



ISOAG Meeting October 7, 2015

Welcome to CESC!





ISOAG October 7, 2015 Agenda

- | | |
|-----------------------------------|----------------------|
| I. Welcome & Opening Remarks | Michael Watson, VITA |
| II. Strategic Goals for 2015/2016 | Mike Watson, VITA |
| III. Executive Directive #6 | Mike Watson, VITA |
| IV. ISO SharePoint Site | Andy Hallberg, VITA |
| V. Phishing Exercise/Pen Testing | Andy Burge, VITA |
| VI. OWA | Bob Baskette, VITA |
| VII. Cloud Security Standard | Bob Baskette, VITA |
| VIII. Data Disposal Standard | Bob Baskette, VITA |
| IX. ISO Certification | Ed Miller, VITA |
| X. Partnership Update | NG |



Virginia Information Technologies Agency

Strategic Goals for 2015/2016

Michael Watson
CISO

ISOAG Meeting
10/7/2015



CSRM Objectives

- Identity Management
 - Internal Commonwealth Users
- Improved Security Training
 - ISO, End User, COV Leadership, and IT User Training
- Continue Development of Risk Management
- Third Party Hosting Requirements
- COV Critical Infrastructure Readiness



Cyber Commission Goals

- ISAO
 - Build the Joint Cyber Security Operations Center (JCSOC) for the purpose of Information Sharing
- Identity Management
 - Accelerate Adoption of Identity and Access Management (IAM) and Encryption.
- Risk Management
 - Accelerate Adoption of a Common Cyber Security Guidance Framework



Executive Directive #6

Michael Watson
CISO

ISOAG Meeting
10/7/2015



Key Goals

- Identify data sets used
- Identify all applications
 - Third party hosted
 - Agency/NG hosted
- Identify sensitivity of the data
 - Confidentiality, Integrity, and Availability
- Identify type of data
 - PII, PCI, PHI, etc.
- Prioritize risk of each system based on their data sets
- Identify risk based approach to protect systems



Approach

- Step 1 – Identify data sets
 - Collect attributes of data sets
 - Classify data sets in regulatory categories
 - PCI, PII, PHI, etc.
- Step 2 – Identify data set sensitivity
 - Collect and analyze any attributes that contribute to sensitivity of data
 - Request agency ISO opinion to sensitivity of the data



Approach

- Step 3 – Identify Security Controls In Place
 - Focused on controls protecting data rather than systems
 - Identify controls supporting first five of Top 20 Critical Security Controls
- Step 4 – Identify Technology Used to Access Data
 - Associate all data sets with applications
 - Associate all devices with applications



Approach

- **Step 5 – Reconcile Issues**

- Identify data that appears to be in conflict
 - Sensitive data on a non-sensitive system
 - Data that is or should be PHI, PCI, PII, etc. but isn't identified as sensitive
 - Devices/Applications that are not associated or are incorrectly associated
- Identify unlikely scenarios
 - Disproportionate ratio of devices to applications or data sets to applications
- Controls that are not adequate



Preliminary Results

General Info gathered

# of Data sets	2071
# of Apps associated with Devices	1287
# of Sensitive Applications associated with Devices	514
# of Devices associated with an application	983
# of Devices	5256
# of Completed Data sets	1183
CSRM Approved Data sets	1143
Records Stored Annually	186,831,383,433
Records Processed Annually	159,923,537,436
Agencies with data sets	72

Comparison of 8/15 to today			
	<u>8/15/2015</u>	<u>10/6/2015</u>	<u>Difference</u>
# of Applications	2006	2495	24% INCREASE
# of Sensitive Applications	763	774	Needs to be trued-up
Projected # of sensitive applications due to C,I, A	763	1345	76% INCREASE



Preliminary Results

Types of Data	Data Sets	Agencies
PHI	157	31
PMI	93	29
PCI	12	9
FERPA	40	13
FTI	154	32
Critical Infrastructure	58	14
Legal or Investigative	75	32
Intellectual Property	30	15
SCADA	12	6
Law Enforcement	55	25

Contains none of the above

data sets	437
agencies	51
records stored	4,228,032,583
records processed	815,530,261



What's Next?

- Report
 - Section 1
 - Analysis of the data collection
 - Section 2
 - Identify and recommend security audit and security staff resources necessary to perform full review and remediation
 - Prioritize remediation of systems based on riskiness of systems
 - Identify risks based on resources available to each agency

**IS COUNCIL
ISO KNOWLEDGE SHARING
COMMITTEE**

ANDY HALLBERG / ALCOHOLIC BEVERAGE CONTROL

Site Name: ISO Knowledge Sharing

Link:

<https://share.virginia.gov/sites/VITASec/ISOKnowledgeSharing>



Simulated Phishing

CSRM will be conducting simulated Phishing exercises

- Starting October 2015
- Phase I - VITA only
- Phase II – Commonwealth-wide
- Official notice being sent to agency ISOs & AITRs

Simulated Phishing

- Exercise will measure vulnerability to Phishing
- Post-exercise statistics will be shared
- Users who get hooked will land on a Phishing education page:
<http://vita2.virginia.gov/phishingEducation>
- Education page designed to improve user protection against Phishing
- Follow-up exercises to measure improvement



Pen-Testing Program

CSRM will be conducting Pen-Testing

- Scope will cover entire Commonwealth
- Program will run continuously
- Purpose is to test exposure as issues are identified
- CSRM will provide testing time frame to agencies



Pen-Testing

- **CSRM will only utilize test methods with low potential of service disruption**
- **Emergency contact:
commonwealthSecurity@vita.virginia.gov**



Virginia Information Technologies Agency

Questions?





Two-Factor Authentication for OWA

- All access to OWA (Outlook Web Access) will require Two-Factor authentication starting November 2015.
- The exact date will be determined once testing is completed on October 28, 2015.

ISOAG meets the 1st Wednesday of each month in 2015



Two-Factor Authentication for OWA

- VITA will issue a set of communications describing the authentication change for OWA access over the next month.
- Agencies can utilize physical tokens or soft tokens as the secondary authentication factor for OWA access.

ISOAG meets the 1st Wednesday of each month in 2015



Two-Factor Authentication for OWA

- Physical tokens can be purchased via eVA. Please contact your CAM for more information.
- Soft tokens can be requested for COV assets via a VCCC ticket. Please include the user's name, email address, and asset tag number.

ISOAG meets the 1st Wednesday of each month in 2015



Two-Factor Authentication for OWA

- The deployment of soft tokens for non-COV devices is currently under review. Devices under consideration for a test are iOS and Android 5.x devices.
- More information on non-COV devices will be available after additional testing.

ISOAG meets the 1st Wednesday of each month in 2015



Two-Factor Authentication for OWA

Questions:

Please send all questions to
CommonwealthSecurity@vita.virginia.gov

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Commonwealth Security has created the Cloud-Based Computing Information Security Standard.
- This document defines the minimum security requirements and controls necessary to store Commonwealth data outside of a data center owned or leased by the Commonwealth.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- The standard is based on the security requirements defined in COV ITRM SEC 501-09 as well as “Best Practices” as defined by FEDRAMP and Cloud Security Alliance.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- This document should be posted to ORCA in December.
- Commonwealth Security encourages all ISOs, AITRs, and any other interested parties to review the document and provide comments on the content via ORCA.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - This standard addresses COV data not stored in a data center owned or leased by the Commonwealth.
 - COV ITRM SEC 501-09 still applies to all data stored at an agency or within the Partnership.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - Encryption of data at rest required.
 - Encryption of data in transit required.
 - Agency must maintain exclusive control of the encryption keys.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - Password length set to 12-character.
 - Password expiration set to 42-days.
 - Password complexity requires all four characteristic: Upper Case, Lower Case, Special characters, and numbers.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - Vulnerability scans of the systems performed every 30-days.
 - All security patches for the operating system and application installed within 60-days of release by OEM.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - All authentication credentials must be encrypted in transit.
 - If an agency requires COV credentials to be used within the cloud a one-way trust must be established to the External Authentication Domain provided by VITA.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - All data center storage and replication is limited to the Continental United States.
 - Hosting center support staff must be physically located in the Continental United States.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - Hosting center support staff must be US citizens or H1B visa holders.
 - All hosting center software must be supported by OEM vendors.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - All agency leased computing systems must reside in same rack if hosting vendor utilizes multi-tenancy.
 - All agency leased computing systems must maintain the 2-or-3 architecture tier separation across hypervisors

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - The same Hypervisor cannot support both the Internet/User interface and the data storage service.
 - The same Hypervisor cannot support both production and non-production environments.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - The hosting vendor must conduct vulnerability testing of physical controls once a year.
 - The hosting vendor must provide a summary of findings from all vulnerability scans.

ISOAG meets the 1st Wednesday of each month in 2015

COV ITRM SEC 525-01

- Important items of note in the standard:
 - The hosting vendor must conduct penetration testing once a year
 - The hosting vendor must provide a summary of findings from all penetration tests.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - The hosting provider must submit to a SSAE-16 audit once a year
 - The hosting provider must provide a summary of findings from all audit activities.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Important items of note in the standard:
 - The CIO of the Commonwealth has the authority to end a hosting agreement and return the business function to the control of the Commonwealth if the agency is not performing the required due diligence to protect the data assigned to that agency.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-01

- Please note, the approval and publication of the Cloud-Based Computing Information Security Standard does not implicitly grant permission for COV agencies to use cloud/hosting services.
- VITA still reserves the right to review and approve all hosting requests.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 525-04

Questions:

Please send all questions to
CommonwealthSecurity@vita.virginia.gov

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 514-04

- Commonwealth Security has updated the Removal of Commonwealth Data from Electronic Media Standard
- The document is proceeding through a final internal review and will be posted to ORCA in November

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 514-04

- Commonwealth Security encourages all ISOs, AITRs, and any other interested parties to review the document and provide comments on the content via ORCA.

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 514-04

- Important additions to the document:
 - Removal methods for solid state drives
 - Removal methods for mobile devices
 - Removal methods for multi-function devices
 - Removal methods for non-volatile memory
 - Removal methods for embedded devices

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 514-04

- In addition, agencies should contact the Chief Information Security Officer of the Commonwealth of Virginia for guidance on the removal method for any new or emerging technology not covered in SEC 514.
- CommonwealthSecurity@vita.virginia.gov

ISOAG meets the 1st Wednesday of each month in 2015



COV ITRM SEC 514-04

Questions:

Please send all questions to
CommonwealthSecurity@vita.virginia.gov

ISOAG meets the 1st Wednesday of each month in 2015



CONTINUING EDUCATION REQUIREMENTS

Commonwealth ISO Certification Program



Commonwealth ISO Certifications 2015

2013 Non COV Certified ISOs'

2013 Commonwealth Certified ISOs'

2015 Non COV Certified ISOs'

2015 Commonwealth Certified ISOs'

41.89 %

58.11 %

15.56 %

84.44 %



Maintaining Your Certification

In order to maintain your status as a Commonwealth Certified ISO in 2015, you need to meet 4 basic conditions:

1. Agree to the Commonwealth IT Security Code of Ethics
2. Attend any mandatory ISOAG meetings in 2014
3. Attend IS Orientation once every 2 years
4. Obtain 20 hours of continuing education credit per year



1. Code of Ethics

ISOs' are entrusted with an agency's most highly confidential and sensitive information.

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



Commonwealth IT Security Code of Ethics

- Perform all professional activities and duties in accordance with all applicable laws, commonwealth regulations and the highest ethical principles
- Promote current and generally accepted information security 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, or give the appearance of, a conflict of interest or otherwise damage the reputation of the agency or the COV



2. Mandatory ISOAG Meetings

- Annually, we will have a mandatory meeting of all ISOs' in October.
- We encourage all primary ISOs' to attend this meeting in person.
- If you are a primary ISO, and cannot attend, you may designate the backup ISO to attend in your place.



3. Attend IS Orientation Every 2 Years

- All ***primary ISOs' are required*** to attend this 2 hour session at least once every 2 years. The requirement to attend cannot be delegated to a backup ISO or other person unless approved by the CISO. However, backup ISO's and other interested persons are encouraged to attend.
- We are continually changing and evolving the content provided in the IS Orientation session. Some sessions will be offered that will look closer at specific ISO learning areas: Risk Assessments, Policies, Control Implementation, Security Plans, etc.



4. Continuing Education Requirements

- In order to maintain the COV ISO Certification, ISOs' must commit to furthering their education.
- The goal is to ensure that all ISOs' are maintaining a minimal level of current knowledge and proficiency in the field of Information Security.
- In 2015, the continuing education requirement is 20 hours. Each hour of conditioning education is known as a CPE (continuing professional education) credit. CPE can be obtained in a number of ways.



Continuing Education Requirements

- At least one of the 20 CPE credits, must be obtained by completing 1 course in ISO Academy in the Knowledge Center. For the purposes of this requirement, we will equate 1 ISO Academy course to 1 hour or credit of continuing education.



Continuing Education Requirements

- If you already have a nationally recognized IT security certification, then any continuing education that is required by that certifying authority will also be honored by the COV Certification program.
- You **do not** need to obtain an additional 19 CPE hours above and beyond what you are already reporting for continuing education for any other nationally recognized IT security certifications. In other words, the 19 hours that you acquire for your CISSP, CISM, GIAC or other recognized certification can also be applied to your COV ISO Certification.



How to Earn Continuing Education (CPE)

- Take add'l IT security courses in the KC ISO Academy (1 course=1 hr)
- Attend training courses or seminars related to IT Security
- Attend IT security conferences
- Attend ISOAG Meetings
- Attend chapter meetings of a recognized IT security organization
- Take IT security related academic courses at a higher ed institution
- Complete IT Security related webcasts, podcasts or other computer based training
- Read IT security related books or articles (limit of 10 hrs/year)
- Publish an IT Security related book or article
- Attend vendor sales/marketing presentations (limit of 5 hrs/year)
- Teach or present on an IT security related topic
- Serve or volunteer for committee work on the **COV Security Council**



Reporting Continuing Education to CSRM

- When you have completed ***all 20 hours*** of required continuing education activities in 2015, send an email to commonwealthsecurity@vita.virginia.gov indicating that you have completed.
- We do not need notification for each time you complete a specific or individual activity nor do we need any documentation. Your word is gold here. However, please include in the email a brief description of the activities that you have completed.



Maintaining Continuing Education Records

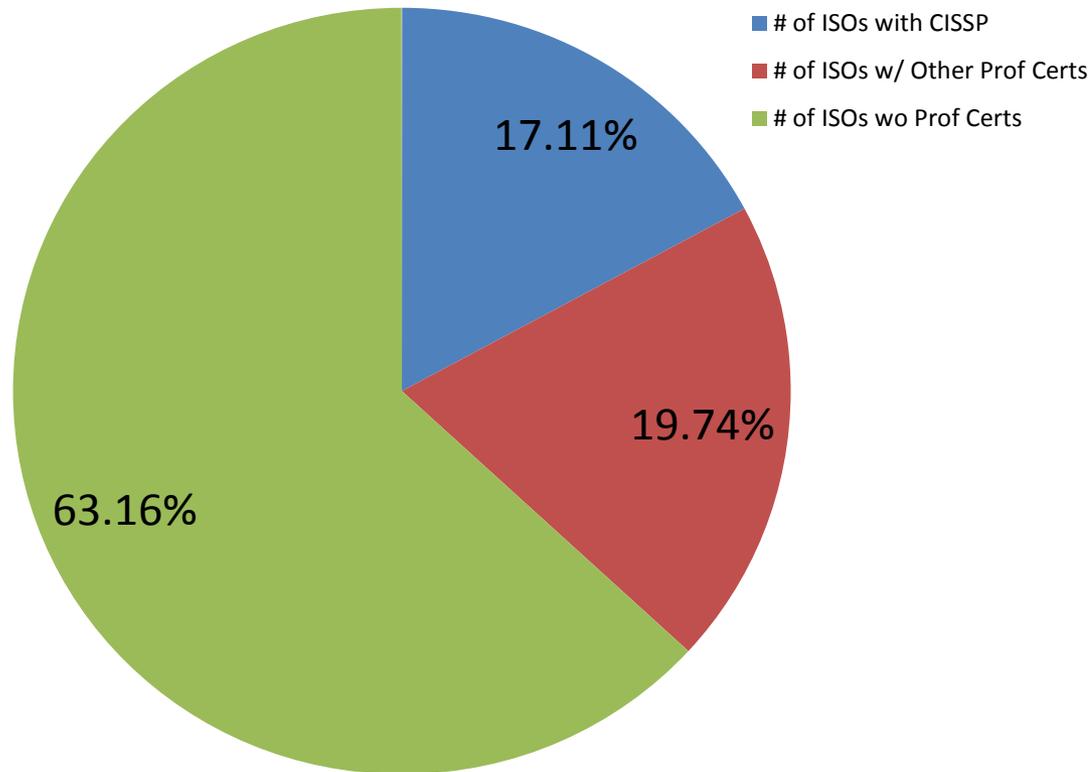
- Maintain for your own records, any documentation that indicates you have completed the activity. Include in your documentation, the name of the activity, the date, time, and hours claimed. You should also keep for your records, any certificates of completion, receipts, program outlines, agendas, brochures, handouts, etc. for any activity that you complete.
- You should maintain your own records of your participation in the activity for 3 years.
- You **do not** need to send any of this documentation to CSRSM, but it is possible, in some cases, that we or an auditor may ask or need to see it, so please maintain a personal file of this information.



Summary of Continuing Education Req's.

1. Agree to abide by the Commonwealth IT Security **Code of Ethics**
2. Attend any **mandatory ISOAG meetings** in the coming year
3. Attend **IS Orientation** at least once every 2 years
4. Obtain **20 hours of continuing education** in IT Security per year

Professionally Certified ISOs





In 2016 and Beyond

1. The importance of the ISO position at an agency cannot be overstated. Ensuring that all ISOs are adequately trained and prepared for this job are critically important to the overall security at an agency and for the commonwealth.
2. Therefore, we are looking to raise the bar on certification requirements for ISOs.
3. The CISSP is one of the oldest and most recognized standards in the IT security certification industry.
4. We would like for every agency ISO to obtain an industry recognized IT security certification, such as the CISSP.
5. We have requested funding to allow us to conduct boot camp type training sessions for the CISSP exam for all ISOs in the commonwealth.
6. We'll keep you posted as to how this initiative is progressing.



Questions on ISO Certification?



Ed Miller

VITA

Commonwealth Security & Risk Management

804-416-6027

edward.miller@vita.virginia.gov



Future ISOAG

November 4, 1:00 - 4:00 pm @ CESC
Speaker: Eric Bowlin, Deloitte

ISOAG meets the 1st Wednesday of each month in 2015

ADJOURN

THANK YOU FOR ATTENDING

