



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

November 5, 2014



ISOAG November 2014 Agenda

- | | |
|---|-----------------------------------|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. How to Keep Your Personal and Business Mobile Devices Protected | Mike Zirkle, Verizon |
| III. 2014 COV Security Annual Report | Mike Watson, VITA |
| IV. ISO Hollywood Squares | Ed Miller, VITA |
| V. Upcoming Events | Bob Baskette/Michael Watson, VITA |
| VI. Partner/Operation Update | Bob Baskette, VITA |



Mike Zirkle, Associate Director of Public
Sector Marketing
Verizon Enterprise Solutions
“How to Keep your Personal and Business
Mobile Devices Protected”

November 5, 2014



Mobile Security

Mike Zirkle

Associate Director Public Sector Marketing

5 November 2014



Proprietary Statement

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

© 2013 Verizon. All Rights Reserved. The Verizon name and logo and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

Mobility is the Growing Trend

Devices



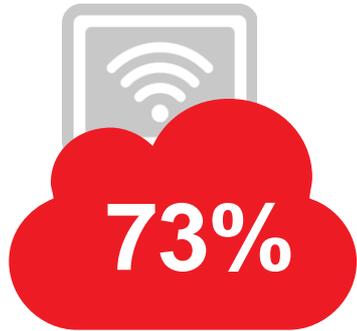
Workers



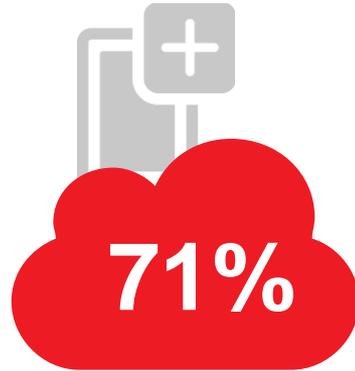
Machines



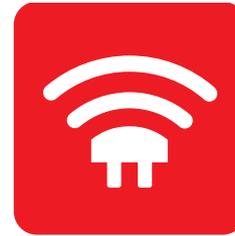
Mobility is the Growing Trend



Enterprise employees work remotely at least part of the time



Organizations are using or planning to use custom mobile applications



Connected devices are expected to exceed world population in 2016.



Monthly mobile data traffic is expected to increase 13x by 2017.

71%

OF SECURITY BREACHES
TARGETED USER DEVICES



52%

OF SUCCESSFUL ATTACKS
USED SOME FORM OF HACKING



40%

OF ATTACKS
INCORPORATED MALWARE



75%

OF BREACHES ARE CONSIDERED
OPPORTUNISTIC ATTACKS.



The entryways for potential attacks include:

- + Employees co-mingling corporate and third-party applications on the same device.
- + Personal and corporate email accounts shared on the same device and employees exchanging information between the two.
- + Employees visiting sites where they encounter malware or malicious threats.
- + The use of employee-owned devices to access enterprise resources and information.



Defense Mobility Guidance

On June 15, 2012, DoD CIO rolled out its Mobile Device Strategy meant to maximize the potential uses of mobile devices, and focuses on three key areas: wireless infrastructure, mobile devices and mobile applications



Goal 1

Advance and Evolve the DoD Information Enterprise Infrastructure to Support Mobile Devices

Evolve Spectrum Management, Expand Infrastructure to support wireless capabilities, establish a mobile device security architecture

Goal 2

Institute Mobile Device Policies and Standards

Develop mobile device policy and standards, establish a mobile device management service, educate and train mobile device users

Goal 3

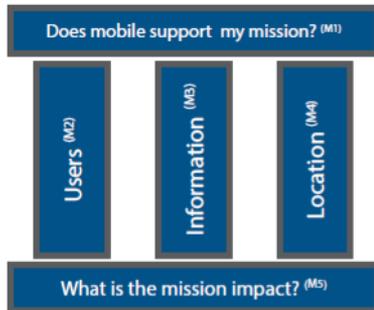
Promote the Development and Use of DoD Mobile and Web-Enabled Applications

Establish a common mobile application development framework, Institute a mobile application certification process, Provide an enterprise mobile application environment, “Web-enable” IT capabilities for mobile device support

Federal Mobility Guidance

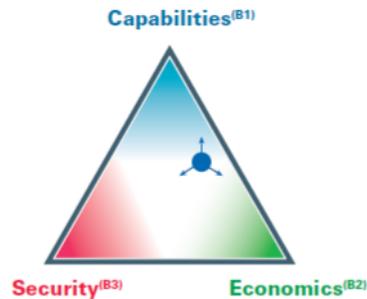
Mission Requirements

How would mobile support the mission?



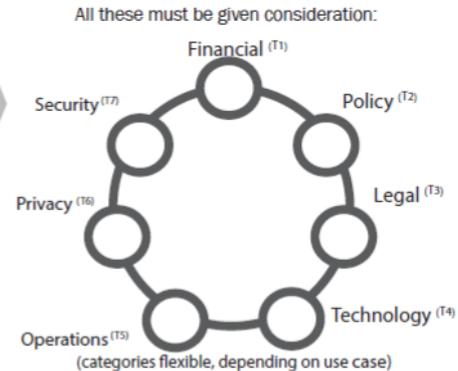
Decision Balancing

How shall I weight the dimensions?



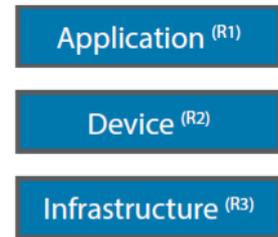
Risk-Based Tailoring

How will I cover the various risks?



Results

Selecting the right solution



1. Mobile Computing Decision Framework, CIO Council Published 23 May 2012: <https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Decision-Framework.pdf>



The Federal mobile security baseline maps the NIST SP 800-53 Rev 4 moderate baseline to the controls tailored for mobility¹



NIST 800-53 Controls		Rationale for Addition or Removal		Allocation to Seven Types of Risk							Reason for Risk Type Allocation			
No.	Name	NIST SP 800-53 Rev 4	MDM	MAM	COMMENTS	Finance	Policy	Legal	Technology	Operations	Privacy	Security	Reason*	
ID	TITLE (NIST SP 800-53 Rev 4)	W	M	M		T1	T2	T3	T4	T5	T6	T7		
1	AC-1 Access Control Policy and Procedures	X	AC-1	AC-1			Policy	Legal			Privacy		ISO/IEC 27001 (Annex A) Controls: §A.15.1.1, Identification of Applicable Legislation.	
2	AC-2 Account Management	X	AC-2		Controls in NIST Baseline and MDM Overlay				Technology		Privacy		Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account - authorization is sometimes given based on what access to PII is appropriate.	
3	AC-2(1) Account Management Automated System Account Management	X	AC-2(1)	AC-2						Technology				
4	AC-2(2) Account Management Removal of Temporary / Emergency Accounts	X	(-)	(-)		No temporary accounts on the MDM server, so requirement is essentially N/A.								
5	AC-2(3) Account Account		AC-2(3)		Control Removed from NIST Baseline for MDM Overlay				Technology					
20	AC-3(4) Access Enforcement Discretionary Access Control		+ AC-3(4)			Controls Added to NIST Baseline for MDM Overlay				Technology			Security	Add only for multiple-user devices NOTE: If the mobile device operating system is a single-user system, upon which the user does *not* have administrator privileges, discretionary access control requirements can reasonably be tailored out of the baseline for specified use cases.
21	AC-3(5) Access Enforcement Security-Relevant Information		+ AC-3(5)							Technology			Security	

1. Government Mobile and Wireless Security Baseline, CIO Council Published 23 May 2012; <https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf>

Security Requirements Guides – Mobility

SRGs represent an intermediate step between Control Correlation Identifiers (CCIs) and STIGs. CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in policy, such as those originating in Department of Defense Instruction (DoDI) 8500.2 and National Institute of Standards and Technology (NIST) Special Publication 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product's technology area



The Mobile Operating System (MOS) SRG addresses security for the operating system installed on mobile devices, primarily in the smartphone and tablet form factor.



The Mobile Device Management SRG addresses centralized management of mobile operating systems and applications. The MDM SRG also covers aspects of device integrity verification and enterprise email.



The Mobile Applications SRG addresses the security of applications that run on mobile OS. The IA controls in the Mobile Applications SRG also map to the IA controls in the core Applications SRG.



The Mobile Policy SRG addresses management, operational, personnel, and physical security controls related to mobile devices. The IA controls in the Mobile Policy SRG map to the IA controls in the core Policy SRG.



SRG Example

The MDM server must have the capability to enable and disable a managed mobile device.

Group ID (Vulid): V-36170

Group Title: SRG-APP-134-MDM-166-MDM

Rule ID: SV-47574r1_rule

Severity: CAT I

Rule Version (STIG-ID): SRG-APP-134-MDM-166-MDM

Vulnerability Discussion: Under some conditions, a compromised device represents a threat to other computing resources on the network. For example, a compromised device may attempt to conduct a denial of service attack on other devices, or may be executing a mechanism to spread malware before a countermeasure has been put in place. In these situations, it is critical that an MDM server be able to disable the device to protect other network resources.

Check Content: Review the MDM server configuration to ensure the MDM server can enable and disable a managed mobile device. If this function is not present, this is a finding.

Fix Text: Configure the MDM server so it can enable and disable a managed mobile device.

Steps to a Successful Mobile Strategy

- Business needs and goals
- Security and mobile device management
- Deployment
- Support
- Positioning for the future



**BUSINESS
NEEDS**



**SECURITY AND
MOBILE DEVICE
MANAGEMENT**



DEPLOYMENT



SUPPORT



EVOLUTION



Verizon Mobility Framework

A Platform That Supports a Mobility Ecosystem



DEVICES

- Smartphones
- Tablets
- Laptops
- Containerization
- Certificate Mgmt
- VPN
- Corporate
- Employee-owned Device



APPLICATIONS

- Deployment
- Management
- Application Wrapping
- Enterprise App Catalog
- Web Apps



CONTENT

- Mobile E-mail
- Secure Browser
- Device Encryption
- Secure Documents
 - Viewing
 - Storage



ENABLED BY VERIZON

- Network Services
 - Fixed
 - Mobile
- M2M
- App Development
- Vertical Applications



Verizon deploys a multipronged strategy for network security





Questions





2014 Commonwealth Security Annual Report

Michael Watson, CISO

November 5, 2014



§ 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.



Detailed Agency Information Security - 2014 Overall Security Program Scores

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

All ISOs must be appointed by their Agency Head. Once formally assigned , ISOs must complete the ISO education requirement by taking one of the two paths described below.

Steps to obtain COV ISO Certification for those who have a professional security certification:

- Possession of recognized professional IT Security Certification CISSP, CISM, CISA, SANS (others to be determined)
- VITA Training, Attend Information Security Orientation training
- ISO Academy, Successful completion of at least one course hour in the KC ISO Academy per year.
- ISOAG attendance, Attend the mandatory October 2014 ISOAG meeting.
- Maintain compliance with the continuing educational requirements of the professional IT security certification body.

Steps to obtain COV ISO Certification for those who do not have a professional security certification:

- VITA Training, attend Information Security Orientation training.
- ISO Academy, successful completion of at least 3 course hours per year in the KC ISO Academy.
- ISOAG attendance, attend the mandatory October 2013 ISOAG meeting.

Continuing Education Requirements in 2014 for ISOs that have already obtained the ISO Certification:

- Agree to the Commonwealth IT Security Code of Ethics
- Attend any mandatory ISOAG meetings each year
- Attend IS Orientation once every 2 years
- Obtain 20 hours of continuing education credit



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

Audit Plan Status: The Agency Head has submitted an IT Security Audit Plan for the period of fiscal year (FY) 2014-2015 or 2014-2016 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2014, Audit Plans submitted shall reflect FY 2015-2016)

- Pass - Plan is up to date and meets the criteria
- Fail - The IT Security Audit Plan on file does is not up to date and or does not meet the criteria

Current Percentage of Audits Received: The percentage of Audit Reports received per the IT Security Audit Plan in the current year.

- % - Submitted % of Audits Received for current year, based on Audit Plan
- N/A - Not Applicable due to no audits planned for the year
- N/C - Non Compliant due to no current Audit Plan in place

Percentage of Quarterly Updates Received in 2014:

- % - Submitted % of QUs for all open findings per CAPs submitted
- N/A - No Security Audits scheduled to be completed



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

3 Year Audit Obligation: This is the percent of sensitive systems audited within the last 3 years. The sensitive system list is validated against the Commonwealth Enterprise Technology Repository (CETR). For agencies required to submit to CETR, audits are not complete unless the sensitive system subject to the audit can be identified within CETR. 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."

- N/C - Values cannot be calculated due to lack of current Audit Plan
- N/A - No Sensitive Systems to be audited

Business Impact Analysis Status: The Business Impact Analysis (BIA) has been provided by the agency. [To be considered complete all applications must follow the requirements of the IT Risk Management Standard \(SEC520-00, 3.2.2\)](#) Please note: If you have already submitted a BIA in 2012 or 2013 and have no changes, let Commonwealth Security know so you get credit for reviewing and having a current BIA on file.

- Pass – BIA is complete
- Fail – BIA has not been submitted or is incomplete
- Incomplete – Agency has submitted a BIA that is currently under review or required additional information.

BIA shall, at a minimum, identify:

- Business function name and owner
- Date BIA Completed and name of person that completed the BIA
- Primary objective of the business function
- Customers of the function (internal customers, Commonwealth Agency customers, government entity customers, public customers)



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

BIA shall, at a minimum, identify (con't):

- Identify whether the functions are mission essential
- Identify IT systems that the business functions rely on
- Description of the data used by the function, including the source, destination, and sensitivity
- Identify the recovery time objective (RTO)
- Identify the recovery point objective
- Rate the impact of non-performance of the function for:
 - Confidentiality – Impact on customer service, public perception/trust, impact on sensitive data
 - Integrity – Impact on finance, legality, regulation, customer service, public perception/trust
 - Availability – Impact on life, safety, customer service, public perception/trust, finance, recovery time objective, recovery point objective

Risk Assessment Plan Status: The Agency Head has submitted an IT Risk Assessment Plan for the period of fiscal year (FY) 2014-2015 or 2014-2016 for systems classified as sensitive based on confidentiality, integrity or availability (*Note: after July 1, 2014, Audit Plans submitted shall reflect FY 2015-2016*)

- Pass - Plan is up to date and meets the criteria
- Fail - The IT risk assessment plan on file does is not up to date and or does not meet the criteria



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

3 Year Risk Assessment Obligation: The percentage of Risk Assessment obligation met is calculated based on the percentage of sensitive systems that have had risk assessments conducted and submitted to Commonwealth Security and Risk Management within the last three years. The risk assessment date is assigned to each sensitive system and calculated as a percentage of total sensitive systems identified within the agency. For agencies required to submit to CETR, Risk assessments are not complete unless the sensitive system subject to the assessment can be identified within CETR. [The Risk Assessment information reported must follow the requirements of the IT Risk Management Standard \(SEC520-00, 3.3.3\).](#)

Pending CETR - Indicates the values cannot be calculated until the agency reconciles their audit plan system names with the CETR database.

Please Note: A status of "Pending Agency CETR Reconciliation" will change to "Failed" as of December 16, 2014. Again, please note that the closing date for the 2013 Commonwealth of Virginia Information Security Annual Report is **December 31, 2014.**



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

IDS Reports Submitted – Agencies shall provide Intrusion Detection System Reports to VITA at the end of each quarter. IDS reports should provide the following information:

1. Name of Agency
2. Date Range for the Report (example: Jan 1st 2013 – March 31st, 2013)
3. Total number of attacks per month (example: Jan 2013 = 1,000,000, Feb 2013=1,500,000, March 2013= 1,250,000)
4. Total number of high attacks per month
5. Total number of medium attacks per month
6. Total number of low attacks per month
7. Top 10 high attacks & number of attacks seen (example: SSH Brute Force, total: 100 attacks)
8. Top 10 Source IPs
9. Top 10 Destination IPs
10. Top 10 countries of origin of attacks with percentages per month (example: Jan 2013: US – 80%, China =4%, Russia = 3%, Canada = 3%, U.K. = 3%, India=2%, Brazil=2%, Germany=2%, Ireland=2%, Sweden=2%)
11. Top 10 types of attacks (example: Denial of Service, Privilege Escalation)
12. Top 10 inbound attacks by protocol/service/port (http/www/80)
13. Top 10 outbound attacks by protocol/service/port (http/www/80)



Detailed Agency Information Security - 2014 Overall Security Program Scores Con't

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
XYZ			N/A	50%	50%		N/C	Pending		

Vulnerability Scans Results Reported - For each IT system classified as sensitive, the data owning agency shall:

1. Conduct a vulnerability scan of the information system and hosted applications at least once every 90-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported.
2. Document and report vulnerabilities and risks identified in the vulnerability scans and related remedial actions to CSRM once every 90-days.

*Note: If no vulnerabilities were identified in a vulnerability scan, Agency must notify CISO that the vulnerability scan was conducted and there were no findings.

**Note: If VITA is an agency's service provider for performing the required vulnerability scans on an agency's behalf, those results are automatically reported to the CISO on the agency's behalf.

Vulnerability scans must be reported to the CISO using the Risk Assessment and Risk Treatment Plan templates



Secretariat: Administration

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
CB			N/C	N/A	N/C		N/C			
DGS			100%	0%	100%		N/C			
DHRM			0%	N/A	0%		N/C			
ELECT			0%	N/A	0%		0%	Pending		



Secretariat: Agriculture & Forestry

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DOF			100%	33%	24%		N/C	Pending		
VDACS			100%	85%	100%		N/C			



Secretariat: Commerce & Trade

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
BOA			N/A	N/A	100%		N/C			
DHCD			0%	0%	20%		N/C			
DMME			N/C	0%	N/C		N/C			
DOLI			N/C	N/A	N/C		N/C			
DPOR			N/A	100%	100%		N/C	Pending		
SBSD			N/C	N/A	N/C		N/C			
TIC			0%	N/A	N/A		N/C			
VEC			0%	75%	67%		N/C			
VEDP			N/A	N/A	0%		N/C			
VRA			N/C	N/A	N/C		N/C			
VRC			N/A	N/A	N/A		N/C			



Secretariat: Education

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DOE	●	●	0%	N/A	24%	●	N/C	●	●	●
FCMV	●	●	N/A	N/A	N/A	●	N/C	●	●	●
GH	●	●	N/C	N/A	N/C	●	N/C	●	●	●
JYF	●	●	N/A	N/A	17%	●	N/C	●	●	●
LVA	●	●	0%	N/A	67%	●	N/C	●	●	●
NSU	●	●	50%	N/A	35%	●	N/C	●	●	●
RBC	●	●	20%	N/A	50%	●	N/C	●	●	●
SCHEV	●	●	0%	N/A	0%	●	N/C	●	●	●
SMV	●	●	N/A	N/A	0%	●	N/C	●	●	●
SVHEC	●	●	N/A	N/A	N/A	●	N/C	●	●	●
VCA	●	●	N/A	N/A	N/A	●	N/C	●	●	●
VMFA	●	●	N/C	0%	N/C	●	N/C	●	●	●
VSDB	●	●	N/C	N/A	N/C	●	N/C	●	●	●
VSU	●	●	83%	62%	63%	●	N/C	Pending	●	●



Executive

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
GOV			0%	N/A	0%		N/C			
OAG			N/C	N/A	N/C		N/C			
OSIG			N/A	N/A	N/A		N/C	Pending		



Secretariat: Finance

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DOA			0%	0%	53%		N/C			
DPB			N/A	N/A	0%		0%	Pending		
TAX			42%	50%	89%		N/C			
TD			0%	N/A	0%		N/C			



Secretariat: Health & Human Resources

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
CSA			N/C	N/A	N/C		N/C			
DARS			50%	47%	79%		N/C			
DBHDS			N/C	N/A	N/C		N/C			
DHP			0%	N/A	50%		100%			
DMAS			20%	75%	84%		N/C			
DSS			0%	0%	6%		N/C			
VDH			75%	80%	71%		N/C			
VFHY			N/A	N/A	N/A		N/A			



Independent Branch Agencies

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
IDC			0%	0%	50%		N/C			
SCC			33%	80%	100%		N/C	Pending		
SLD			40%	0%	67%		N/C			
VCSP			0%	N/A	83%		N/C			
VRS			0%	36%	100%		N/C	Pending		
VWC			0%	0%	100%		N/C			



Secretariat: Natural Resources

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DCR			N/C	0%	N/C		N/C			
DEQ			0%	0%	83%		N/C			
DGIF			N/C	N/A	N/C		N/C			
DHR			0%	33%	N/A		N/A			
MRC			0%	N/A	100%		100%			
VMNH			N/A	N/A	0%		100%	Pending		



Secretariat: Public Safety

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
ABC			0%	79%	50%		N/C			
CASC			N/A	N/A	N/A		N/C			
DCJS			N/C	N/A	N/C		N/C			
DFP			N/C	N/A	N/C		N/C	Pending		
DFS			0%	N/A	75%		N/C			
DJJ			0%	100%	100%		N/C			
DMA			N/C	N/A	N/C		N/C			
DOC			33%	73%	90%		100%			
DVS			N/A	N/A	100%		100%			
VDEM			0%	N/A	0%		N/C			
VSP			100%	72%	60%		N/C			



Secretariat: Technology

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
IEIA			0%	N/A	0%		0%			
VITA			0%	75%	0%		N/C			



Secretariat: Transportation

Agency Acronym	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Business Impact Analysis Status	IDS Quarterly Reports	Vulnerability Scanning
DMV			N/C	25%	N/C		N/C			
DOAV			N/C	75%	N/C		N/C			
DRPT			N/C	N/A	N/C		N/C	Pending		
MVDB			N/C	N/A	N/C		N/C			
VDOT			11%	55%	76%		N/C			



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, 2014



Virginia Information Technologies Agency

ISO Hollywood Squares

Ed Miller, VITA

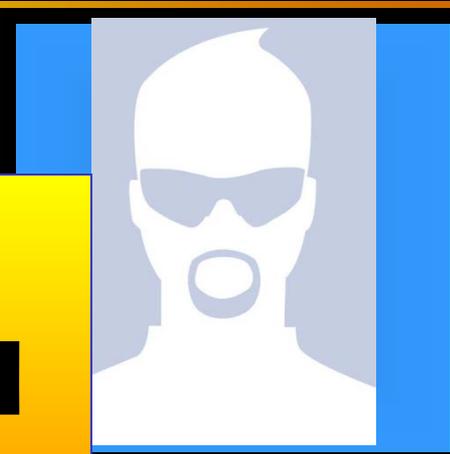
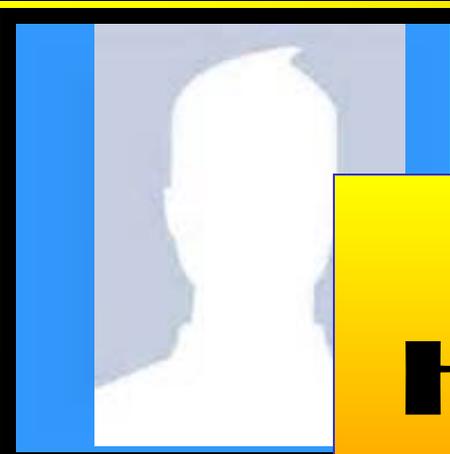
November 5, 2014

Welcome to...

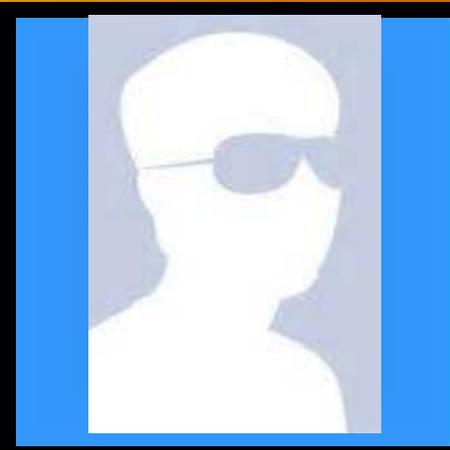
150 Hollywood Squares

Tic-Tac-Toe with X's and O's

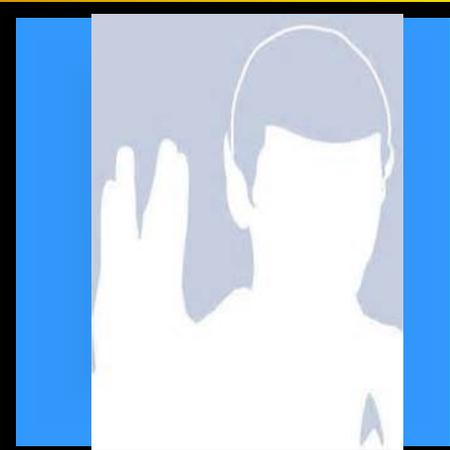
Your host: Ed Miller



**ISO
Hollywood
Squares!**



***Come see
which
Hollywood
ISOs will
play!***



ISO Hollywood Squares Rules

- Sort of the like the show & like Tic-Tac-Toe, but we play in teams
- Except, in the show, the celebrities sometimes gave wrong answers. In this version, the celebrity ISOs are **ALWAYS** right
- The team with the highest percentage of correct answers wins the square
- The team with 3 squares in a row wins the round
- Otherwise, the most squares in the round wins
- I have 3 rounds of questions.

ISO Hollywood Squares Rules

- **Blocks:** In real Hollywood Squares & real Tic-Tac-Toe, a “block” is a good move to prevent the other player from getting 3 squares in a row.
- However, in this version, it might not always be the smartest play.
- If your team is right, you get the block. But if your team is wrong, the other team wins the game.
- Clickers in use, speed scoring is turned on.



Virginia Information Technologies Agency

Upcoming Events





2015 Security Conference

"COVA Information Security Conference: Unifying the Business Enterprise"

April 2 & 3, 2015

Location: Crowne Plaza

2015 Security Conference



Keynote Speaker

April 2, 2014

Michael Fey

**Chief Technology Officer and General
Manager of Corporate Products for
Intel Security Group**

2015 Security Conference



Keynote Speaker

April 3, 2014

Karen Evans

National Director for the US Cyber Challenge (USCC).



IS Orientation

When: Thursday, December 4, 2014

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1223

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



Future ISOAG

December 3, 1:00 - 4:00 pm @ CESC

Speaker: TBA

ISOAG meets the 1st Wednesday of each month in 2014



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*

5 November, 2014



NORTHROP GRUMMAN



Partnership Q & A

Bob Baskette

5 November, 2014



NORTHROP GRUMMAN

ADJOURN

THANK YOU FOR ATTENDING

