u>\$300</u>	<u>\$300</u>
<u>\$400</u>	<u>\$400</u>	<u>\$400</u>	<u>\$400</u>	<u>\$400</u>
<u>\$500</u>	<u>\$500</u>	<u>\$500</u>	<u>\$500</u>	<u>\$500</u>



2012
Commonwealth Security Annual Report

Michael Watson
Chief Information Security Officer



§ 2.2-2009

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly 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 or 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 (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.



New data points for 2012

- The percentage of Audit report(s) received per Audit plan on file
- Documentation on information about the agency's BIA, RA(s) (*Risk Assessment(s) for sensitive system(s) scheduled to be audited this calendar year*)
- IDS reports
- Risk Profile Survey – per new risk profile survey tool
- The number of open Audit and Risk findings rated High, Medium, or Low per Security Standard domain.
- The percentage of Audit and Risk Findings with Exceptions on file.



Datapoints for 2012 Annual Report

Agency Information Security Datapoints Dashboard – Legend

ISO Designated

-  - The agency head has designated an Information Security Officer (ISO) for the agency within the past two years.
-  - The agency head has NOT designated an ISO for the agency within the past two years.

Attended ISO Certification

-  - The Primary ISO is certified
-  - The Primary ISO is NOT certified.

2012 Overall Audit Program

-  - All documents received as scheduled
-  - Missing CAP(s) or Quarterly update(s)
-  - Missing Audit plan or
 - % < 100 % - **Audit report(s) received per Audit plan on file** or
 - % < 85% - Percentage of 3 year obligation completed

2012 Overall Risk Profile

-  - All documentation received as requested information about the agency's BIA, RA(s)^[1], IDS, Risk Profile Survey^[2]
-  - Missing IDS report(s)
-  - Missing any required documentation as requested information about the agency's BIA, RA(s), IDS report, Risk Profile Survey

^[1] Risk Assessment(s) for sensitive system(s) scheduled to be audited this calendar year

^[2] Depending on acquisition and deployment of risk profile survey tool



Agency Information Security Datapoints - Dashboard

Agency	Agency Name	ISO Designated	ISO Certification	2012 Overall Audit Program	2012 Overall Risk Profile
xyz1	Agency 1	Green	Red	Red	Green
xyz2	Agency 2	Green	Green	Red	Red
xyz3	Agency 3	Green	Green	Green	Yellow
xyz4	Agency 4	Yellow	Green	Yellow	Red
xyz5	Agency 5	Green	Red	Green	Green
xyz6	Agency 6	Green	Red	Green	Green
xyz7	Agency 7	Yellow	Red	Yellow	Green
		Grey	Grey	Grey	Grey
xyz8	Agency 8	Green	Red	Green	Yellow
xyz9	Agency 9	Green	Red	Green	Yellow
		Grey	Grey	Grey	Grey
xyz10	Agency 10	Red	Red	Red	Green
xyz11	Agency 11	Green	Red	Red	Green



Detailed Audit Program Information by Agency

2012 Overall Audit Program Score - will be tallied using same methodology as in 2011

Security Audit Plan Received

Yes - The agency head has submitted a current security audit plan for systems classified as sensitive.

No - The agency head has never submitted a security audit plan for systems classified as sensitive.

Expired - Audit plan on file is does not cover the required 3 year period.

Security Audit Reports Received

X% - The percentage of due audit reports received based on the security audit plan

N/A - Not applicable as the agency had no audits due or the agency head has not submitted a security audit plan.

Corrective Action Plans Received & Quarterly Updates Received

X% - The percentage of due corrective action plans & quarterly updated received based on the security audit plan

N/A - Not applicable as the agency had no corrective action plans or quarterly updated due or the agency head has not submitted a security audit plan.

Percentage of Audit Obligation Completed

X% - The percentage of audit work completed as measured against the agency's security audit plans over the past three years.



Detailed Agency Information Security - 2012 Overall Audit Program Scores

Agency	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
XYZ	Current	100%	90%	75%	100%

Security Audit Plan Received: The Agency Head has

Current - submitted a Security Audit Plan for the period of fiscal year (FY) 2012-2014 or 2013-2015 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2012, Audit Plans submitted shall reflect FY 2013-2015)

No - not submitted a Security Audit Plan since 2006

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY FY 2012-2014 or FY 2013-2015

Pending –submitted a Security Audit Plan that is currently under review

2012 - Percentage of Audit Reports Received per the Audit Plan: The Agency Head or designee has

% – submitted % of Audit Reports or planned audits listed on submitted Audit Plan

N/A - not had Security Audits scheduled to be completed

Pending –submitted a Corrective Action Plan that is currently under review

2012 - Percentage of CAPs Received: The Agency Head or designee has

% – submitted % of CAPs for planned audits listed on submitted Audit Plan

N/A - not had Security Audits scheduled to be completed

Pending –submitted a Corrective Action Plan that is currently under review



Detailed Agency Information Security - 2012 Overall Audit Program Scores Con't

Agency	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
XYZ	Current	100%	90%	75%	100%

2012 - Percentage of Quarterly Updates Received: The Agency Head or designee has

% – submitted % of QUs for all open findings per CAPs submitted

N/A - not had Security Audits scheduled to be completed

Pending –submitted a Corrective Action Plan that is currently under review

3 year - Percentage of Audit Obligation Completed:

Percent of sensitive systems reported **by 2009** (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *“At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.”*

Agencies that did not submit an IT Security Audit Plan **by 2009** were not in compliance and therefore there is no data to report on for **2012**.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

N/C – agency not in compliance by 2008, agency did not submit an IT Security Audit Plan **by 2009**

Pending – currently under review

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved



2012 Complete Risk Profile Totals of Audit and Risk Findings

Agy Acronym	Risk Level	Risk MANAGEMENT	IT Contingency Planning	Information Systems Security	Logical Access Control	Data Protection	Facilities Security	Personnel Security	Threat Management	IT Asset Management	Percentage Of Findings with Exceptions
XYZ	High	4	0	0	0	9	0	3	0	0	100%
	Medium	0	0	0	0	0	0	0	0	0	
	Low	0	0	0	0	0	0	0	0	0	

2012 Complete Risk Profile – Data collected will be used in summary to show the Risk Profile for the COV .

nn - The number of open Audit and Risk findings rated High, Medium, or Low per Security Standard domain.

% - The percentage of Findings with Exceptions on file.

N/A - Not applicable as the agency had no open findings

Notes:

Exceptions will be included as part of the risk scoring this year. Exceptions should be on file for any findings identified in the risk assessment process or identified as part of the security audit process.

Risk findings will come from Information about Risk Assessment(s) and Risk Profile Survey

Audit findings will come from information included in the security audit reports.

SEC501 Domains are Risk Management, IT Contingency Planning, Information Systems Security, Logical Access Control, Data Protection, Facilities Security, Personnel Security, Threat Management, IT Asset Management



FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings, CSRM will record this action from the audit report received. No further action will be needed.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

December 31, 2012



Questions ???????

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

Thank You!



Virginia Information Technologies Agency

Upcoming Events





Information Security System Association

ISSA

DATE: Wednesday, May 9, 2012

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: *David Frei, Capital One*

TOPIC: Mobile Device Risk Assessment



COV Training Offered by DOA

Implementing Enterprise Risk Management: A Practical Approach w/ ARMICS

This class incorporates references to Virginia's ARMICS process and will focus on training governmental employees and incorporating the mission statement of the agencies represented at the training.

- When: May 8 & 9
- Time: 8:15am to 4:45pm each day
- Where: James Monroe Building
- Cost: \$320
- Register: <https://hrtraining.doa.virginia.gov/>

Earn 16 CPEs for taking this class

Questions? Contact: Tim.Sadler@DOA.Virginia.Gov



ISACA Offering Training

CISA Review Class

Location: EdgeComm, 4913 Fitzhugh Ave, Ste: 201, Richmond, VA 23230

Time: 6 – 9 pm

Dates: May 7, 9, 14, 16, 21, 23

Instructor: Jerry Jarvis, CISA, CRISC, CIA, CFSA

Registration: Online at www.isaca-va.org/

Discount for early registration before April 15. Registration closes May 4.

Course will cover all (5) job practice domains of the CISA body of knowledge.

The process of Auditing Information Systems

Governance and Management of IT

Information Systems Acquisition, Development & Implementation

Information Systems Operations, Maintenance & Support

Protection of Information Assets

Sample tests will be administered and discussed.



ISACA Offering Training

CISM Review Class

Location: EdgeComm, 4913 Fitzhugh Ave, Ste: 201, Richmond, VA 23230

Time: 6 – 9 pm

Dates: May 8, 10, 15, 1, . 22, 24

Instructor: John Karabaic, CIPP/IT, CISM, CISSP &
Chandra Barnes, CISM,CRISC

Registration: Online at www.isaca-va.org/

Discount for early registration before April 15. Registration closes May 4.

Course will cover all (5) domains of the CISM body of knowledge.

Information Security (IS) Governance

Information Risk Management

IS Program Development

IS Program Management

Incident Response & Management

Sample tests will be administered and discussed.



Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - June 6, 2012

Topic: Obtaining IS Certifications

Wednesday - July 11, 2012 (2nd Weds. due to holiday)

Topic: PCI Challenges

ISOAG will be held the 1st Wednesday of each month in 2012



IS Orientation Sessions

Tuesday - May 15, 2012

9:00 – 11:30a
(CESC)

Email CommonwealthSecurity@VITA.virginia.gov if you are interested in attending.

IS Orientation also available via webinar!



Submit Events

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

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

May 2, 2012



NORTHROP GRUMMAN

ADJOURN

