



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

December 4, 2013



ISOAG December 2013 Agenda

- | | | |
|------|---|---|
| I. | Welcome & Opening Remarks | Mike Watson, VITA |
| II. | MACH 37 Project Demo's | David Ihrie, CIT |
| III. | UAC & DEP: Protection Mechanisms for Windows | Bob Baskette, VITA |
| IV. | 2013 Commonwealth Security Annual Report | Mike Watson, VITA |
| V. | Upcoming Events | Mike Watson, VITA |
| VI. | Partnership Update | Bob Baskette, VITA Michael Clark, NG |



PIERCE

**GLOBAL THREAT
INTELLIGENCE**

CORPORATE OVERVIEW

WWW.PIERCEGT.COM <Confidential>
PRESENTER: ROY STEPHAN, CEO

2013

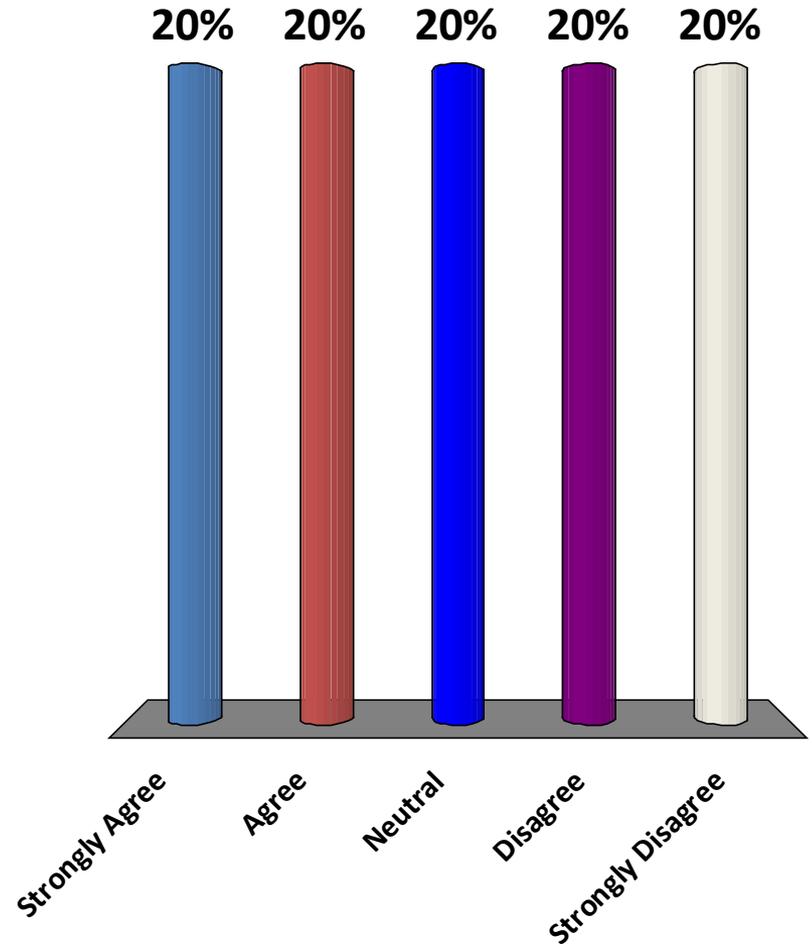
NOVEMBER 15

MACH37 Project Presentation

Individual Project Questions?

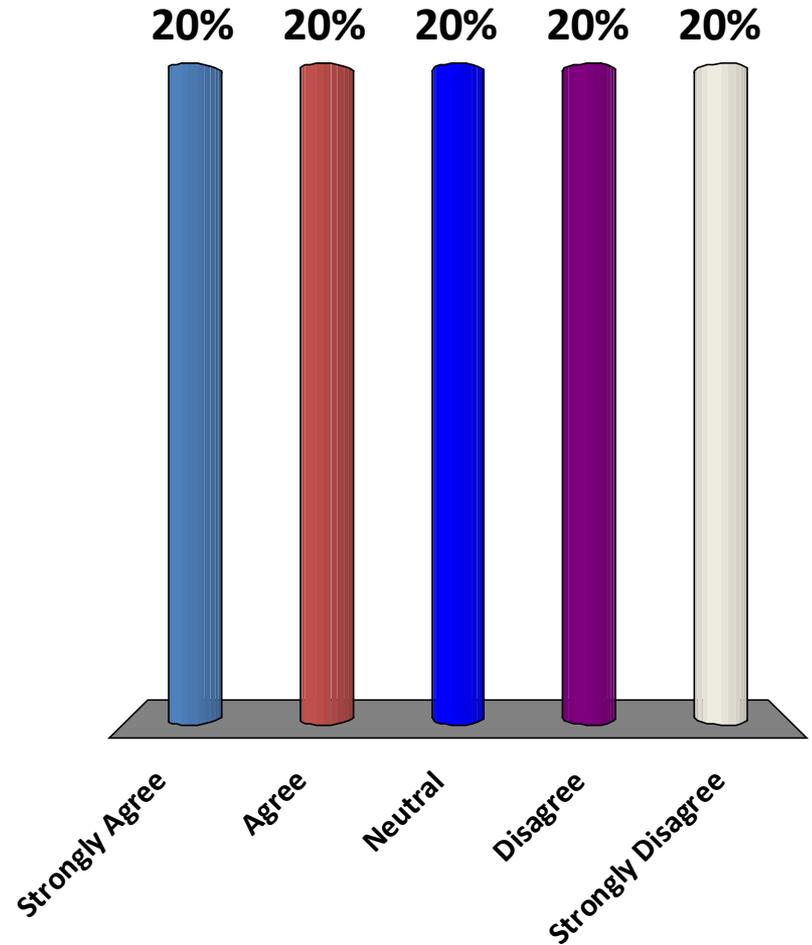
Do you feel the presenter explained their product thoroughly?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



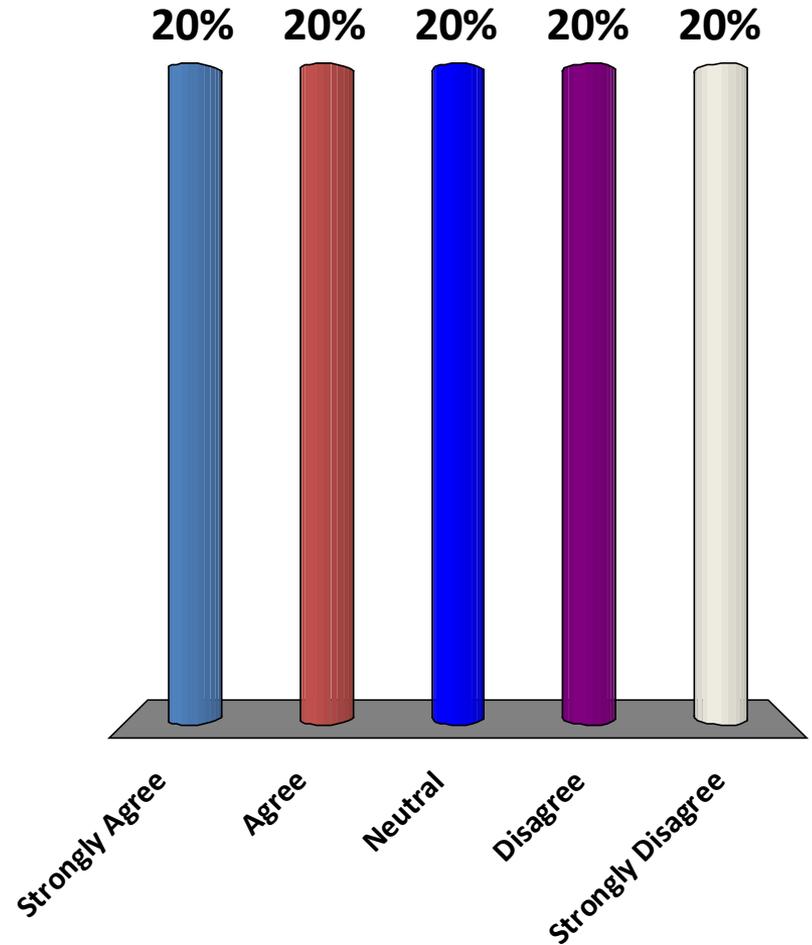
Do you think you this product will provide benefit directly to your environment?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



CONATIX *Reinventing Business Research*

Virginia ISO

4 December 2013

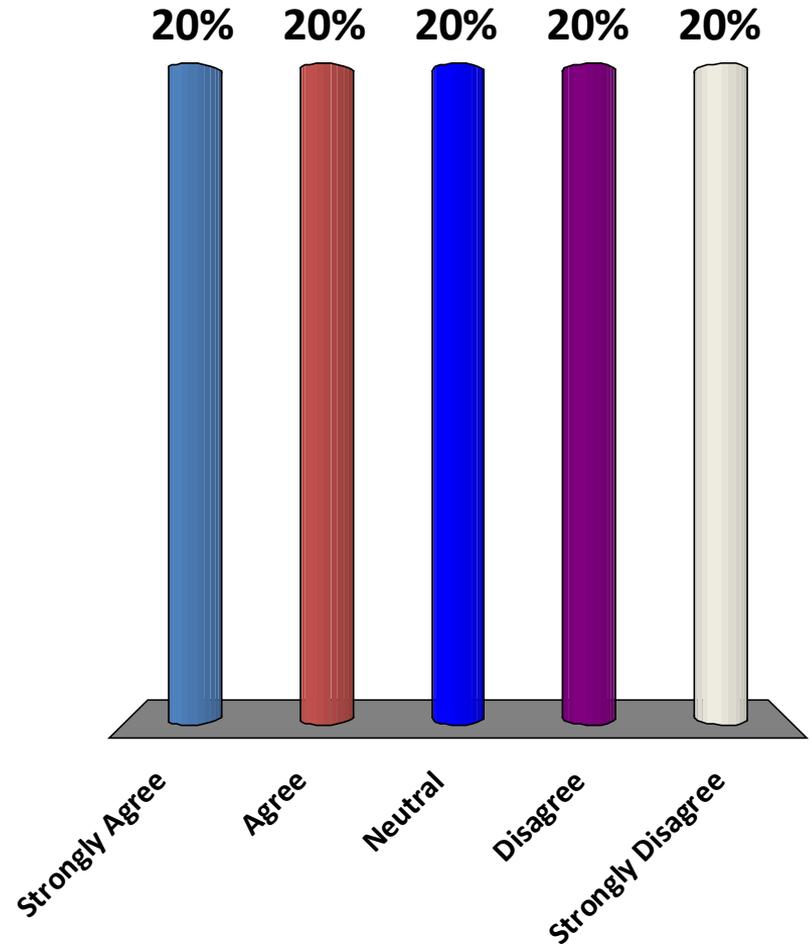
CEO: David Lehrer | Operations: Johann Quassowski
1-571-425-8705 | team@conatix.com

MACH37 Project Presentation

Individual Project Questions?

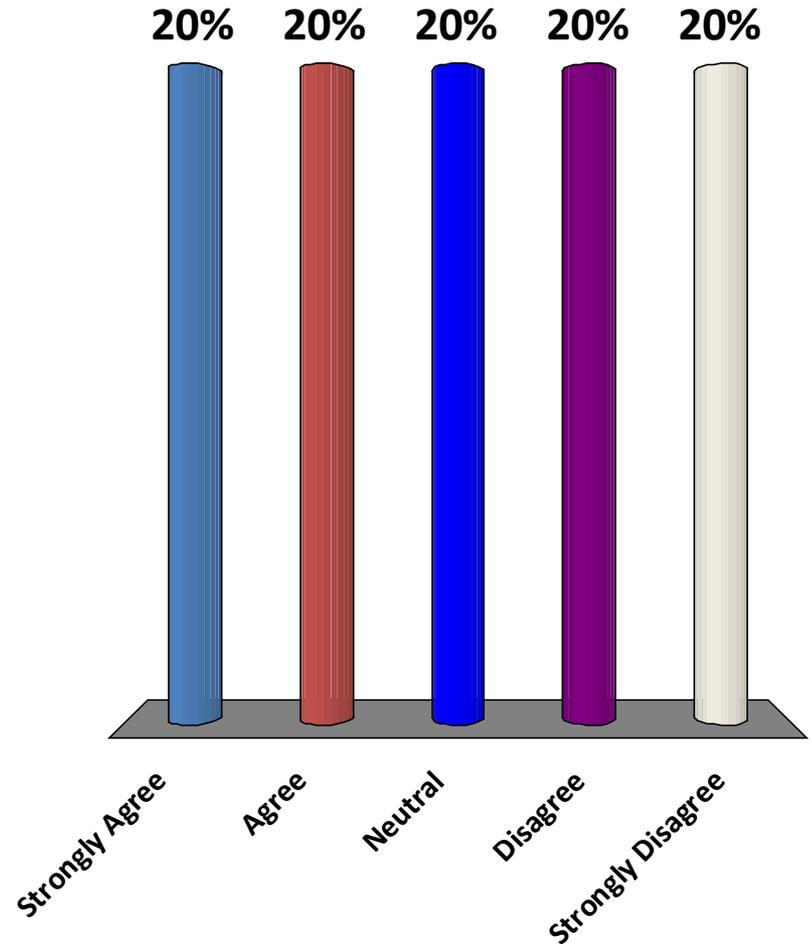
Do you feel the presenter explained their product thoroughly?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



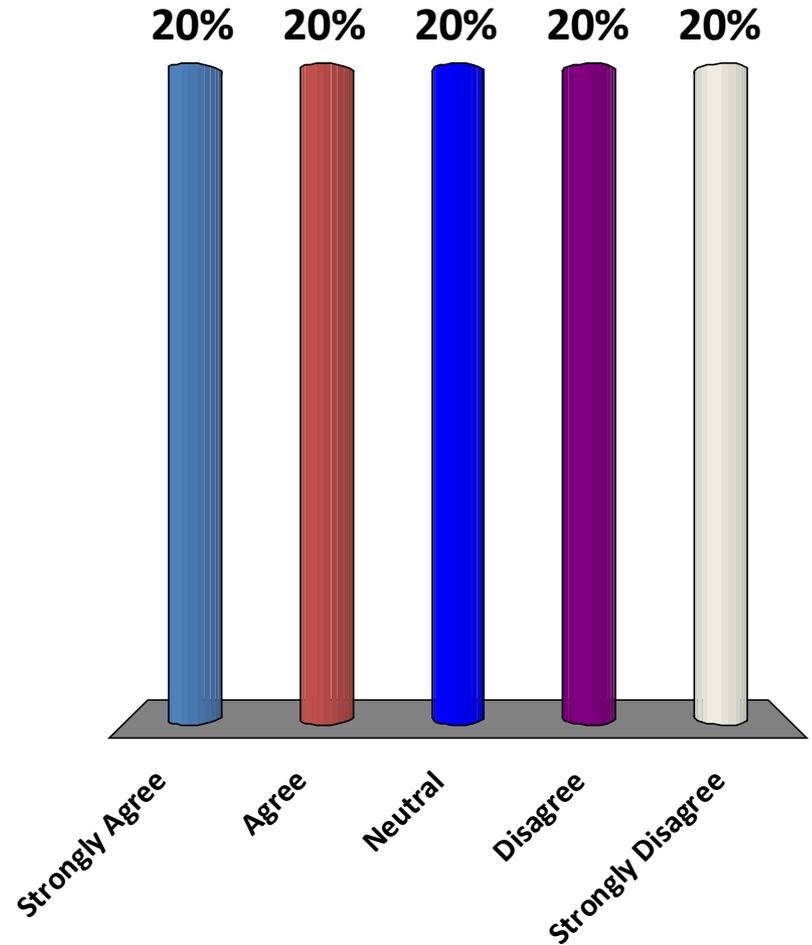
Do you think you this product will provide benefit directly to your environment?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree





SIKERNES
RISK MANAGEMENT

CERTAINTY ♦ PEACE OF MIND ♦ CONFIDENCE

Next Generation of Vulnerability & Risk Management

Ethan Allen, CEO

415.902.0516

eeallen@sikernes.com

Roderick Flores, CTO

505.401.1412

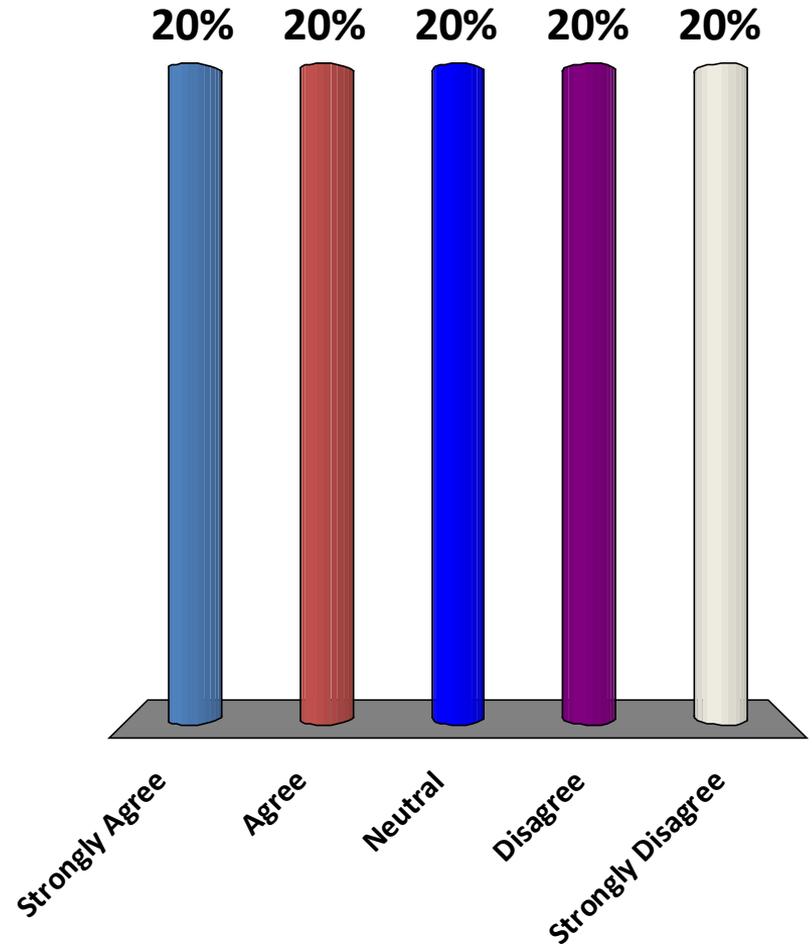
raflores@sikernes.com

MACH37 Project Presentation

Individual Project Questions?

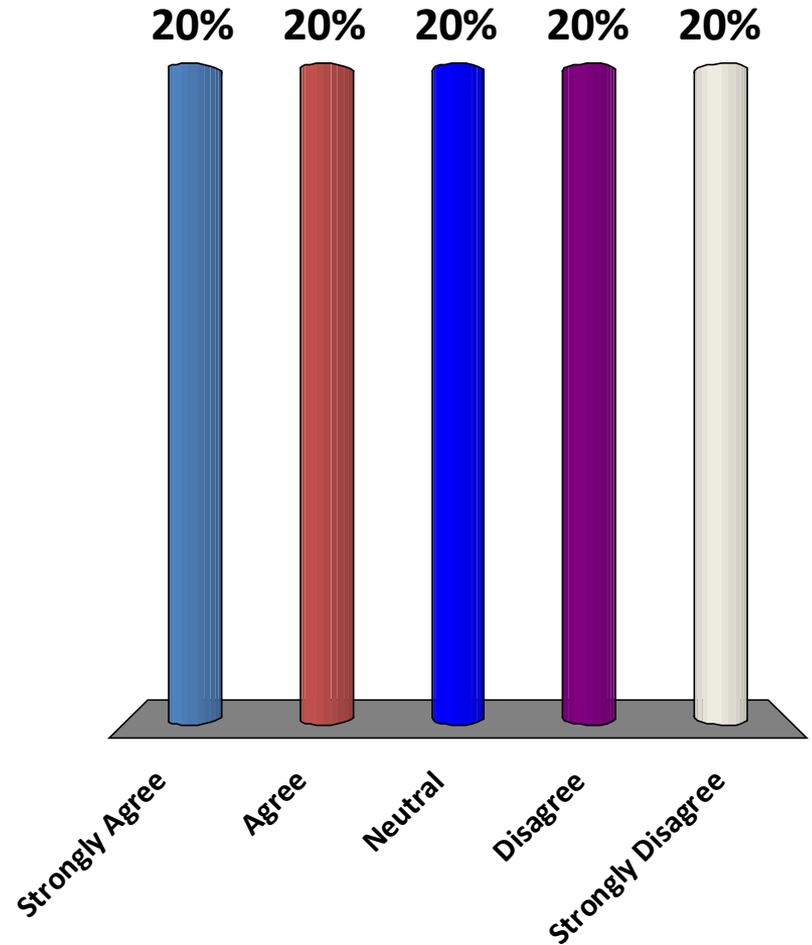
Do you feel the presenter explained their product thoroughly?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



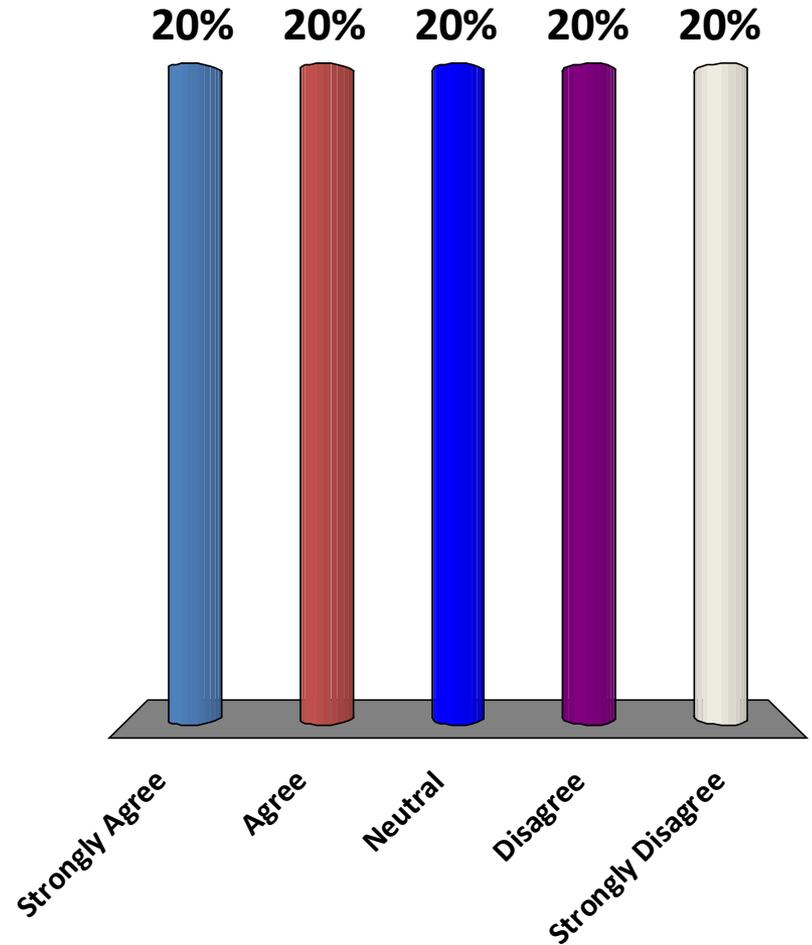
Do you think you this product will provide benefit directly to your environment?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree





CyberMerlin™

Key Cybersecurity, Inc.
17959 Dumfries Shopping Center Suite B
Dumfries, VA 22026-2490
703.402.2542

Shawn Key
CEO, President
skey@keycybersecurity.com

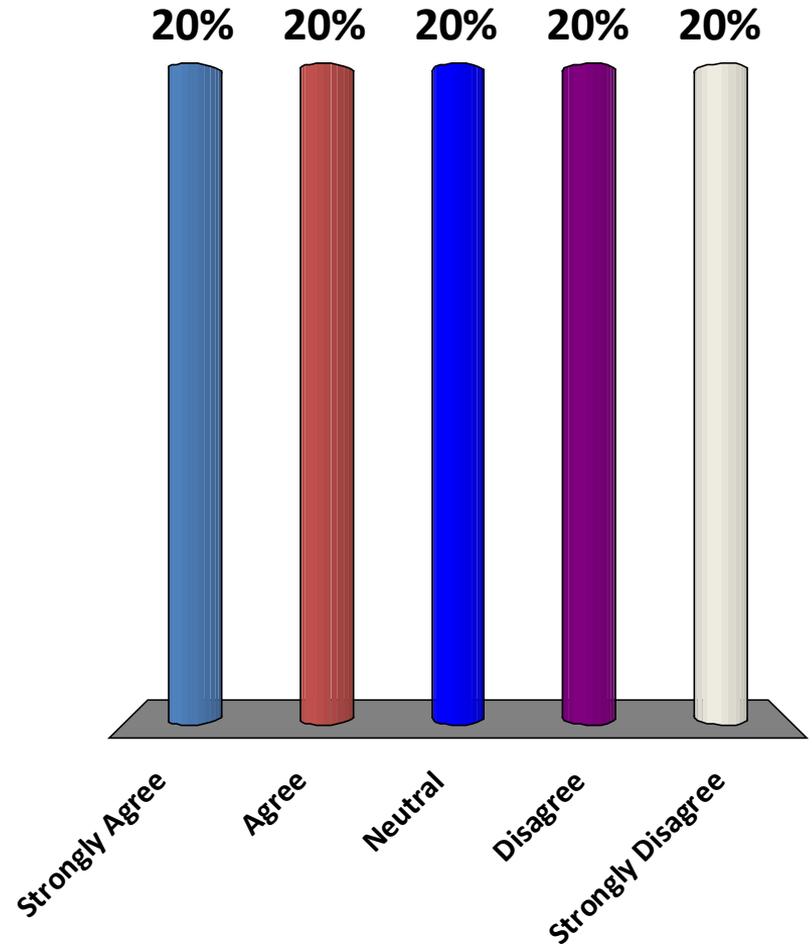


MACH37 Project Presentation

Individual Project Questions?

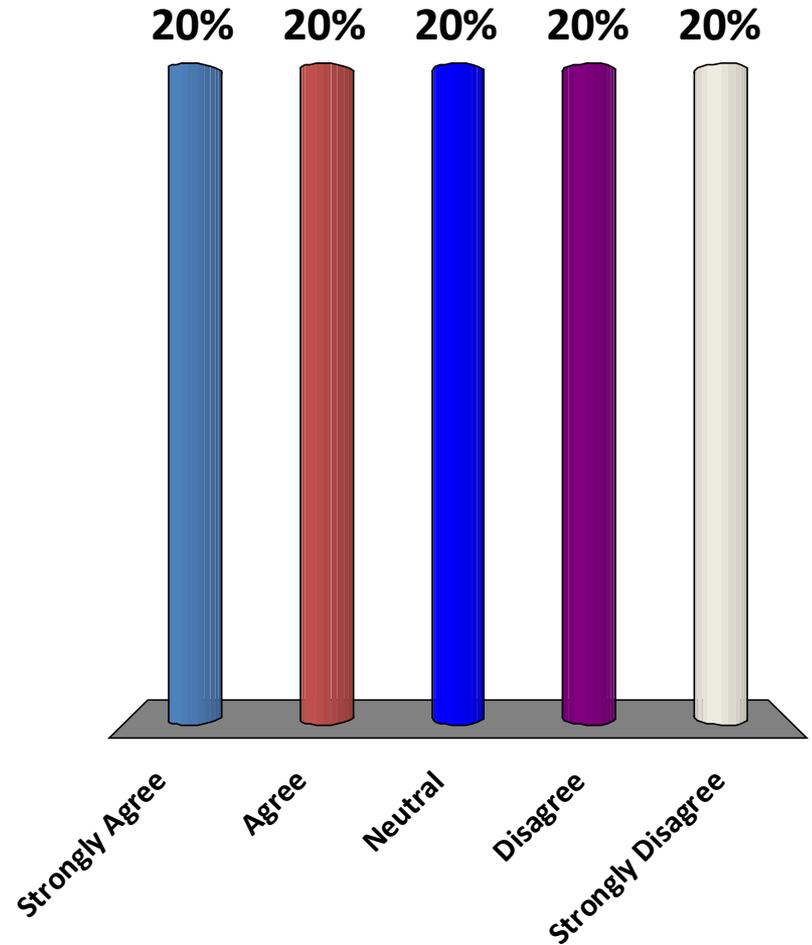
Do you feel the presenter explained their product thoroughly?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



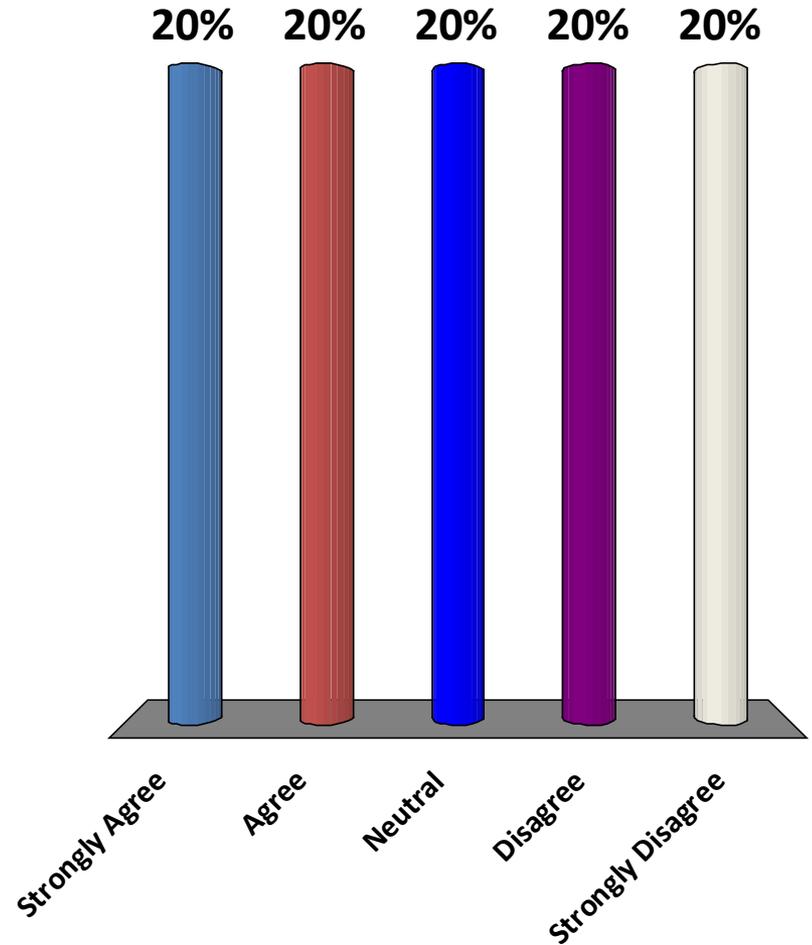
Do you think you this product will provide benefit directly to your environment?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



**Mobile
System**



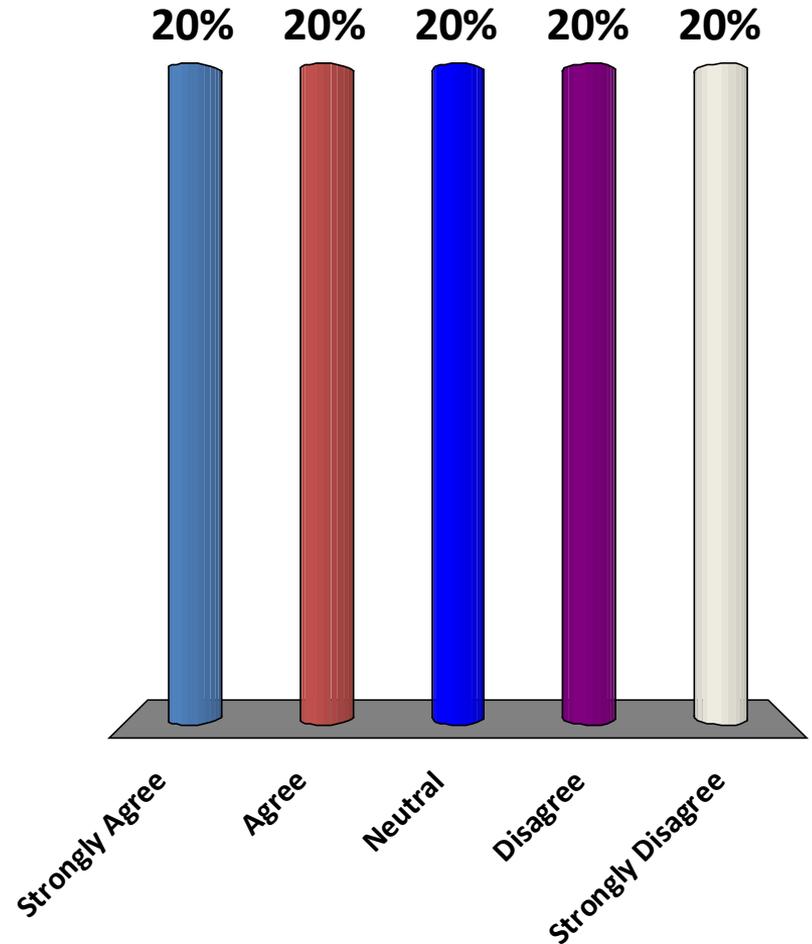
Enterprise Mobile Security

MACH37 Project Presentation

Individual Project Questions?

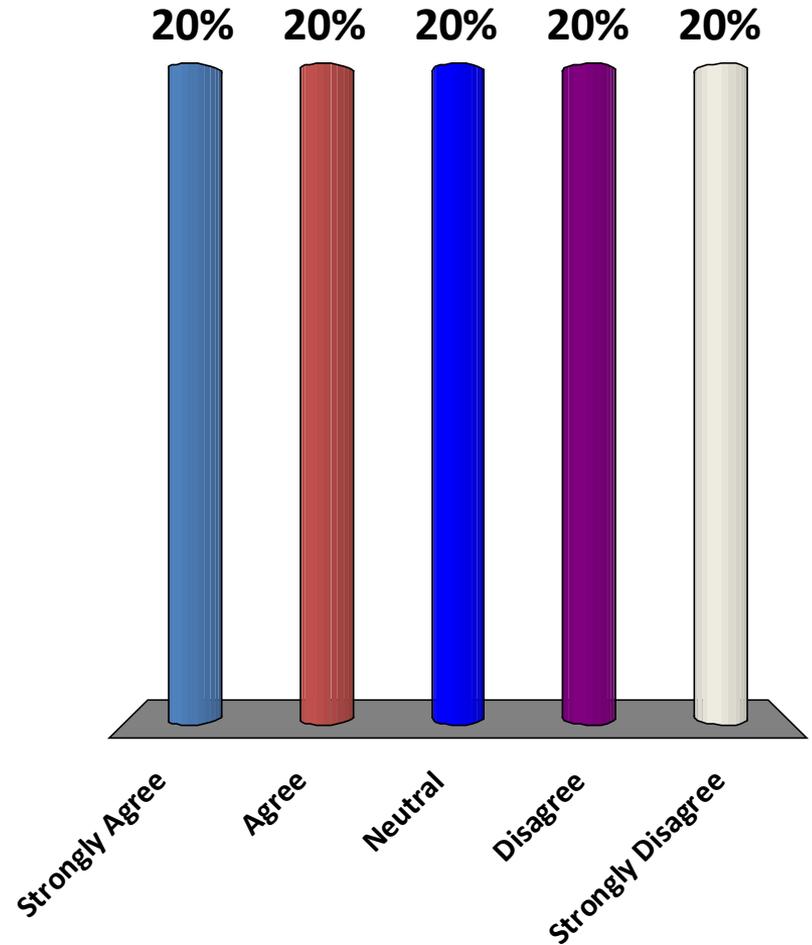
Do you feel the presenter explained their product thoroughly?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



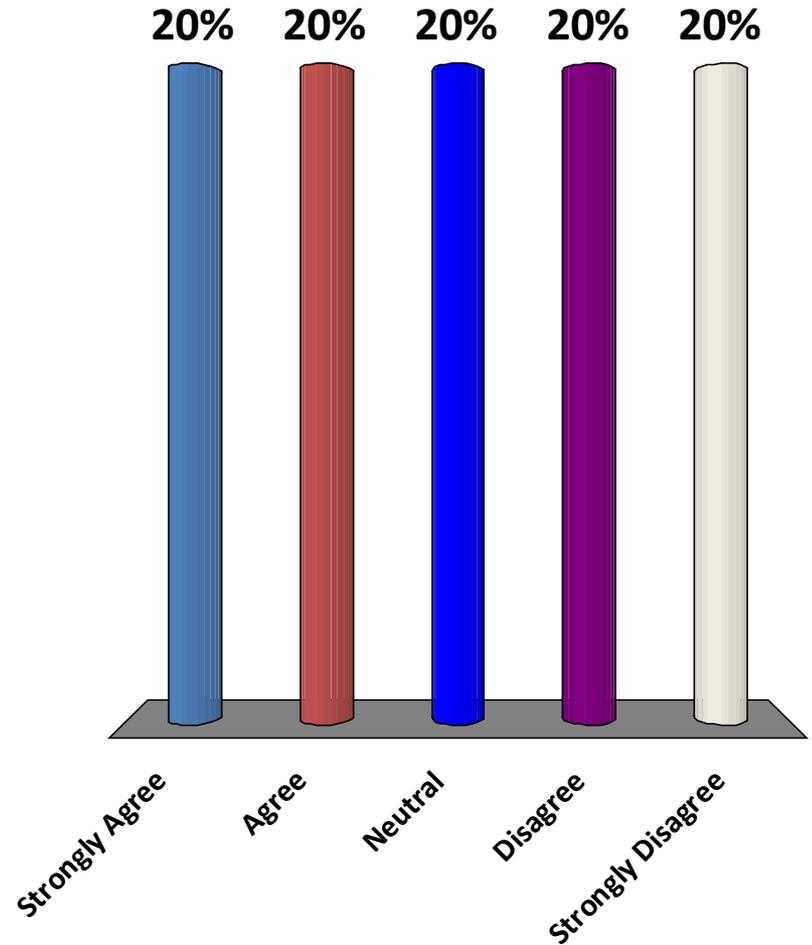
Do you think you this product will provide benefit directly to your environment?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree

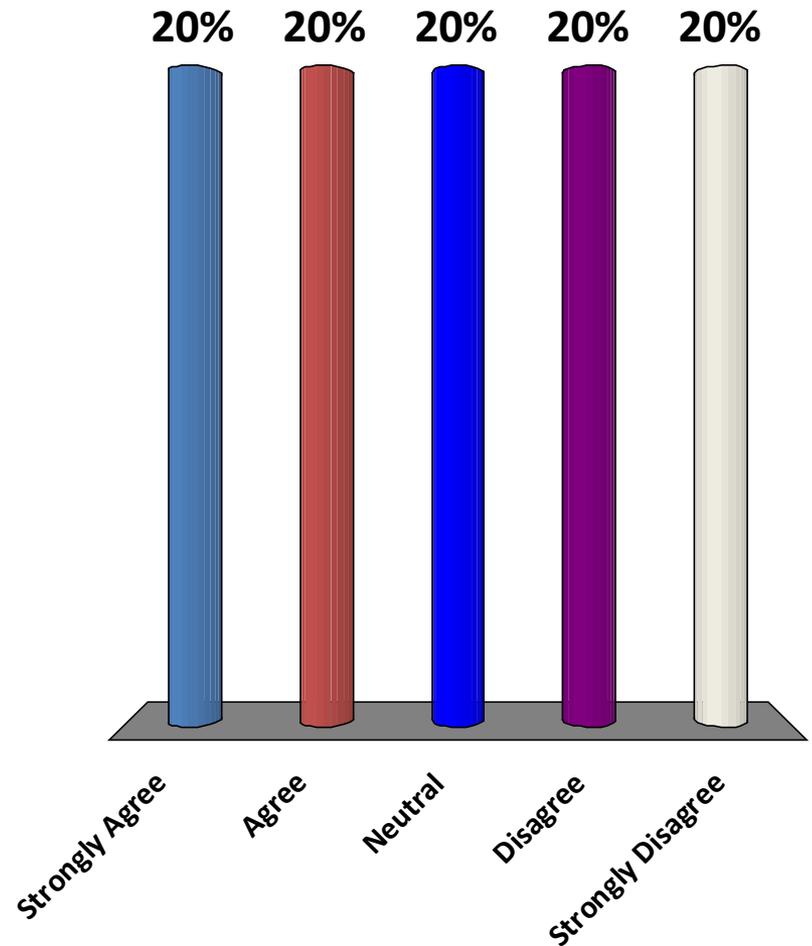


MACH37 Project Presentations

Summary Questions

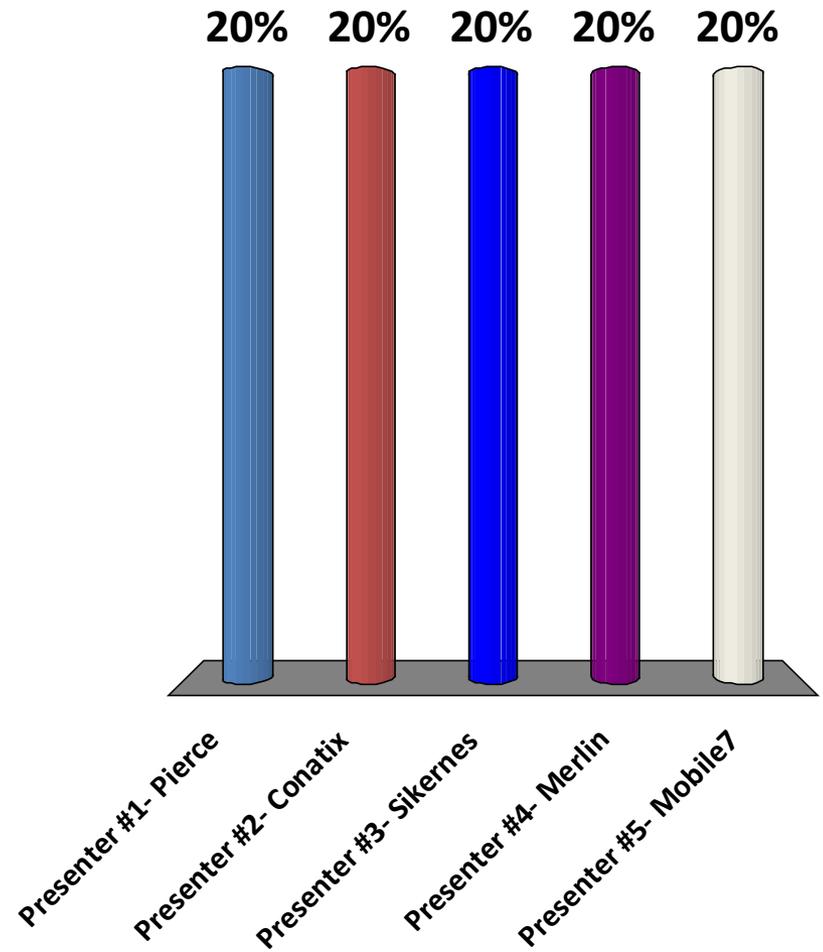
Do you feel you received enough detail about the products and/or services to decide whether to invest in it or not?

- A. Strongly Agree
- B. Agree
- C. Neutral
- D. Disagree
- E. Strongly Disagree



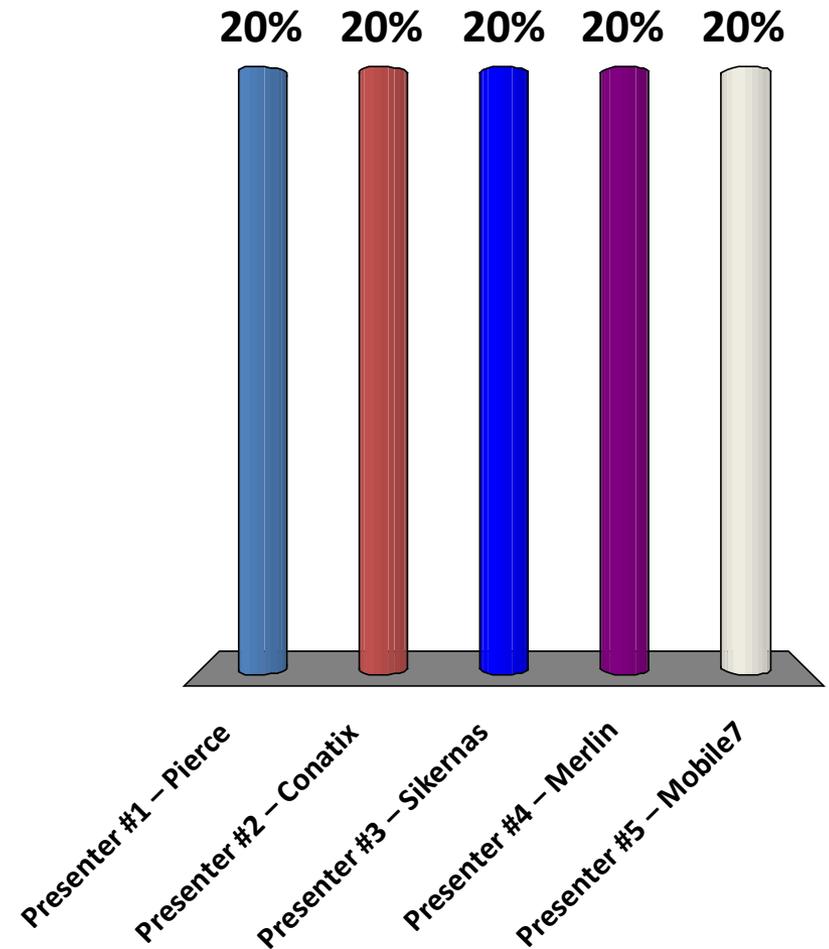
Pick one product which you would recommend investing in first

- A. Presenter #1- Pierce
- B. Presenter #2- Conatix
- C. Presenter #3- Sikernes
- D. Presenter #4- Merlin
- E. Presenter #5- Mobile7



If there is one product you would be interested in being a POC/Beta evaluator, which one would it be?

- A. Presenter #1 – Pierce
- B. Presenter #2 – Conatix
- C. Presenter #3 – Sikernas
- D. Presenter #4 – Merlin
- E. Presenter #5 – Mobile7





UAC and DEP: Protection Mechanisms for Windows

Bob Baskette
Senior Manager, Security Operations
and Architect



Historical Need for UAC

- Prior to User Account Control (UAC) an end-user logged on to a system as an administrator was automatically granted full access to all system resources.
- While utilizing an administrator account the end-user could unintentionally or intentionally install a malicious program.



User Account Control - Basics

- UAC is a system facility used to inform the end user when an application requests a system change that requires administrator-level permission.
- UAC provides the ability to adjust the permission level of current user account to match the requirement of the executing application.



User Account Control - Basics

- UAC can be configured to “dump” privileges if tasks such as reading e-mail or creating documents are performed using an account with administrator privileges.



User Account Control - Basics

- UAC provides a facility to temporarily provide the needed administrative rights to complete the requested task and then reduce privilege levels back to that of a standard user.
- This facility can prevent unintended and unannounced changes to the system.



User Account Control - Prompts

- UAC utilizes one of four types of dialog boxes to notify the user of an administrative-level change.
- Each dialog box will provide guidance on how to respond to the request.



User Account Control - Prompts

- Native Windows Settings or Features
- This type of update will have a valid digital signature that verifies that Microsoft is the publisher.
- Microsoft recommends that it is safe to proceed.



User Account Control - Prompts

- A Program that not supplied by Microsoft
- This type of update will have a valid digital signature from the software vendor.
- Microsoft recommends verifying that the software should be implemented as well as that the software vendor is trusted by the organization.



User Account Control - Prompts

- A Program from an unknown publisher
- This type of update does not have a valid digital signature. Many legacy software packages are not signed by the software vendor.
- Microsoft recommends that extra caution be used and the software should only be permitted if from a trusted source.



User Account Control - Prompts

- Software update blocked by administrator
- This type of update has been determined to be not trustworthy.
- Microsoft recommends that the user contact the system administrator.



Permission Level Recommendations

- The standard user account should be used for everyday activities such as browsing the Internet, sending e-mails, or utilizing an office suite.
- The standard user account can also be used when installing a new program or changing a system setting since the system will prompt for permission to perform the task.



UAC Decision Factors

- Things to consider when the UAC box pops up (software installation/configuration change):
 - Check the name of the program, the publisher information, and the certificate information.
 - Is the software from a trusted source such as the original CD or a publisher's website.
 - Research the software to determine if it's a known program or malicious software.



UAC Changes for Windows 7

- Increased the number of tasks that the standard user can perform that do not prompt for administrator approval.
- Allow a user with administrator privileges to configure the UAC experience in the Control Panel.



UAC Changes for Windows 7

- Provide additional local security policies that enable a local administrator to change the behavior of the UAC messages for local administrators in Admin Approval Mode.
- Provide additional local security policies that enable a local administrator to change the behavior of the UAC messages for standard users.



UAC Changes for Windows 7

- By default, standard users and administrators access resources and run applications in the security context of standard users.
- The system will create an access token for the standard user. The access token contains information about the level of access granted, including specific security identifiers (SIDs) and Windows privileges.



UAC Changes for Windows 7

- The system will create two separate access tokens when an administrator logs into the system: a standard user access token and an administrator access token.
- The standard user access token contains the same user-specific information as the administrator access token, but the administrative Windows privileges and SIDs have been removed.



UAC Changes for Windows 7

- The standard user access token is used to start applications that do not perform administrative tasks.
- When the application must perform an administrative task the user must change or "elevate" the security context to an administrator (called Admin Approval Mode).



UAC Events

- Any tasks that require administrator privileges will generate a UAC prompt
- The event are marked by a security shield icon with the 4 colors of the Windows logo for Vista and Windows Server 2008 or with two panels yellow and two blue for Windows 7 and Server 2008 R2.



UAC Events

- Executing the application as an Administrator
- Changes to system-wide settings or to files in %SystemRoot% or %ProgramFiles%
- Installing and uninstalling applications



UAC Events

- Installing device drivers
- Installing ActiveX controls
- Changing settings for Windows Firewall
- Changing UAC settings
- Configuring Windows Update



UAC Events

- Adding or removing user accounts
- Changing a user's account type
- Configuring Parental Controls
- Running Task Scheduler
- Restoring backed-up system files



UAC Events

- Viewing or changing another user's folders and files
- Running Disk Defragmenter
- Changing the system time itself since the system time is commonly used in security protocols such as Kerberos.



Data Execution Prevention

- DEP is a security feature included in most modern operating systems including Microsoft Windows, Linux, Mac OS X, iOS, and Android.
- DEP is designed to prevent an application or service from executing code from a non-executable memory region, thus preventing exploits that store code in that region via a buffer overflow.



Data Execution Prevention

- DEP is based on the Linux Write XOR Execute memory protection facility.
- Marks areas of memory as either writeable or executable, but not both.
- DEP is designed to prevent code execution of code loaded onto the process stack or the function's heap area.



Data Execution Prevention

- Executable code should only be loaded into pages explicitly marked for code execution such as the code segment.
- Any attempt to run code from a page marked non-executable will generate an exception and the process will terminate.



Memory Basics – The Heap

- Program code is loaded into an area of memory known as the Heap.
- The Heap contains four memory segments:
 - Code Segment
 - Data Segment
 - BSS Segment
 - Heap Segment



Memory Basics – The Code Segment

- The Code segment holds the executable instructions for a program.
- The Code segment is often loaded into a lower memory location than the other segments.
- Since the Code segment holds executable code it should be non-writable.

Memory Basics – The Data Segment

- The Data segment holds the initialized global variables used by the program.
- This segment holds initialized variables:
 - `int y = 1;`
 - `char *MyString = "Hello World";`
- Since the Data segment holds variables it should be non-executable.

Memory Basics – The BSS Segment

- The BSS segment holds the uninitialized for the program such as:
 - `int Y;`
 - `char *OpenString;`
- Since the BSS segment holds variables it should be non-executable.
- So what does BSS stand for???



Memory Basics – The Heap Segment

- The Heap segment is a very dynamic area of memory.
- Used to hold user data or feature-rich application content
- Since the Heap segment holds variables and other application content it should be non-executable.



Data Execution Prevention Modes

- DEP supports two modes:
 - Hardware mode enforces DEP via registers in the CPU that mark memory pages as not executable
 - Software mode enforces DEP on those systems that do not provide hardware support in the CPU.
 - Software mode does not protect against execution of code in data pages but instead counters SEH overwrite



DEP Hardware Enforcement

- Hardware mode DEP enables the NX (No Execute) bit on AMD processors and the XD (Execute Disable) bit on Intel processors.
- Hardware mode DEP requires the use of the PAE kernel for 32-bit Windows and is supported natively on 64-bit kernels.



DEP Software Enforcement

- The function must be compiled with Software DEP/SafeSEH enabled.
- The vast majority of Microsoft Windows DLLs and Microsoft programs have been compiled to support Software DEP/SafeSEH.
- To fully secure a program all related files must be compiled to support SafeSEH.



DEP Software Enforcement

- Software DEP is also known as SafeSEH in the Microsoft Windows world.
- Software DEP/SafeSEH builds a table of trusted exception handling routines during code compilation and then verifies that any exception raised by the running function is registered in that function's exception table.



DEP Software Enforcement

- If a function generates an exception only the trusted exception handling routines will be allowed to execute.
- If a trusted exception handler cannot be found for the raised exception, the “Unhandled” exception handler will be invoked to terminate the process.



Questions???

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

Thank You!



2013
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.



Detailed Agency Information Security - 2013 Overall Security Program Scores

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| XYZ | Incomplete | Pass | 50% | 50% | Fail | 75% | Yes |

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 2013 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, Obtain an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to 3 hours each).

- Pass – Met the criteria
- Incomplete – Have yet to meet the criteria
- Unassigned – ISO not designated



Detailed Agency Information Security - 2013 Overall Security Program Scores Con't

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| XYZ | Incomplete | Pass | 50% | 50% | Fail | 75% | Yes |

Audit Plan Status: The Agency Head has submitted an IT Security Audit Plan for the period of fiscal year (FY) 2013-2014 or 2014-2016 for systems classified as sensitive based on confidentiality, integrity or availability (*Note: after July 1, 2013, Audit Plans submitted shall reflect FY 2014-2016*)

- Current - Plan is up to date and meets the criteria
- Expired - The IT Security Audit Plan on file does is not up to date and or does not meet the criteria
- Pending - Under review
- N / C - Non Compliant

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

- Pending - In review
- N/A - Not Applicable

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."

- Pending CETR - Values cannot be calculated until the agency reconciles their audit plan system names with the CETR database.
- Pending Review - In review



Detailed Agency Information Security - 2013 Overall Security Program Scores Con't

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| XYZ | Incomplete | Pass | 50% | 50% | Fail | 75% | Yes |

Business Impact Analysis Status: The Business Impact Analysis (BIA) has been provided by the agency. To be considered complete all applications must be associated with a business process, all business processes must be rated, have a recovery time objective (RTO) and be labeled as either Mission Essential (ME) or not ME.

Pass – BIA is complete

Fail – BIA has not been submitted or is incomplete

Open – Agency has submitted a BIA that is currently under review or required additional information.

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.

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

IDS Reports Submitted – Agency has submitted the required quarterly IDS/IPS reports to Commonwealth Security

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



Secretariat: Administration

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| CB | Incomplete | Expired | 0% | 0% | Fail | 0% | Yes |
| DGS | Pass | Current | 0% | 0% | Fail | 7% | Yes |
| DHRM | Incomplete | Current | N/A | 17% | Fail | 0% | Yes |
| DMBE | Incomplete | Expired | N/A | 100% | Fail | 100% | Yes |
| SBE | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Agriculture & Forestry

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| DOF | Incomplete | Current | 0% | 13% | Fail | 20% | Yes |
| VDACS | Pass | Current | 50% | 97% | Pass | 86% | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Commerce & Trade

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| BOA | Incomplete | Current | N/A | 100% | Pass | 100% | Yes |
| DBA | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| DHCD | Incomplete | Expired | 0% | Pending CETR | Fail | Pending CETR | Yes |
| DMME | Pass | Expired | 0% | Pending CETR | Fail | Pending CETR | Yes |
| DOLI | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| DPOR | Incomplete | Expired | 80% | 67% | Fail | 50% | Yes |
| TIC | Incomplete | Current | 0% | Pending CETR | Fail | Pending CETR | Yes |
| VEC | Incomplete | Current | 0% | 73% | Open | 0% | Yes |
| VEDP | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| VRA | Unassigned | N/C | N/A | 0% | Fail | 0% | Yes |
| VRC | Incomplete | Expired | N/A | 100% | Fail | 100% | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Education

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| DOE | Pass | Expired | N/A | 44% | Fail | 4% | Yes |
| FCMV | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| GH | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| JYF | Pass | Current | N/A | Pending CETR | Open | Pending CETR | Yes |
| LVA | Incomplete | Expired | 0% | 67% | Fail | 75% | Yes |
| NSU | Incomplete | Expired | 0% | 67% | Open | 0% | Yes |
| RBC | Incomplete | Expired | N/A | 0% | Fail | 40% | Yes |
| SCHEV | Incomplete | Expired | N/A | 0% | Open | 0% | No |
| SMV | Incomplete | Expired | 0% | 0% | Fail | 0% | Yes |
| SVHEC | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| VCA | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| VMFA | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| VSDB | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| VSU | Pass | Current | 0% | 67% | Fail | 94% | No |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Executive

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| OSIG | Pass | Pending | N/A | Pending Review | Pass | Pending Review | Yes |
| GOV | Incomplete | Current | N/A | 0% | Fail | 0% | Yes |
| OAG | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Finance

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| DOA | Incomplete | Expired | 0% | 56% | Fail | 0% | Yes |
| DPB | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| TAX | Pass | Current | 83% | 52% | Fail | 56% | Yes |
| TD | Incomplete | Current | N/A | Pending CETR | Fail | Pending CETR | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Health & Human Resources

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| CSA | Incomplete | Current | N/A | Pending CETR | Fail | Pending CETR | Yes |
| DBHDS | Pass | Expired | N/A | 0% | Fail | 0% | Yes |
| DHP | Pass | Current | N/A | 50% | Open | 100% | Yes |
| DMAS | Incomplete | Current | 91% | Pending CETR | Fail | Pending CETR | Yes |
| DRS | Incomplete | Expired | 14% | Pending CETR | Open | Pending CETR | Yes |
| DSS | Incomplete | Pending | Pending | Pending CETR | Open | Pending CETR | Yes |
| VDH | Pass | Current | 62% | Pending CETR | Open | Pending CETR | Yes |
| VFHY | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Independent Branch Agencies

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| IDC | Incomplete | Expired | 0% | 0% | Fail | 0% | No |
| SCC | Incomplete | Current | 17% | 100% | Fail | 0% | No |
| SLD | Incomplete | Expired | 0% | 0% | Fail | 0% | No |
| VCSP | Pass | Current | 0% | 50% | Fail | 0% | No |
| VRS | Incomplete | Current | 33% | 100% | Fail | 30% | Yes |
| VWC | Pass | Current | 50% | 100% | Pass | 0% | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Natural Resources

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| DCR | Incomplete | Expired | 0% | 50% | Fail | 0% | Yes |
| DEQ | Incomplete | Current | 75% | 50% | Fail | 50% | Yes |
| DGIF | Incomplete | Expired | 0% | 0% | Open | 0% | Yes |
| DHR | Pass | Pending | N/A | 100% | Open | 100% | Yes |
| MRC | Pass | Current | N/A | 100% | Pass | 100% | Yes |
| VMNH | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Public Safety

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| ABC | Pass | Current | 100% | 59% | Open | 15% | Yes |
| CASC | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| DCJS | Incomplete | Expired | N/A | 0% | Fail | 100% | Yes |
| DEM | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| DFP | Pass | Current | 0% | Pending CETR | Open | Pending CETR | Yes |
| DFS | Pass | Current | N/A | 100% | Pass | 100% | Yes |
| DJJ | Incomplete | Current | 33% | Pending CETR | Fail | Pending CETR | Yes |
| DMA | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| DOC | Pass | Current | 60% | Pending CETR | Open | Pending CETR | Yes |
| DVS | Pass | Current | 0% | 67% | Pass | 100% | Yes |
| VSP | Pass | Expired | 64% | 44% | Fail | 9% | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Technology

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| IEIA | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| VITA | Pass | Expired | 0% | Pending CETR | Fail | Pending CETR | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Transportation

| Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage of Audits Received | 3 Year Audit Obligation | Business Impact Analysis Status | 3 Year Risk Assessment Obligation | IDS Report Submitted |
|--------|--------------------------|-------------------|--|-------------------------|---------------------------------|-----------------------------------|----------------------|
| DMV | Pass | Current | 0% | Pending CETR | Fail | Pending CETR | Yes |
| DOAV | Incomplete | Current | N/A | 100% | Pass | 100% | Yes |
| DRPT | Incomplete | Expired | N/A | 0% | Fail | 0% | Yes |
| MVDB | Incomplete | Expired | N/A | 0% | Open | 0% | Yes |
| VDOT | Incomplete | Expired | 63% | Pending CETR | Fail | Pending CETR | Yes |

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



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, 2013



Questions ???????

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

Thank You!



Virginia Information Technologies Agency

Upcoming Events





General Assembly

**General Assembly convenes
January 8, 2014**



CIS/MS-ISAC & SANS

Center for Internet Security & SANS Institute for Security Awareness Training

As part of the Center for Internet Security and SANS partnership agreement they are offering this aggregate purchasing opportunity for state, local, territory and tribal governments, as well as related educational and not-for-profit entities, during the ***December 1, 2013 to January 31, 2014*** timeframe.

Please follow your agencies procurement policies and procedures when purchasing security training

For more information:

<http://alliance.cisecurity.org/opportunity/training.cfm>



Future ISOAG

Jan 8 **1:00 – 4:00 pm @ CESC**

Keynote: “e-Discovery” with Jeffery Jacobs, DTI
CSRM Panel Q&A

ISOAG meets the 1st Wednesday of each month in 2014



IS Council

When: Monday, Dec 16, 2013

Time: Noon to 2pm

Where: CESC

Guest Speaker: CGI



IS Orientation

When: Thursday, Dec 5, 2013

Time: 1:00pm to 3:00pm

Where: CESC , Room 1221

Register here:

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

Next IS Orientation will be held on Mar 9, 2014



Save The Date

IT Security Conference ***“Information Security Enabling the Business”***

Date: April 3 & 4, 2014

The event will include numerous topics.

More details will be provided soon!



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*

4 December, 2013



NORTHROP GRUMMAN

ADJOURN

THANK YOU FOR ATTENDING

