



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

November 2, 2011



# ISOAG November 2011 Agenda

- |      |   |  |
|------|---|--|
| I.   | Welcome & Opening Remarks                                       | Michael Watson, VITA   |
| II.  | The Mobile Revolution   | Dan Ford, Good Technologies                                      |
| III. | VITA/Personal Mobile Device Policy                              | Bob Baskette, VITA   |
| IV.  | Application Testing Using Random Data Patterns: Fuzzing 4 Short | Bob Baskette, VITA   |
| V.   | 2011 Commonwealth Security Annual Report                        | Michael Watson, VITA   |
| VI.  | Upcoming Events & Other Business                                | Michael Watson, VITA   |
| VII. | Partnership Update  | Bob Baskette, VITA<br>Michael Clark, NG<br>Demetrias Rodgers, NG |



# The Mobile **R**Evolution

How Public Sector is shifting to “Mobile Convergence”

Daniel Ford  
World Wide Public Sector  
Lead Cybersecurity Technologist

# The Changing Information Technology Landscape

**10 YRS AGO** 

**5 YRS AGO** 

**NOW** 

## Mobility



**Pagers & PDAs**



**PPCs & Smartphones**



**Smartphones & Tablets**

## Cloud







Microsoft Online Services **mobileme**

**Google Apps**

## Web 2.0



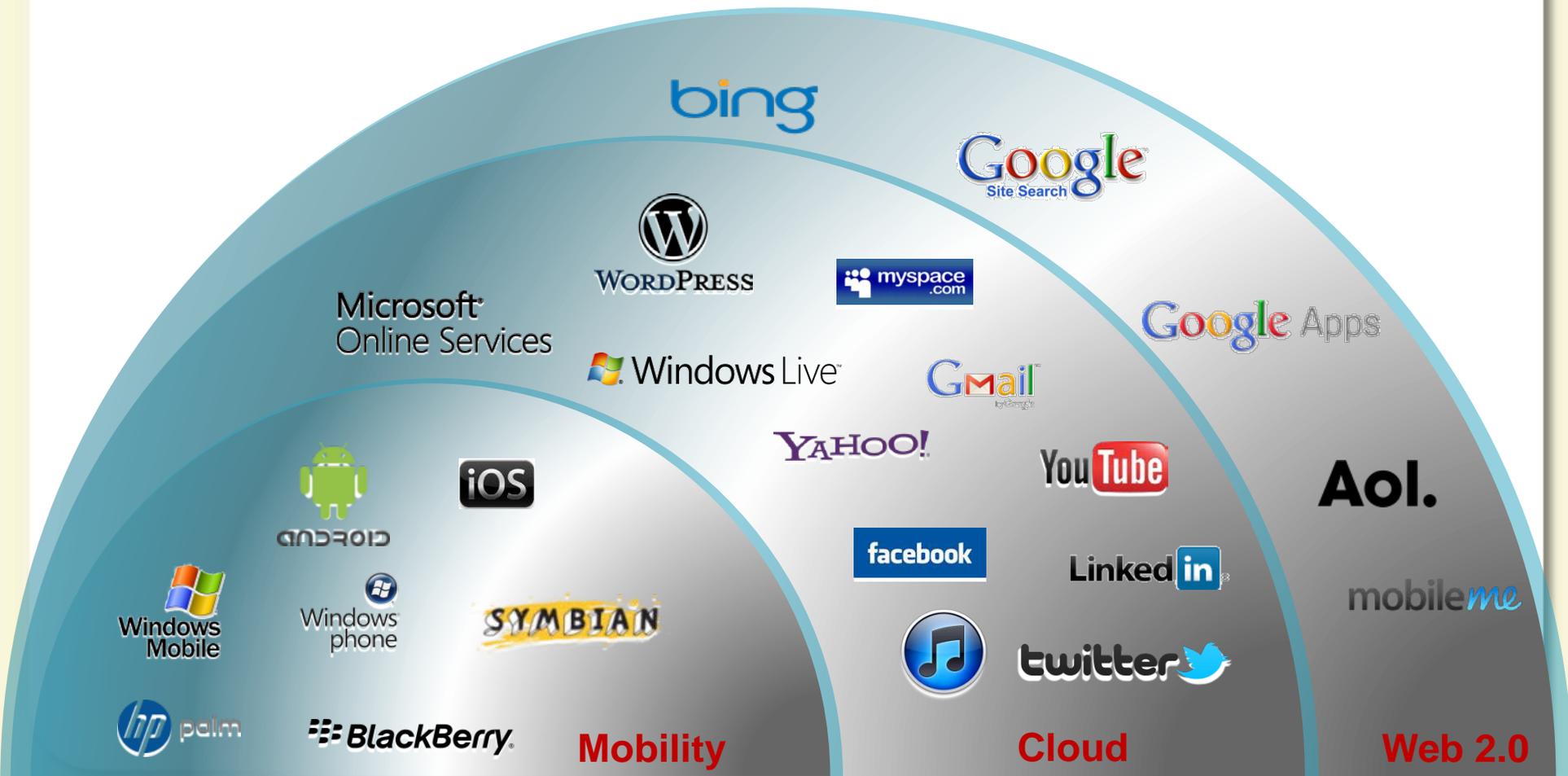









# The Changing Information Technology Landscape



# Mobile Productivity Demands

## Explosion of consumer App Stores...



...Has blurred the line  
between consumer  
and **enterprise devices**

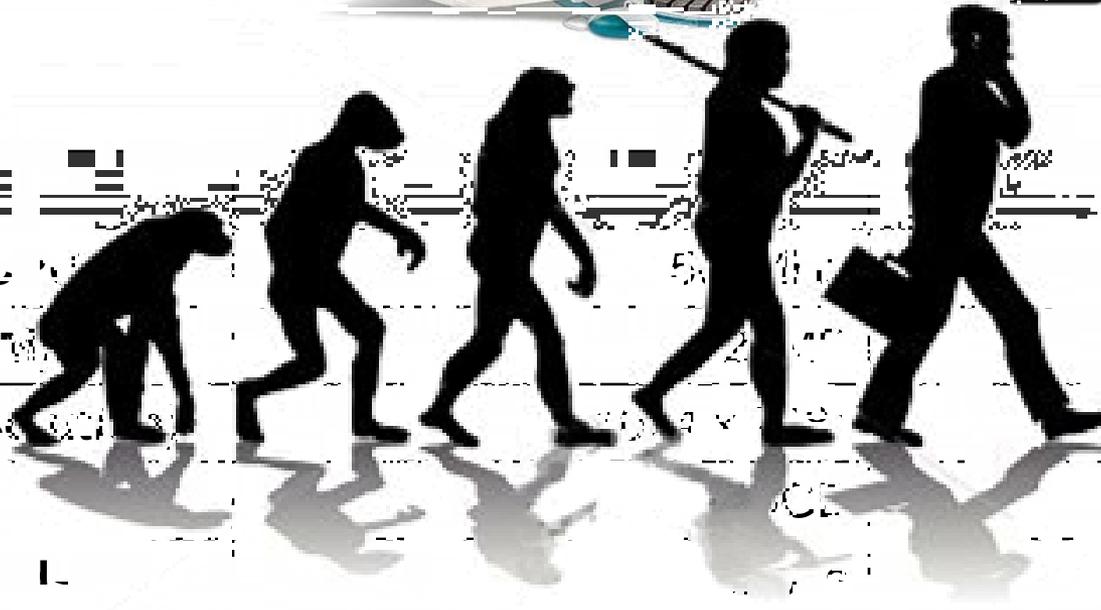
# Evolution of Mobility – Mobile Horsepower!

**“By 2013, mobile phones will overtake PCs as the most common Web access device worldwide.”**

- Gartner

2000

2010

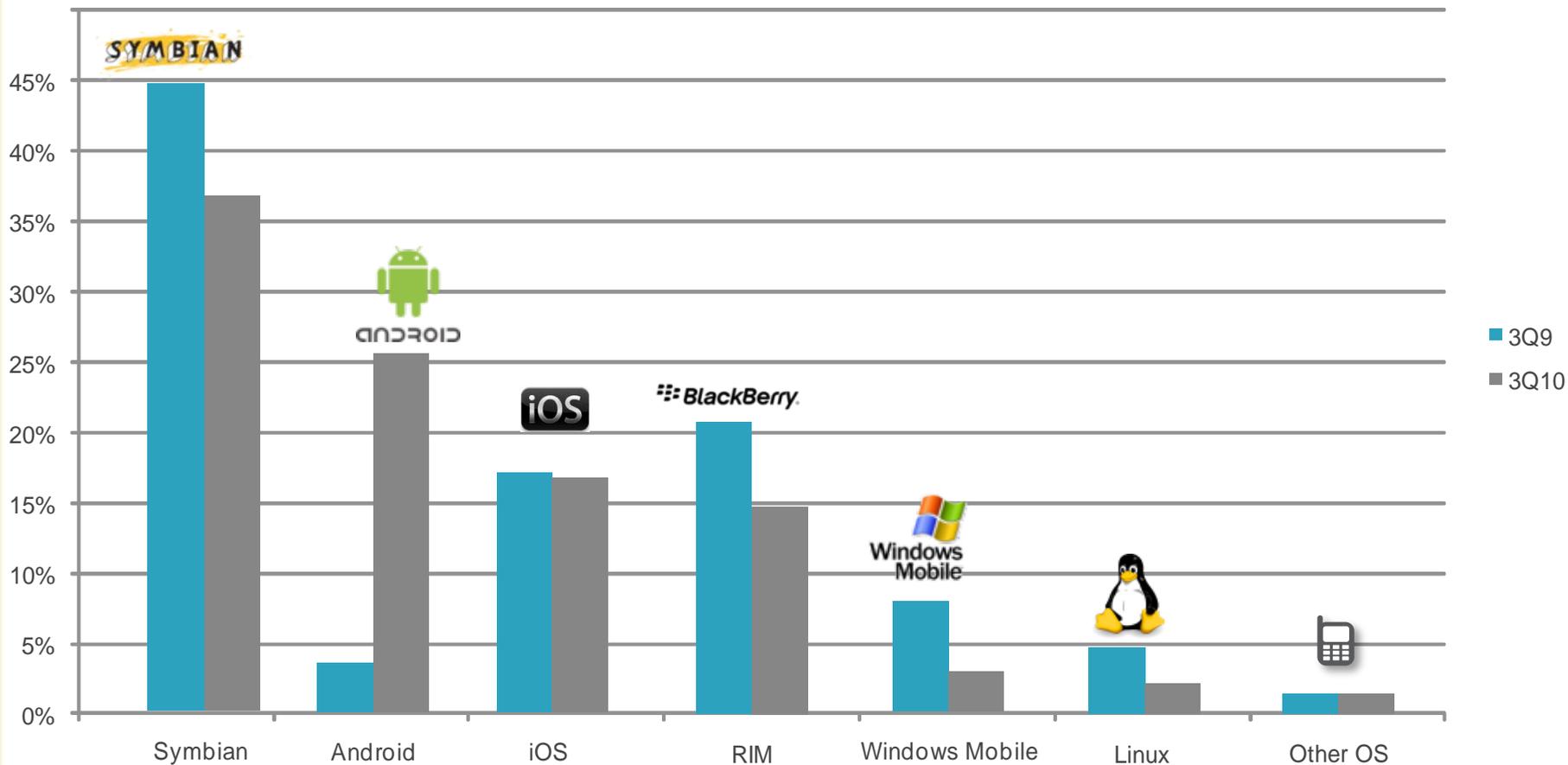


	one 4
Processor (GHz)	1Ghz
Memory (RAM)	512MB
Display (Res)	960 x 640**
Storage	32GB
Internet Speed	~6Mbps

# Modern Smartphone Explosion!



# Modern Smartphone Explosion!



**“Google is activating 550,000 Android Phones per day!”**

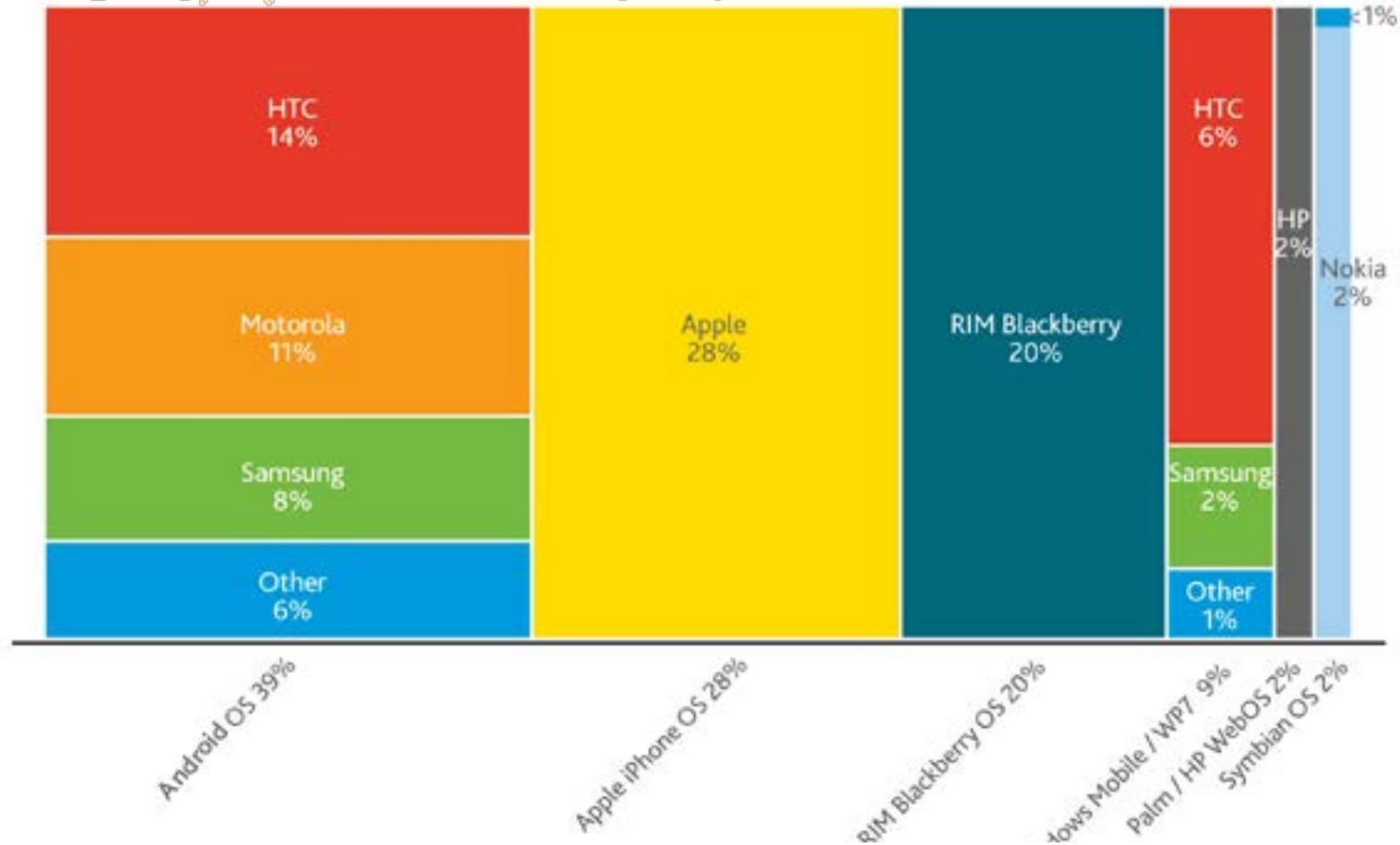
– Google Q2 Earnings Call, July 14, 2011, Larry Page, CEO Google

**Gartner.** Gartner: Android market share up with 22%, Symbian down 8% in Q3 2010  
– November 10, 2010

# Market Share by Device Manufacturer

## Manufacturer operating system share-smartphones

Q2 '11; postpaid mobile subscribers, n=20,202



Source: Nielsen

nielsen

# 3 Major Shifts in the Mobility Landscape (summary)

## Consumerization of Smartphones

*“190M smartphones sold in 2009, will more than double to 525M by 2012”<sup>1</sup>*

*“Consumer adoption of smartphones is exploding – fastest growing market segment at 43% for 2010”<sup>1</sup>*

## Mobile phones are mobile computing platforms

*Smartphone’s and Tablets are quickly becoming the top devices for remote data entry and retrieval.*

## Web > consumer apps > enterprise apps

***iTunes App Store:** 500,000 apps, 15 billion downloads <sup>2</sup>  
**Android Market:** 200,000 apps, 4.5 billion downloads <sup>3</sup>*

<sup>1</sup>Gartner Forecast Analysis: Mobile Devices, Worldwide, 2003-2014, 1Q10 Update

<sup>2</sup>Phil Schiller, Press Release, July7, 2010

<sup>3</sup>Android Team, Google I/O Conference, May 10, 2011

# What the Analysts are Saying...

## Employee behavior is changing

*“A wide variety of device models is entering the business domain, creating havoc for IT organizations...”*

**Gartner**<sup>®</sup>

Use Managed Diversity to Support Endpoint Devices  
– May 2010, Ken Dulaney



# What the Analysts are Saying...

## **Companies need to change, too.**

*“75% of Forrester enterprise survey respondents indicated user demand for support of devices on multiple platforms.”*

Five-Year Forecast for Enterprise  
Smartphone Marketshare, January 13, 2010

*“Nearly 30% of companies experienced a breach due to unauthorized mobile device use.”*

Q1 Enterprise and SMB Survey, 2009  
- Forrester Research

**FORRESTER®**

# Mobile Productivity

## **Mobile workers are more productive.**

*“Mobilizing a workforce can increase productivity and sales, and improve customer satisfaction.”*



Mobile Enterprise Strategy Key Initiative Overview  
– Phillip Redman, February 2010

- Mobile users are experiencing new levels of personal productivity.
  - Productivity is actually *better* in our personal lives.
  - More power in the consumer space.
- Workers are frustrated in their levels of business productivity.
- Workers need their work life to co-exist with their personal life.
- Consumer applications are raising demand for enterprise applications.

# Mobile Productivity Example – “Operation Blue Roof”

The Army Corps of Engineers is considered a first responder command. Whenever there is some sort of natural disaster, one of their objectives is called “Operation Blue Roof.” This entails them putting a blue tarp over any damaged roof to prevent further damage.

In order to complete their mission they needed to carry the following equipment:

- Rugged Laptop with broadband card
- Portable Printer
- Paper Notepad
- Cellular Phone
- Camera
- Portable Scanner



Now they can consolidate all of these peripherals in to one device!

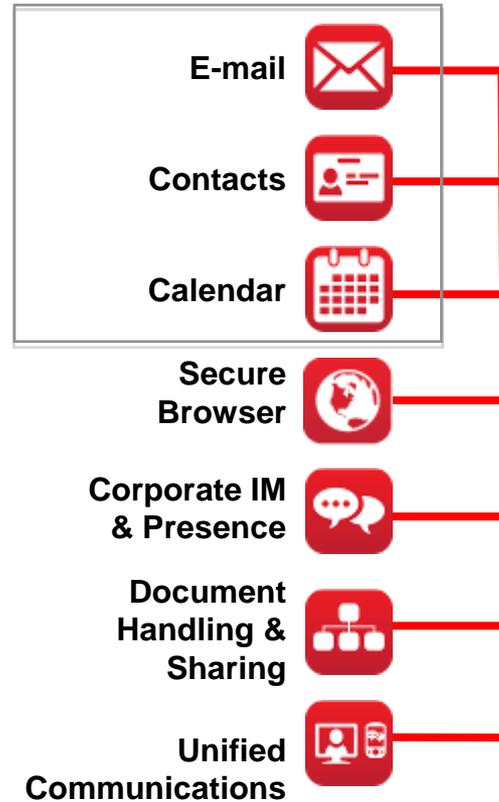
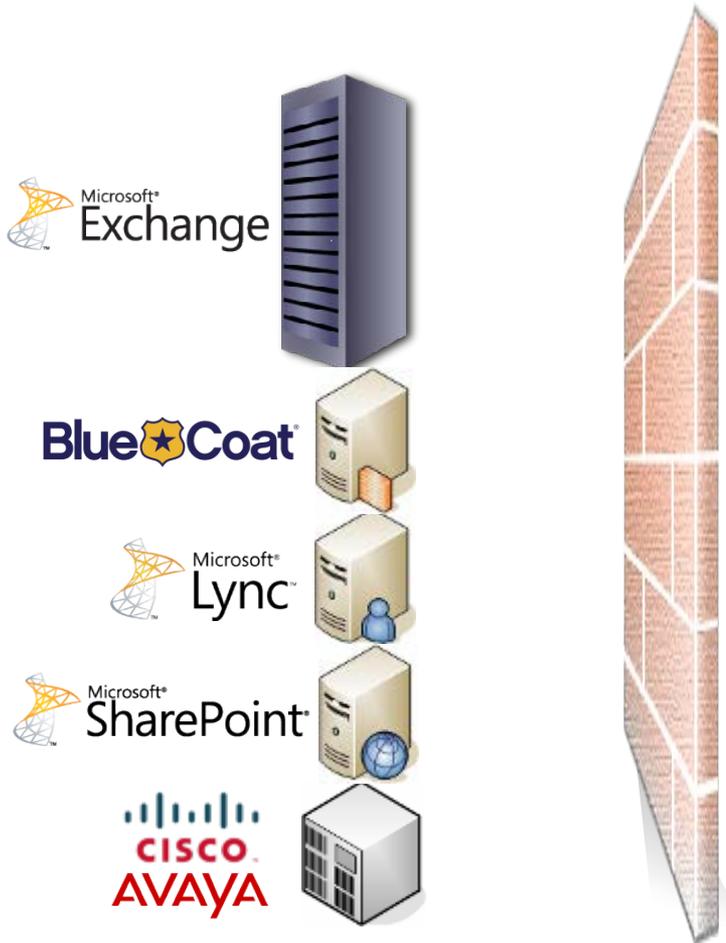


# Productivity Examples Continued

- The USAF is looking to replace all cockpit manuals with iPads on all aircrafts thus saving them millions of dollars annually on fuel
- The State Department and Pentagon both want to use iPads for handling all of their briefings, speech preparations, and read aheads. By utilizing the iPad, they get to eliminate carrying 3-ring binders of the same contents in printed form
- Every military recruiting command is looking at utilizing iPhones and iPads as a replacement for laptops for when they go out and meet with potential recruits
- The US Army challenged Army personnel to create applications for iOS and Android that could help the mobile warfighter. This initiative was called Apps4Army!



# Convergence between your Enterprise and Mobility Platform



# Cost Considerations

*“Enterprises with a mobility strategy have an annual TCO 71% less than companies that don’t support personal devices.”*

**Aberdeen Group**  
A Harte-Hanks Company

Enterprise Mobile Strategies 2010  
- Andrew Borg, Nathaniel Rowe



# Risks in Today's Mobility Environment



## Device Risk:

- Designed to easily share & replicate data
- Lack Government certifications (e.g. FIPS 140-2)

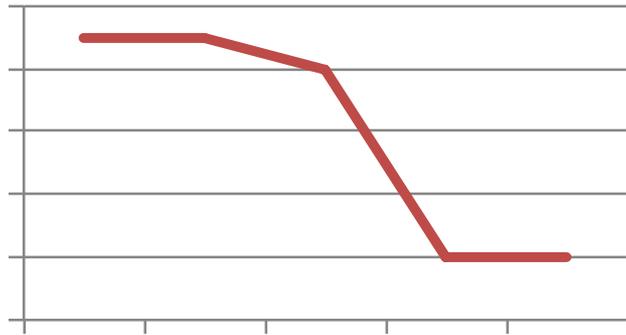
## User-based Risk:

- Uses unsecure consumer device without IT's knowledge
- Does not comply with security policies
- Unknowingly or purposely replicates government data to personal storage (e.g. Dropbox, box.net, Google Docs)

## Enterprise Risk:

- Expose agency to potential data breaches
- Lack consistent security policies
- Single Vendor Support causes users to circumvent the system

# Maintaining a Consistent Information Assurance Policy



e Policy



*From an IA perspective, the Desktop, Laptop, and Blackberry device maintain a high level of compliance to an agencies respective IA policy. However, as soon as a consumer oriented Smartphone gets introduced compliance typically takes a nose dive!*

# MDM Alone is Not Enough to Prevent Data Loss

Limited to O.S. & device security services

No hardware encryption!



Policies implemented at device level

No separation of personal/work

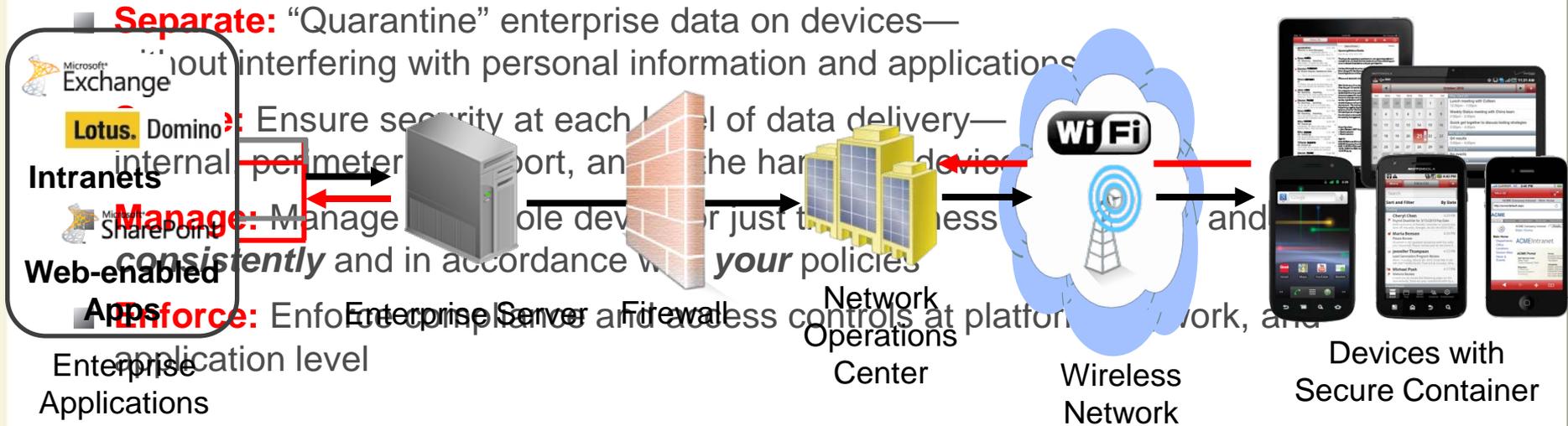


Limited ability to control consumer applications

Data potentially exposed



# How Do You Protect Government Data and Apps?



## Regulatory Compliance

- FIPS 140-2
- HIPAA
- FISMA
- HSPD12
- DoD Directive 8100.2



## Internal Security

- Control traffic by:
  - IP address
  - Subnet
  - Service
  - Protocol



## Perimeter Security

- Policy Groups
- No firewall holes
- Authorized device check
- Role-based admin
- Outbound Connections



## Container Security

- Push Services
- Secure Storage
- Secure Transport
- Container Management
- Threat Detection
- Authentication Framework

# Secure Container Concept

## Personal Data

Devices remain personal, untouched by enterprise

- Justifies shared employee expense

Freely access your applications

- Music
- Pictures
- Videos



## Government Data

Enterprise data lockdown

- Data encryption
- Password policies
- Remote wipe
- Secure data at rest

Access corporate apps

- Email, attachments & PIM
- Intranets
- Collaboration tools (e.g. Sharepoint)
- Web-enabled applications



# DISA STIG Requirements – Filling in the Gaps

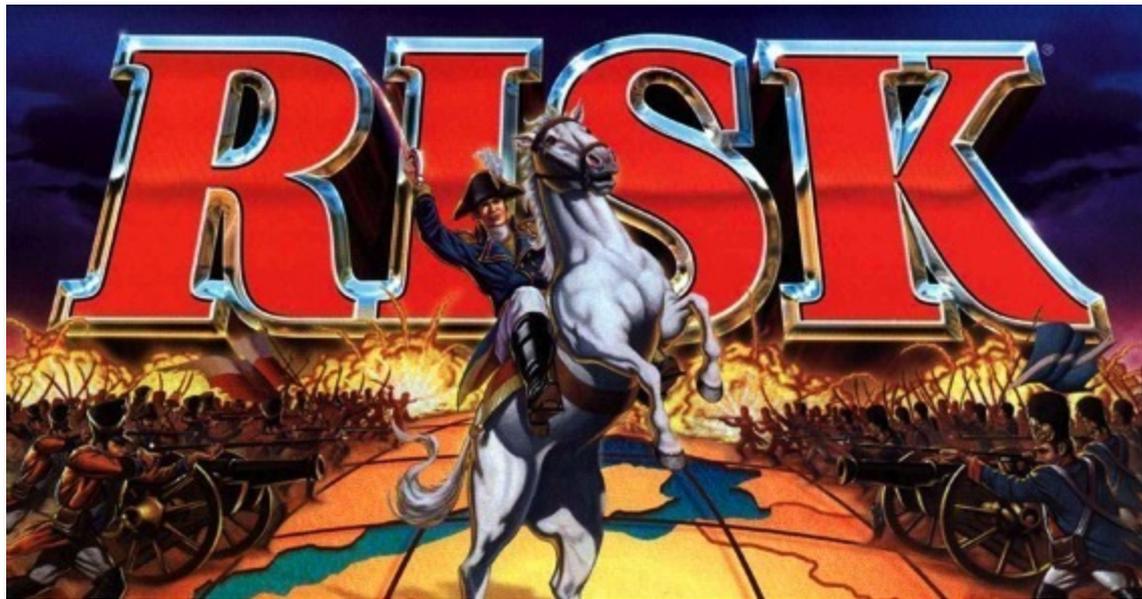
Requirement	iOS	Android	Good
Email System Requirements	✘	✘	✓
Data Protection/DAR [Using FIPS Crypto]	✘	✘	✓
Encryption of Transmitted Data/Email [Using a FIPS Crypto]	✘	✘	✓
S/MIME Requirements	✘	✘	✓
Public Key Infrastructure Requirements	✘	✘	✓
Smartphone Provisioning	✘	✘	✓
Internet Connections	✘	✘	✓
Smartphone Unlock & Password Requirements	★	★	✓
Application Controls	★	★	✓
Bluetooth Requirements	✘	✘	✓
Security Policy Enforcement	★	★	✓
WiFi Controls	✘	✘	★
Malware Controls	✘	✘	✓
Active Content in Email	✘	✘	✓

**Key:** ✓ = Met ★ = Partially Met ✘ = Not Met

# Consumerization of IT is Like Playing the Game of Risk

## What are the perceived risks vs. the actual risk?

- **Answer:** Many of the inherent risks that impact the native OS do not impact the container architecture



# Case Study: U.S. Dept of Defense



## Challenge

- Stringent requirements around DoD Directive 8100.2 specific to S/MIME and CAC integration
- Must be able to lock-down device features/functions (e.g. Camera, App Store, etc...)

## Impact

- Allows DoD Commands to use one common operating procedure to secure and manage both their iOS and Android OS devices.
- Status: Currently both the iOS and Android STIGs are in DRAFT form.

## Solution

- Government Furnished Equipment ONLY
- Secured and managed by Good for Enterprise

# Case Study: Dept of Energy



## Challenge

- Reduce mobility costs due to budgetary issues
- Secure government data on consumer devices

## Solution

- Shift to “Bring-Your-Own-Device” model
- Employees adopting iOS and Android devices
- Implement Good for Enterprise to ensure consistent security across multiple platforms and prevent data spillage/leaks

## Impact

- Labs are experiencing increased productivity and end user satisfaction because they get to choose the device they bring to and use for work.
- Labs are seeing cost savings because the end user is paying for their device



**Thank You**



# VITA Mobile Device Policy

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## VITA Mobile Device Policy

- The draft policy is under final review and should be published in early November
- This policy only addresses the use of mobile devices purchased by the Commonwealth of Virginia
- Personal devices are addressed by a separate policy



## STATEMENT OF POLICY:

- This Policy establishes the minimum requirements for the use of a COV owned and maintained mobile device to access, process, or store COV data in accordance with IT Security Standard (SEC501).
- This Policy stipulates the enhanced controls required for mobile devices and does not rescind the obligation to adhere to COV ITRM SEC501-06.



## Prior to Use

1. The mobile device must be authorized by the Agency Head or his/her designee.
2. The mobile device must be registered with the Agency's Information Security Officer.



## Prior to Use

3. The mobile device must be marked in a manner to clearly identify the device as COV property and indicate a method of return if the device is lost.
4. The mobile device user must read and sign the Agency acceptable use policy.



## Configuration Requirements

1. The mobile device must be configured to receive security policy and configuration information from the VITA Mobile Policy Servers.
2. The mobile device screen lock must be configured to engage after a maximum of 15 minutes of inactivity.



## Configuration Requirements

3. The mobile device must be configured to prohibit the storage of passwords in clear text.
4. The mobile device must be configured to automatically wipe the contents of the mobile device if 10 consecutive invalid login attempts occur.



## Configuration Requirements

5. Mobile device hardware options (wireless, infrared, Bluetooth, camera, GPS, etc.) that are not required for COV business functions (as defined by the Agency Head) must be disabled.
  
6. Mobile device applications that are not required for COV business functions (as defined by the Agency Head) must be disabled.



## Password Requirements

1. The mobile device must be configured to use a strong, complex password in accordance with the COV ITRM Information Security Standard.
2. The mobile device password must be changed after a period of 90 days.



## Password Requirements

3. The mobile device must be configured to not reuse a password prior to 24 password changes.
4. The mobile device must be configured not to cache/store passwords on the device.
5. The mobile device must be configured to suppress the display of passwords on the screen as the password is entered into the device.



## Connectivity Requirements

1. The mobile device must be configured to use an encrypted network connection at all times when accessing COV data.
2. The mobile device user must not connect non-COV devices to the COV mobile device. Wall and vehicle charging devices and devices that provide sound input and output are permitted.



## Connectivity Requirements

3. The mobile device must be connected to an approved/assigned COV software sync station to backup all COV data at least once every 21-days.
4. The mobile device must not be attached to a non-COV computing system without the written permission of the Agency Head or his/her designee.



## Software Requirements

1. The mobile device must use only the boot ROM and operating system as supplied by the device vendor/carrier.
2. The mobile device must only utilize software developed by the Agency, a software vendor under contract to the Agency, or acquired via the device vendor's or suppliers' authorized application store.



## Software Requirements

3. The mobile device must be configured to not allow the user to escalate the base privilege level.
4. The mobile device user must not tamper with security controls configured on the device.



## Software Requirements

5. The mobile device user must not install personal software on the mobile device.
  
6. The mobile device must install all security updates within 30-days of release by the original equipment manufacturer or the authorized device reseller.



## Data Storage Requirements

1. The mobile device shall only store sensitive COV data if approved by the Agency Head or his/her designee.
2. The mobile device must be configured to require all sensitive COV data be encrypted.



## Data Storage Requirements

3. The mobile device must utilize an industry-standard encryption protocol to store sensitive COV data (128-bit Advanced Encryption Standard at a minimum).
4. The mobile device must be configured to allow a remote wipe of all COV data stored on the device.



## Data Storage Requirements

5. The mobile device must be configured to store all COV data only on internal memory or non-removable media.



# Physical Security Requirements

1. The physical security of the mobile device is the responsibility of the employee to whom the device has been assigned.
2. The mobile device must be protected at all times from unauthorized access.
3. The mobile device must not be left unattended in any area accessible by the general public.



## Physical Security Requirements

4. Any mobile device to be decommissioned or transferred to another employee must adhere to the COV ITRM Removal of Commonwealth Data from Electronic Media Standard SEC 514.



## Physical Security Requirements

5. If the mobile device is lost or stolen, the incident must be reported to the VITA Customer Care Center and Commonwealth Security and Risk Management Incident Management within 24-hours in accordance with §2.2-603(F) of the Code of Virginia.
6. The lost or stolen mobile device will be wiped within 24-hours of the incident. The wiping action will be initiated by a VCCC ticket.



## Connecting to non-COV devices

- Connecting to Home/Public networks
  - Allowed if in compliance with the SEC 511 Telework Standard
- Connecting to Home/Public computers for charging
  - Not allowed since USB charging cables can transfer data as well as power
  - Car chargers are permitted



## COV Data

- COV data is any data that is provided to the Commonwealth for processing or storage by COV computing systems
  - COV email
  - COV form data
  - Working papers and documents
  - Data associated with web services
- Also includes configuration information
  - Must be included in the backup schedule



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



# Personal Mobile Device Policy

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## Personal Mobile Device Policy

- The draft policy is under final review and should be published in early November
- This policy only addresses the use of mobile devices not purchased by the Commonwealth of Virginia
- COV-owned devices are addressed by a separate policy



## STATEMENT OF POLICY:

- This Policy establishes the minimum requirements for the use of non-COV owned and maintained mobile devices to access, process, or store COV data in accordance with IT Security Standard (SEC501).
- This Policy stipulates the enhanced controls required for mobile devices and does not rescind the obligation to adhere to COV ITRM SEC501-06.



## Prior to Use

1. The mobile device must be authorized by the Agency Head or his/her designee.
2. The mobile device must be registered with the Agency's Information Security Officer.
3. The mobile device user must read and sign the Agency acceptable use policy.



## Prior to Use

4. The device must only be used to access COV data via the COV Messaging Service, a web service accessible from the public Internet, or from a COV internal network in accordance with the COV ITRM IT Standard Use of Non-Commonwealth Computing Devices to Telework SEC 511. This requirement does not restrict the use of the device for personal activities so long as those activities do not violate any other requirement of any existing COV policy.



## Prior to Use

5. The mobile device user must agree in writing to allow remote wiping and the erasure of all data on the device without warning, if so requested by the Agency Head or the Agency Head designee.
6. The mobile device user must agree to surrender the device to Commonwealth Security for review and forensic imaging upon request of the associated Agency Head or the Agency's Information Security Officer.



## Configuration Requirements

1. The mobile device must be configured to receive security policy and configuration information from the VITA Mobile Policy Servers.
2. The mobile device must be configured to use an encrypted network connection at all times when accessing COV data.



## Configuration Requirements

3. The mobile device screen lock must be configured to engage after a maximum of 15 minutes of inactivity.
4. The mobile device must be configured to prohibit the storage of passwords in clear text.



## Configuration Requirements

5. The mobile device must be configured to automatically wipe the contents of the mobile device if a maximum of 10 consecutive invalid login attempts occur.



## Password Requirements

1. The mobile device must be configured to use a strong, complex password in accordance with the COV ITRM Information Security Standard.
2. The mobile device password must be changed after a period of 90 days.



## Password Requirements

3. The mobile device must be configured to not reuse a password prior to 24 password changes.
4. The mobile device must be configured not to cache/store passwords on the device.
5. The mobile device must be configured to suppress the display of passwords on the screen as the password is entered into the device.



## Software Requirements

1. The mobile device must use only the boot ROM and operating system as supplied by the device vendor/carrier.
2. The mobile device must be configured to not allow the user to escalate the base privilege level.



## Software Requirements

3. The mobile device user must not tamper with security controls configured on the device.
4. The mobile device must install all security updates within 30-days of release by the original equipment manufacturer or the authorized device reseller.



## Data Storage Requirements

1. The mobile device shall only store sensitive COV data if approved in advanced by the Agency Head or his/her designee.
2. The mobile device must be configured to require all sensitive COV data be encrypted.



## Data Storage Requirements

3. The mobile device must utilize an industry-standard encryption protocol to store sensitive COV data (128-bit Advanced Encryption Standard at a minimum).
4. The mobile device must be configured to allow a remote wipe of all COV data stored on the device.



## Data Storage Requirements

5. The mobile device must be configured to store all COV data only on internal memory or non-removable media.



# Physical Security Requirements

1. The mobile device must be protected at all times from unauthorized access.
2. If the mobile device is lost or stolen, the incident must be reported to the VITA Customer Care Center and Commonwealth Security and Risk Management Incident Management within 24-hours in accordance with §2.2-603(F) of the Code of Virginia.



## Physical Security Requirements

3. The lost or stolen mobile device will be wiped using an automated method within 24-hours of the incident.



## COV Data

- COV data is any data that is provided to the Commonwealth for processing or storage by COV computing systems
  - COV email
  - COV form data
  - Working papers and documents
  - Data associated with web services
- Also includes configuration information
  - Must be included in the backup schedule



## Password requirements

- The Mobile Device must adhere to the password requirements set forth in SEC 501 for length, complexity, lifetime, and history
  - Simple PINs are too easy to defeat prior to automated wiping windows
  - The device must use a password for screen lock and device configuration access



## Use of Personal Devices

- The use of personal devices is a privileged granted by the Agency Head, not a right
  - The Acceptable Use Policy will stipulate the right of the Agency to remotely wipe a device without warning
  - The AUP will stipulate the right of the Agency to conduct a forensic review of the device



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



# Application Testing using Random Data Patterns: or Fuzzing for Short

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## Fuzz Testing Background Info

- Software testing technique used to expose security issues in applications by introducing invalid, unexpected, or random data into the inputs of an application
- The application is monitored to detect process exceptions such as faults or failing built-in code assertions



## Fuzz Testing Background Info

- The concept and term originates from a class project conducted at the University of Wisconsin Madison in 1989  
<http://www.cs.wisc.edu/~bart/fuzz/>
- Fuzz testing is considered a Black Box testing technique since all testing is performed from an external view

## Why Perform Fuzz Testing

- Fuzz testing is based on the assumption that coding errors exist within every application and therefore a systematic approach will expose the errors
- Fuzz testing will provide another point of view to classical software testing techniques such as code reviews and debugging because Fuzz testing uses a non-human approach



## Why Perform Fuzz Testing

- Fuzz testing improves application security because it can detect defects which may be overlooked by human testers due to the complexity of the application coding



# Fuzzy Testing Targets

- Application code issues to be tested include:
  - Buffer overflows
  - Format strings
  - Code injections
  - Dangling pointers
  - Race conditions
  - Denial of service conditions

## Fuzz Testing Targets

- File formats and network protocols are the most common targets of testing, but any type of program input can be Fuzz tested
- Interesting inputs include:
  - Environment variables
  - Keyboard and mouse events
  - Sequences of API calls
  - Contents of databases
  - Shared memory



# Fuzzy Testing Targets

- Of primary importance is any input that crosses a trust boundary
- It is more important to test code that handles the upload of a user's file than code used to parse a configuration file that is accessible only to a privileged user.
- Any untrusted source of data input is considered to be insecure and inconsistent

## Fuzz Testing Simple Example

- An application that records the selection between three items would use an integer to store a value between 0 – 2. The Fuzz test would determine what would happen if the application attempted to store a larger value than the integer could hold (buffer capacity) or a value not consistent with the application (logic issue)

## Fuzz Testing Advantages

- Application errors uncovered by Fuzz testing can be severe, exploitable coding errors that could be used by a real attacker
- Fuzz testing can be used to uncover the same application issues used by malicious individuals since the same techniques and tools are now used by attackers to exploit deployed software



## Fuzz Testing Advantages

- The greatest advantage of Fuzz testing is that the test conditions are extremely simple to design and that the test conditions are free of preconceptions about system behavior

## Fuzz Testing Disadvantages

- The primary concern with Fuzz testing is that basic/simple inputs will usually only yield simple coding errors. The quality of the output is solely depended upon the quality of the input
- The randomness of inputs used in fuzzing is often seen as a disadvantage, as catching a boundary value condition with random inputs is highly unlikely

## Fuzz Testing Disadvantages

- The technique can only provide a random sample of the system's potential behavior
- In many cases passing a Fuzzing test may only verify that an application can handle exceptions without crashing, rather than behaving correctly



# Fuzzy Analysis Common Steps

- Identify the target
- Identify inputs
- Generate Fuzz data
- Execute Fuzz data
- Monitor the output
- Determine the exploitability

## Fuzz Testing Initialization

- It is important to configure the Fuzz testing tool to record the input data (including the pseudo-random number-generated seed value) to be used in the test to a file prior to executing the test.
- The file will be needed to reproduce the testing errors if the Fuzzing software causes the system to crash

# Fuzz Testing Criteria Types

- Mutation-based
  - Fuzz testing that mutates existing data samples to create test data
- Generation-based
  - Fuzz testing that define new test data based on models of the input



## Fuzz Testing Techniques

- A specification-based Fuzz Test involves writing the entire array of specifications into the tool
- The tool then uses model-based test generation techniques to walk through the specifications to add anomalies in the data contents, structures, messages, and sequences

## Protocol-Based Fuzz Testing

- Protocol awareness can be used to generate Fuzz testing criteria and send forged packets to the target application
- The testing criteria can be generated from scratch, or the criteria can be mutated from examples from test suites or real data

## Protocol-Based Fuzz Testing Limitations

- Testing will not be successful until the protocol specification is relatively mature since the specification is a prerequisite for writing the test condition
- Many useful protocols are proprietary or utilize proprietary extensions. If the test conditions are based only on published specifications the test results will be limited

# Fuzz Testing Conditions/Vectors

- Define lists of "known-to-be-dangerous values" for each type
  - For integers: zero, negative, very big numbers
  - For chars: escaped, interpretable characters / instructions
  - For SQL Requests, quotes / commands
  - For binary: random ones

# Application Fuzz Testing

- The attack vectors are within the I/O
- For a desktop application:
  - The UI (testing all the buttons sequences / text inputs)
  - The command-line options
  - The import/export capabilities (see file format fuzzing below)



# Application Fuzz Testing

- The attack vectors are within the I/O
- For a web application
  - URLs
  - Forms
  - User-generated content
  - RPC requests



## File Format Fuzz Testing

- Generates multiple malformed samples and processed the samples sequentially
- When the application generates a fault the debug information is kept for further investigation.

# File Format Fuzz Testing

- Attack vectors include:
  - The codec/application layer
    - Lower-level attacks/ application internals
  - The parser layer (container layer)
    - File format constraints
    - File format structure
    - File format conventions
    - File format field sizes
    - File format flags



## OWASP Information

- Open Web Application Security Project
- Does not focus on complete application security programs but provides a necessary foundation to integrate security through secure coding principles
- Application security includes the people, processes, management, and technology



## OWASP Information

- The Open Web Application Security Project is a 501c3 not-for-profit worldwide organization focused on improving the security of application software
- The mission of OWASP is to make application security visible, so that organizations can make informed decisions about true application security risks



## OWASP Top Ten

OWASP Top Ten project categorizes the application security risks by evaluating the top attack vectors and security weaknesses in relation to their technical and business impact

Each risk will demonstrate a generic attack method independent of the technology or platform in use



# OWASP Top Ten

- A1 Injection
- A2 Cross-Site Scripting
- A3 Broken Authentication and Session Management
- A4 Insecure Direct Object References
- A5 Cross-Site Request Forgery



## OWASP Top Ten

- A6 Security Misconfiguration
- A7 Insecure Cryptographic Storage
- A8 Failure to Restrict URL Access
- A9 Insufficient Transport Layer Protector
- A10 Unvalidated Redirects and forwards



# Fuzz Testing software from OWASP

- WebScarab
  - Framework for analyzing applications that communicate using the HTTP and HTTPS protocols
- JBroFuzz
  - A stateless network protocol Fuzz testing program
- WSFuzzer
  - Real-world manual SOAP pen testing tool



## JBrofuzz

- Well-known platform for web application Fuzz testing
- Supports both HTTP and HTTPS protocols
- Need to supply the URL and the part of the web request to Fuzz

## JBrofuzz

- Can create a request manually or use a predefined set of payloads
  - Cross-site scripting
  - SQL Injection
  - Buffer overflow
  - Format String Error
- The responses will be recorded for tether inspection



# JBroFuzz Application Overview

- Fuzzing Tab
  - The main tab of JBroFuzz
  - Responsible for all Fuzz testing operations performed over the network.
  - It creates the malformed data for each request depending on the payload selected and puts the data on the wire and writes the response to a file

# JBroFuzz Application Overview

- Graphing Tab
  - Is responsible for graphing the responses received from the Fuzz test.
  - Provides a clear indication of a response that is different than the rest received
  - Generates a clear indication of further examination being required.

# JBroFuzz Application Overview

- Payload Tab
  - A collection of Fuzz test with their corresponding payloads that can be used for the Fuzz test
  - Payloads are added to the request in the Fuzzing tab
  - Provides a clear view of what payloads are available, the properties of each payload and how the payloads are grouped for each test



# JBroFuzz Application Overview

- Header Tab
  - A collection of browser headers that can be used while Fuzz testing
  - The headers are obtained from different browsers on different platforms and operating systems.
  - The headers are required since many web applications respond differently to different browser impersonation attacks.

# JBroFuzz Application Overview

- System Tab
  - Represents the logging console of JBroFuzz at runtime
    - Can be used to access
      - Java runtime information
      - Errors that occur
      - Events being logged



## Bunny

- General purpose Fuzz testing program designed specifically to test C programs
- Formulates the compiler-level integration which injects the instrumentation hooks into the application process and monitors its execution for changes in function calls, parameters, and return values in response to changes to the input data

## Bunny

- Operation is performed in real-time and the feedback is provided accordingly
- Supports up to nine different fault injection strategies
- Provides detailed controls over the type, behavior, depth, and likeliness

# Brute force Exploit Detector

- Tool designed to fuzz the plain-text protocols against potential buffer overflows, for-mat string bugs, integer overflows, and DoS conditions
- Automatically tests the implementation of a protocol by sending a different combination of commands with problematic strings to confuse the target



# Brute force Exploit Detector

- BED protocols
  - FTP
  - SMTP
  - POP
  - HTTP
  - IMAP
  - PJJ
  - LPD
  - Finger
  - Socks4/Socks5

## Fuzz Testing Summary

- Fuzz testing is intended to provide an assurance of overall quality rather than an end-all bug-finding tool
- Fuzz testing can suggest which parts of an application should get special attention
  - Code audit
  - Static analysis
  - Partial rewrites

## The Other Fuzzy Topic

- The Fuzzy Navel
  - A mixed drink made from peach schnapps and orange juice.
  - One of the first drinks to arise in the new popularity of cocktails and mixed drinks in the 1980s
  - Originated in Omaha Nebraska at the Wagon Tongue Bar.
  - "Fuzzy" in the name refers to the peach, and "navel" to the orange.



## Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



2011  
Commonwealth Security Annual Report  
as of  
November 1, 2011

Michael Watson  
Acting 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.



# Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011 - Percentage of CAPs Received	2011 - Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

**Acronyms:**

- ISO:** Information Security Officer
- IS:** Information Security
- CAP:** Corrective Action Plan
- CISO:** Chief Information Security Officer of the Commonwealth

**ISO Designated: The Agency Head has**

- Yes** - designated an ISO with the agency within the past two years
- No** – not designated an ISO for the agency since 2006
- Expired** –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

**Attended IS Orientation:**

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to “Extra Credit!”



# Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

**Security Audit Plan Received: The Agency Head has**

**Current** - submitted a Security Audit Plan for the period of fiscal year (FY) 2011-2013 or 2012-2014 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2011, Audit Plans submitted shall reflect FY 2012-2014)

**No** - not submitted a Security Audit Plan since 2006

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

**Expired** –submitted a Security Audit Plan on file that does not contain the current three year period FY FY 2011-2013 or FY 2012-2014

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

**2011 - Percentage of CAPs Received: The Agency Head or designee has**

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

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

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



# Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

**2011 - Percentage of Quarterly Updates Received:** The Agency Head or designee has % – submitted % of quarterly status updates received for corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**N/A** - no open Security Audit findings

**Pending** - submitted quarterly status update that is currently under review



# Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

### 3 year - Percentage of Audit Obligation Completed:

Percent of sensitive systems reported **by 2008** (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *“At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.”*

Agencies that did not submit an IT Security Audit Plan **by 2008** were not in compliance and therefore there is no data to report on for **2011**.

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

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

**Pending** – currently under review

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



## 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 and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

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

**December 31, 2011**



# Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
CB	Yes	1	Expired	0	N/A	0
DGS	Yes	3	Current	N/A	N/A	0
DHRM	Yes	1	Current	0	N/A	100
DMBE	Yes	1	Expired	N/A	N/A	0
EDR	Yes	1	Current	100	100	100
HRC	Yes	0	Current	N/A	N/A	100
SBE	Yes	1	Expired	N/A	0	50

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DOF	Yes	1	Current	100	N/A	100
VDACS	Yes	1	Current	100	Pending	100

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
BOA	Yes	1	Expired	0	N/A	0
DBA	Yes	0	Expired	N/A	N/A	0
DHCD	Yes	0	Current	N/A	100	50
DMME	Yes	4	Current	50	0	57
DOLI	Yes	0	Expired	0	N/A	0
DPOR	Yes	1	Expired	N/A	0	100
TIC	Yes	0	Expired	0	N/A	0
VEC	Yes	0	Expired	25	50	11
* VEDP	Yes	1	Expired	0	N/A	0
VRA	No	0	Expired	N/A	N/A	0
VRC	Yes	1	Pending	Pending	Pending	Pending

\* VEDP includes VTA and VNDIA

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
CNU	Yes	0	Current	N/A	N/A	0
DOE	Yes	1	Current	100	25	76
FCMV	Yes	0	Expired	N/A	N/A	100
GH	Yes	1	Expired	N/A	N/A	0
JYF	Yes	1	Current	N/A	100	100
LVA	Yes	0	Expired	0	N/A	100
NSU	Yes	4	Expired	N/A	N/A	0
RBC	Yes	1	Current	0	N/A	0
SCHEV	Yes	0	Expired	0	N/A	0
SMV	Yes	0	Expired	0	N/A	0
SVHEC	No	0	No	N/A	N/A	0
UMW	Yes	0	Current	50	33.33	80
VCA	Yes	0	Expired	N/A	N/A	100
VMFA	Yes	2	Expired	N/A	0	50
VSDB	Yes	1	Current	0	N/A	0
VSU	Yes	0	Expired	100	36.36	78

**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 [CS&RM](#).



# Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DOA	Yes	1	Current	0	0	25
DPB	Yes	0	Expired	N/A	0	100
TAX	Yes	1	Current	Pending	Pending	Pending
TD	Yes	0	Current	Pending	N/A	Pending

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
*DBHDS	Yes	3	Current	N/A	0	100
DHP	Yes	2	Expired	0	N/A	0
DMAS	Yes	2	Current	N/A	N/A	0
*DRS	Yes	4	Current	80	18.92	48
DSS	Yes	5	Current	Pending	50	22
VDH	Yes	2	Current	N/A	58.33	21
VFHY	Yes	0	Current	N/A	N/A	100

\* DBHDS includes VCBR

\* DRS includes DBVI, VDA, VDDHH,VBPD and WWRC

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DCR	Yes	0	Pending	Pending	Pending	Pending
DEQ	Yes	1	Current	0	0	75
DGIF	Yes	3	Current	0	N/A	0
DHR	Yes	0	Expired	0	N/A	0
MRC	Yes	1	Current	100	0	100
VMNH	Yes	1	Expired	0	N/A	0

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
ABC	Yes	3	Current	75	36.36	100
CASC	Yes	0	Expired	N/A	N/A	100
DCE	Yes	2	Pending	Pending	Pending	Pending
DCJS	Yes	1	Expired	0	N/A	0
DEM	Yes	1	Current	N/A	N/A	0
DFP	Yes	0	Current	N/A	50	100
DFS	Yes	0	Pending	N/A	N/A	0
DJJ	Yes	2	Current	N/A	100	66.67
DMA	Yes	0	No	N/A	N/A	N/C
*DOC	Yes	4	Expired	71.43	100	59
*DVS	Yes	1	Current	100	N/A	100
VSP	Yes	0	Current	100	100	66.67

\*DOC includes VPB

\*DVS includes VWM

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
IEIA	Yes	2	Expired	0	N/A	0
VITA	Yes	2	Current	100	Pending	54.55

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DMV	Yes	1	Current	0	0	100
DOAV	Yes	0	Expired	0	N/A	0
DRPT	Yes	0	Expired	N/A	N/A	0
MVDB	Yes	0	Expired	N/A	N/A	100
VDOT	Yes	7	Expired	29	100	45
VPA	No	0	No	N/A	N/A	N/C

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
IDC	Yes	4	Current	N/A	80	100
SCC	Yes	2	Current	66.67	50	50
SLD	Yes	2	Expired	0	N/A	0
VCSP	Yes	1	Current	N/A	N/A	100
VOPA	Yes	1	Current	0	N/A	0
VRS	Yes	0	Expired	0	15	32
VWC	Yes	0	Current	N/A	N/A	17

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
GOV	Yes	0	Current	N/A	N/A	N/A
OAG	Yes	2	Expired	N/A	N/A	0

**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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Upcoming Events





## MS-ISAC

### *National Webcast Initiative*

Thursday, Dec 15  
2:00 pm – 3:00 pm EDT

Topic: **Social Networking: The Latest Security Issues and How to Manage Them**

Visit MS-ISAC web for more information:

*<http://www.msisac.org/webcast/>*



# Information Security System Association

## ISSA

**DATE:** Wednesday, Nov 9, 2011

**LOCATION:** Maggiano's Little Italy

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

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

Lunch served at 12.

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

**SPEAKER:** Shane Harris, Award Winning Author

**TOPIC:** Business & Policy Implications of Cyber Security



## 2011 Information Security Awareness Tools

The Information Security Toolkit has been updated with new materials!

<http://www.vita.virginia.gov/security/toolkit/>

For printing cost estimates you can contact DMV's  
Damian McInerney at (804)367-0925  
or email: [damian.mcinerney@dmv.virginia.gov](mailto:damian.mcinerney@dmv.virginia.gov)

***Thank you DMV!***



## Future ISOAG's

**From 1:00 – 4:00 pm at CESC**

**Wednesday - December 7, 2011**

*Speaker: David Marcus, Director of McAfee Labs & Threat Research*

**Wednesday - January 4, 2012**

*Speaker: Patrick Gray, Principal Security Strategist at Cisco Systems*

**ISOAG will be held the 1<sup>st</sup> Wednesday of each month in 2012**



# Future IS Orientation Sessions

**Tuesday - November 8, 2011**

**1:00 – 3:30p  
(CESC)**

**Tuesday - February 7, 2012**

**1:00 – 3:30p  
(CESC)**

**IS Orientation is now available via webinar!**



## Submit Events

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

Please submit all upcoming events to:  
[Kathryn.Merhout@VITA.Virginia.Gov](mailto:Kathryn.Merhout@VITA.Virginia.Gov)



# ADJOURN

