



Virginia Information Technologies Agency

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

April 06, 2011



# ISOAG April 2011 Agenda

- |      |   |   |
|------|---|---|
| I.   | Welcome & Opening Remarks                           | John Green, VITA                          |
| II.  | Wireless LAN Security:<br>How Vulnerable Are You?   | Andrea Di Fabio, ISO, Norfolk State Univ. |
| III. | Mobile Device Policy                                | Bob Baskette, VITA                        |
| IV.  | Personnel Security:<br>A Short Review of SEC 501-01 | Bob Baskette, VITA                        |
| V.   | Information Security Standard:<br>SEC 501 Changes   | John Green, VITA                          |
| VI.  | Upcoming Events & Other Business                    | John Green, VITA                          |
| VII. | Partnership Update                                  | Bob Baskette, VITA<br>Michael Clark, NG   |



# *Wireless LAN Security: How vulnerable are you?*

**Andrea Di Fabio** – Information Security Officer



- Common Wireless Devices
- Wireless Security, or lack thereof
- How to secure wireless communication
- Wireless @ NSU
- Scary Live Demos 😬
  - Wireless LAN demo
  - Bluetooth demo

# Common Wireless Devices



Mobile Phones



2 Way Radio



Wireless  
Keyboard & Mouse



Bluetooth



Door/Alarms



Cordless



Really ?



Wireless  
X10 home control



RFID/HID



WiFi



# Wireless Security, or lack thereof

## WEP

This paper, "[Breaking 104 bit WEP in less than 60 seconds](#)," is the best attack against WEP to date:

**Abstract:** We demonstrate an active attack on the WEP protocol that is able to recover a 104-bit WEP key using less than 40.000 frames with a success probability of 50%. In order to succeed in 95% of all cases, 85.000 packets are needed. The IV of these packets can be randomly chosen. This is an improvement in the number of required frames by more than an order of magnitude over the best known key-recovery attacks for WEP. On a IEEE 802.11g network, the number of frames required can be obtained by re-injection in less than a minute. The required computational effort is approximately  $2^{20}$  RC4 key setups, which on current desktop and laptop CPUs is negligible.

# Wireless Security, or lack thereof

## WPA and WPA2

To carry out the WPA dictionary attack using aircrack-ng we either have to:

1. Wait for a WPA client to associate to the network (This could take a while)
2. Force a WPA client off the network, forcing it to reassociate (aireplay, void11).

```
ca\ Aircrack-ng - aircrack-ng.exe -a 2 -w dict capture2.cap
C:\aircrack-ng-0.4.2-win\bin>aircrack-ng.exe -a 2 -w dict capture2.cap
Opening capture2.cap
Read 607 packets.

# BSSID          ESSID          Encryption
1 00:06:25:BF:64:99  cuckoo        WPA <1 handshake>

Choosing first network as target.
```

```
ca\ Aircrack-ng
aircrack-ng 0.4.2

[00:00:25] 4090 keys tested <160.75 k/s>

KEY FOUND! [ passphrase ]

Master Key   : CC 9D 81 0B 93 70 BE 17 BD 60 18 2E D0 D9 11 EB
              E7 51 BD 15 4D 92 30 87 3F BF FC 32 04 D2 F5 1B

Transient Key : 7A C7 4A 43 65 48 0E 21 68 66 2D A8 01 FB 29 37
                C5 2A A2 3A 78 8F 85 24 F8 A2 26 03 CA 62 43 88
                03 F3 9B 7D 1F D0 D0 95 DC 83 51 54 69 CB 96 0A
                24 36 82 C4 80 68 A2 1C A4 E4 9E 2C A7 28 D8 98

EAPOL HMAC   : C3 D0 6C 14 EC B7 74 20 62 05 A0 55 88 38 E8 DB

C:\aircrack-ng-0.4.2-win\bin>
```



## Windows Wireless Vulnerability

News.com, "**Windows Wi-Fi vulnerability discovered**"

**Abstract:** A Windows feature that automatically searches for Wi-Fi connections can be exploited by hackers ... When a PC running Windows XP or Windows 2000 boots up, it will automatically try to connect to a [preferred] wireless network. If the computer can't set up a wireless connection, it will establish an ad hoc connection to a local address ... The danger arises if an attacker listens for computers that are broadcasting in this way, and creates a network connection of their own with that same SSID. This would allow the two machines to associate together, potentially giving the attacker access to files on the victim's PC.



# Wireless Security, or lack thereof

## Critical Broadcom Windows driver exploit released!

ZDNet.com, <http://blogs.zdnet.com/Ou/?p=365>

Exploit code: <http://www.milw0rm.com/exploits/2770>

**Abstract:** According to Johnny Cache, this particular exploit is extremely reliable and results in "100% ownage" which means your computer belongs to the hacker if it's attacked using this exploit. Since the exploit has been rolled in to the Metasploit 3.0 framework which includes kernel-level shell code, the exploit can be performed with a moderate amount of hacking knowledge. This flaw is extremely dangerous because it exploits the kernel of the operating system which means it bypasses all conventional security measures like anti-virus, HIDS, firewalls, and user privileges. The attack range is limited to Wi-Fi range which is typically 100 to 200 feet but can be extended with high-powered antennas.



## Lack of digital certificates validation on various PEAP supplicants

sans.org, <http://isc.sans.org/diary.html?storyid=4036&rss>

**Abstract:** Vulnerabilities on the digital certificate validation process associated to PEAP have been released, due to the supplicant or the deployment failing to properly validate the RADIUS server certificate: During the Shmoocon 2008 conference, Wright and Antoniewicz released the details about how the Windows XP, Mac OS X and other commercial supplicants are affected by the lack of certificates verification. All the details are available on their presentation. In the first case (best scenario), by using the default PEAP settings on Windows the certificate is validated, but the matching between the name (common name or CN) of the RADIUS server and the name on the certificate are not.



# Wireless Security, or lack thereof

## The simple hacks of open WiFi...

- Man in the middle
- Data capture and replay
- Client disconnect / de-authentication
- AP impersonation
- Frequency Jamming
- ARP and DNS spoofing
- You name it ... it all up in the air!





# Securing Wireless

- Open with VPN
- WPA or WPA2
  - Use a SSID that is not in a Dictionary
  - Use a strong passphrase
- 802.1X
  - some implementations are flawed.
- Cannot secure against radio based attacks



# What is NSU doing

## 1. The Challenge

- Manageability
- End User Configuration
- Campus and User Security
- Wireless Standards
- Hardware and Vendors

## 2. The Results

- Selection of Standards
- Hardware and Vendor Selection
- Wireless Site Survey

## 3. Pitfalls and Solutions

- Shared Computers
- PDA's

## 4. Conclusion

- Least time managing the infrastructure
- Standard Configuration = fast deployment
  - Access Points
  - End User
- Health monitoring tools
- Simple effective and secure



# End User Configuration

As simple as possible

- Standard configuration for all users
- Secure communication
- Awareness Program
  - Flyers and Web instructions



# Campus and User Security

## GOAL: Simple effective and secure

### Protect the end user

- Encryption
- Dynamic keys
- Key rotation
- Protect the Campus Network
  - VLAN's and ACL's
  - Encryption
  - Authentication
- Role-based security context
  - Automatic VLAN switching
  - Per VLAN ACL's
- User Authentication Required
- Wireless Encryption Required
- Awareness VS Technical Controls



# The Challenge Matrix

Manageability	Configuration	Security
Least time	Simple	User Authentication
Standard configuration	Standard	Role-Based Context
Simple and Secure	Secure	Encryption
Health monitoring		



# Possible Solutions

<b>Wi-Fi</b>	<b>Manageability</b>	<b>Configuration</b>	<b>Security</b>
Open	Simplest	Simplest	None
Plain Text & Authenticated	Moderate	Moderate	User Access
Encrypted & No Auth	Complex	Moderate	Data
Encrypted & Authenticated	Complex?	Complex?	User & Data

- Some Technical Jargon and ...
  - Let the fun begin!
- 802.11a/b/g/n
- 802.1x
- EAP, PEAP, LEAP, TLS, TTLS
- WEP, WPA, WPA2, TKIP, CCMP
- RADIUS, IETF, EXTENDED TAGS
- WIRELESS MESH





# Wireless Standards

	<b>PEAP with Generic Token Card (GTC)</b>	<b>PEAP with MS-CHAP Version 2</b>	<b>Cisco LEAP</b>	<b>EAP-TLS</b>
<b>User Authentication</b>	Windows NT Active Directory Novell NDS OTP	Windows NT Active Directory	Windows NT Domains, Active Directory	Windows NT Active Directory Novell NDS OTP
<b>Requires Server Certificates</b>	Yes	Yes	No	Yes
<b><u>Requires Client Certificates</u></b>	No	No	No	Yes

## Network Team:

- Select vendor supporting selected standards
- Determine needs for additional VLANS
- Conduct site survey and deploy AP's

## ■ Server Team:

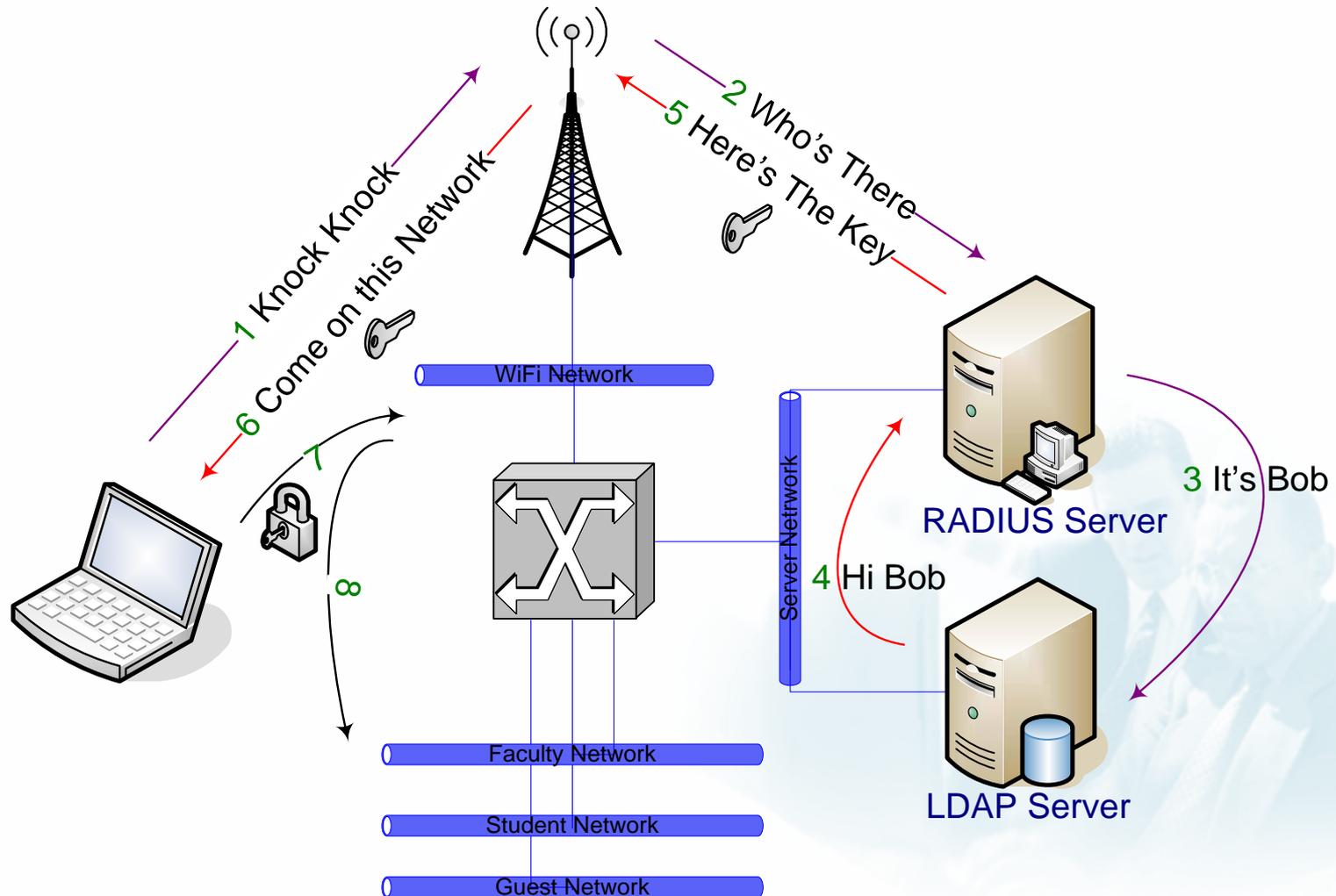
- Define/Create AD groups for VLAN mappings
  - User<->Dept mappings delegated to depts.
  - ADSI Scripts to regroup users

## ■ Security Team:

- Selecting and implementing the standards
- Defining and implementing QoS requirements

# The Implementation

## 802.1X PEAP Authentication with Dynamic VLAN Assignment



# RADIUS CONFIGURATION

- Database Mappings
  - Prioritize group mappings

Group Mappings for Domain : NSU\_LAN 

NT groups	CiscoSecure group
<a href="#">Students, *</a>	Student
<a href="#">FACULTY, *</a>	VLAN 138
<a href="#">OIT Staff, *</a>	OIT
<a href="#">Domain Computers, *</a>	Computers
<a href="#">All other combinations</a>	Default Group

# RADIUS CONFIGURATION

- Use RADIUS Shared Secret
  - Between AP and RADIUS Server
- Make good use of RADIUS Attributes
  - VLAN TAGGING

[064] Tunnel-Type

Tag 0 Value VLAN

Tag 1 Value

[065] Tunnel-Medium-Type

Tag 0 Value 802

Tag 1 Value

[081] Tunnel-Private-Group-ID

Tag 0 Value 172

Tag 1 Value

[083] Tunnel-Preference

Tag 1 Value

Tag 2 Value



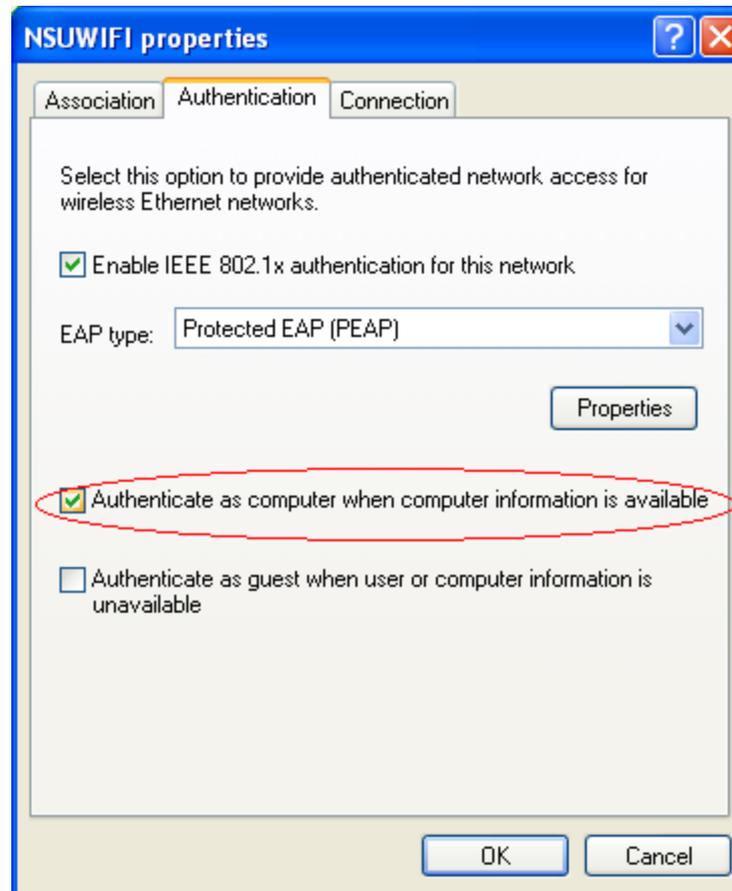
## The Instructions and the software ...

<http://www.nsu.edu/wifi>

## ... and the Pitfalls



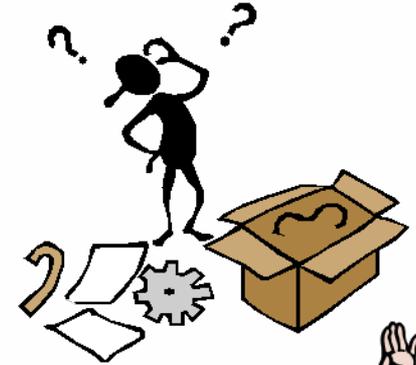
- The Problem
  - Authentication of new users
- The Solution



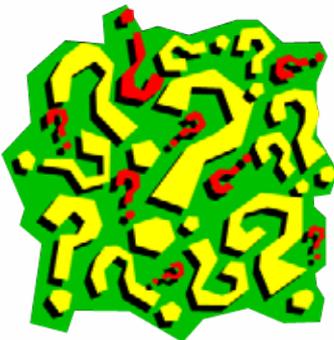
- *Auto VLAN + encryption + authentication can be SIMPLE*
- *Need for a well developed directory infrastructure*
- *Assemble a diverse team: InfoSec, Network, Server, Faculty/Staff*
- *Use well know vendors and upgradeable hardware*
- *Know the Pro and Cons in your Options*
- *Balance Security, User Access, Configuration and Administration*
  
- **802.1X PEAP MS-ChapV2 with Dynamic VLANS**
- **WPA2 AES**
- **Natively supported by Windows and MAC OS**
- **Linux Support in WPA\_SUPPLICANTS and Open1X**

# Scary Live Demos 😬





[adifabio@nsu.edu](mailto:adifabio@nsu.edu)



It's **QUESTION TIME!!**

A large yellow rounded rectangle containing three circular icons of a person thinking, a question mark with radiating lines, and the text "It's QUESTION TIME!!".



Virginia Information Technologies Agency

# Mobile Device Policy

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## Mobile Device Policy

- Policy under development and has reached draft version #3
- Two device categories
  - COV purchased devices
  - Personally owned devices
- Tablets and smart phones are essentially the same type of device



## Mobile Device Operating Systems

- Operating systems under review for known vulnerabilities and potential Enterprise-level security controls
  - Apple iOS 4.3
  - Google Android 2.2
  - Microsoft Windows 7
  - RIM Blackberry 5/6



## Mobile Device Uses/Applications

- COV-owned devices
  - COV messaging
  - Web forms/access
  - RDP/Citrix access
  - TN3270/5250
  - Custom applications
- Personally owned devices
  - COV messaging
  - Access to public facing websites



## Mobile Device Concerns

- COV-owned devices
  - Device sync/backup
  - Application purchase process and installation
  - OS updates and patches
- Personally owned devices
  - Managing data contained in device backup
  - OS updates and patches
  - Use of custom ROMs and escalation of privilege



## Questions???

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

Thank You!



Virginia Information Technologies Agency

# Personnel Security: A short review of SEC 501-01

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## SEC 501 8.1

### Personnel Security

- Purpose
  - Personnel Security requirements delineate the steps necessary to restrict access to IT systems and data to those individuals who require such access as part of their job duties.



## SEC 501 8.1

### Personnel Security

- Purpose
  - This component of the COV Information Security Program defines requirements in the following four areas:
    - Access Determination and Control
    - Information Security Awareness and Training
    - Acceptable Use
    - Email Communications



## SEC 501 8.2

# Access Determination & Control

- Purpose
  - Access Determination and Control requirements identify the steps necessary to restrict access to IT systems and data to authorized individuals.



## SEC 501 8.2

# Access Determination & Control

- Requirements
  - 1. Perform background investigations of all internal IT System users based on access to sensitive IT systems or data. Existing users may be grandfathered under the policy and may not be required to have background investigations.
  - Note: Agencies should consult the Code of Virginia § 2.2-1201.1 and Department of Human Resource Management (DHRM) Policy 2.10.



## SEC 501 8.2

# Access Determination & Control

- Requirements
  - 2. Restrict visitor access from facility areas that house sensitive IT systems or data.
  - 3. Require non-disclosure and security agreements for access to IT systems and data, based on sensitivity and risk.



## SEC 501 8.2

### Access Determination & Control

- Requirements
  - 4. Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist, as required in Section 5.2 and Section 7.2.
  - 5. Establish termination and transfer practices that require return of agency logical and physical assets that provide access to sensitive IT systems and data and the facilities that house them.



## SEC 501 8.2

### Access Determination & Control

- Requirements
  - 6. Temporarily disable physical and logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.
  - 7. Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.



## SEC 501 8.2

# Access Determination & Control

- Requirements
  - 8. Establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of the agency prohibit a complete separation of duties. Example: Such compensating controls may include increased supervisory review; reduced span of control; rotation of assignments; independent review, monitoring, and/or auditing; and timed and specific access authorization with audit review, among others.



## SEC 501 8.2

# Access Determination & Control

- Requirements
  - 9. Explicitly grant physical and logical access to sensitive IT systems and data and the facilities that house them based on the principle of least privilege.



## SEC 501 8.3 Information Security Awareness & Training

- Purpose
  - Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 1. Include any agency-specific information security training requirements in the agency information security awareness and training program. Example: An agency that processes data covered by the Health Insurance Portability and Accountability Act (HIPAA) must have an information security awareness training program that addresses specific HIPAA data security requirements.



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 2. Require that all IT system users, including employees and contractors, receive information security awareness training annually, or more often as necessary. Generally, best practice is that annual security awareness training lasts at least one hour.



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 3. Require additional role-based information security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary. Example: Agency employees and contractors who are members of the Disaster Recovery Team or Security Incident Response Team require specialized training in these duties.



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 4. Implement processes to monitor and track completion of information security training.
  - 5. Require information security training before (or as soon as practicable after) IT system users receive access rights to the agency's IT systems, and in order to maintain these access rights.



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 6. Develop an information security training program so that each IT system user is aware of and understands the following concepts:
    - a. The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
    - b. The concept of separation of duties;



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 6.
  - c. Prevention and detection of information security incidents, including those caused by malicious code;
  - d. Proper disposal of data storage media;



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 6.
  - e. Proper use of encryption;
  - f. Access controls, including creating and changing passwords and the need to keep them confidential;



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 6.
  - Note: It is considered best practice not to base passwords on a single dictionary word. It is strongly recommended that system users be educated not to base passwords on a single dictionary word.



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 6.
  - g. Agency acceptable use policies;
  - h. Agency Remote Access policies;
  - i. Intellectual property rights, including software licensing and copyright issues;



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 6.
  - j. Responsibility for the security of COV data;
  - k. Phishing; and
  - l. Social engineering.



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 6.
  - Note: Over a period of years, security awareness training should include the concepts above based on the needs of the agency relative to the sensitivity of the agency's data and IT systems.



## SEC 501 8.3

# Information Security Awareness & Training

- Requirements
  - 7. Require documentation of IT system users' acceptance of the agency's security policies after receiving information security training.



## SEC 501 8.4 Acceptable Use

- Purpose
  - Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of IT systems.



## SEC 501 8.4 Acceptable Use

- Requirements
  - 1. Document an agency acceptable use policy. Executive branch agencies must adhere to Virginia Department of Human Resource Management (DHRM) Policy 1.75 – Use of Internet and Electronic Communication Systems. Each Executive branch agency shall supplement the policy as necessary to address specific agency needs. Note: This policy can be found at [http://www.dhrm.virginia.gov/hrpolicy/policy/pol1\\_75.pdf](http://www.dhrm.virginia.gov/hrpolicy/policy/pol1_75.pdf).



## SEC 501 8.4 Acceptable Use

- Requirements
  - 2. Direct the proper use of encryption for transmitting sensitive data.
  - 3. Direct the use of an agency authorized COV warning banner to communicate that IT systems and their use may be monitored and viewed by authorized personnel; and there is no expectation of privacy when using a Commonwealth IT system.



## SEC 501 8.4 Acceptable Use

- Requirements
  - 4. Require acknowledgement that monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.



## SEC 501 8.4 Acceptable Use

- Requirements
  - 5. Prohibit users from:
    - a. Installing or using proprietary encryption hardware/software on Commonwealth systems;
    - b. Tampering with security controls configured on COV workstations;
    - c. Installing personal software on a Commonwealth system;



## SEC 501 8.4 Acceptable Use

- Requirements
  - d. Adding system hardware to, removing system hardware from, or modifying system hardware on a COV system; and
  - e. Connecting non-COV devices to a COV IT system or network, such as personal computers, laptops or handheld devices, except in accordance with the current version of the Use of Non-Commonwealth Computing Devices to Telework Standard (COV ITRM Standard SEC511).



## SEC 501 8.4 Acceptable Use

- Requirements
  - 6. Prohibit the storage, use or transmission of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with licensing and copyright laws governing the materials.
  - 7. When connected to internal networks from COV guest networks or non-COV networks, data transmission shall only use full tunneling and not use split tunneling.



## SEC 501 8.4 Acceptable Use

- Requirements
  - 8. Require documentation of IT system users' acceptance of the agency's Acceptable Use Policy before, or as soon as practical after, gaining access to agency IT systems.



## SEC 501 8.5

### Email Communications

- Purpose
  - Email shall not be used to send sensitive data unless encryption is used. As stated in the Encryption section of this Standard, encryption may be required for the transmission of data that is sensitive relative to confidentiality and integrity. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus. An email disclaimer is a set of statements that are either pre-pended or appended to emails.



## SEC 501 8.5

# Email Communications

- Purpose
  - These statements are frequently used to create awareness of how to treat the data in the email. An email disclaimer is not a substitute for judgment on what content to put into an email.



## SEC 501 8.5

### Email Communications

- Requirements
  - 1. Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality or integrity; however, digital signatures may be utilized for data that is sensitive solely relative to integrity as stated in the encryption component of this Standard. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.



## SEC 501 8.5

### Email Communications

- Requirements
  - 2. Consult with the agency's legal counsel before adopting an email disclaimer. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such.



## Questions???

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

Thank You!



Virginia Information Technologies Agency

# Information Security Standard SEC501 Changes

John Green

Chief Information Security Officer



# SEC501 Changes

- **PREFACE** - VITA's New Governance; the ITIB replaced with SOTECH and ITAC
- Various requirements throughout the standard were tweaked for clarification.
- **Major Changes:**
- **1.2 Organization of this Standard - Recommended Best Practices** are advisory in nature and provide guidance to agencies in the development of their information security programs.
- **2.7 IT Security Audits** - IT Security Audits should only be performed by independent parties who are not associated with the processes or procedures of the system.
- **4.3 System Hardening** -\_Apply all software publisher security updates to the associated software products.
- All security updates must be applied as soon as possible after appropriate testing, not to exceed 90 days for implementation.
- Prohibit the use of software products that the software publisher has designated as End-of-Life (i.e., software publisher no longer provides security patches for the software product).



# SEC501 Changes

# Con't

- **5.3 Password Management** - An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may determine the appropriate validity period of the password, commensurate with sensitive and risk. The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.
- An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitive and risk. The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.
- An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may allow the citizen to continue to use the initial password so long as the Agency provides a mechanism to the citizen that allows the citizen to create a unique initial password.
- Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for COV devices.



# SEC501 Changes

# Con't

- **6.2.2 Data Storage Media Protection** – Prohibit the storage of any Commonwealth data on IT systems that are not under the contractual control of the Commonwealth of Virginia. The owner of the IT System must adhere to the latest Commonwealth of Virginia information security policies and standards as well as the latest Commonwealth of Virginia auditing policies and standards.
- **8.3 Information Security Awareness and Training - Note:** Over a period of not more than two years, security awareness training should include the concepts above based on the needs of the agency relative to the sensitivity of the agency's data and IT systems.
- **9.5 Data Breach Notification** – added Medical Data breach guidance.

**Compliance date is 3 months after posting.**



Virginia Information Technologies Agency

# Upcoming Events





# Gartner Group Webinar Series

## Free Web seminars offered by the Gartner Group

These one-hour sessions feature tactical advice with an emphasis on reducing costs. Examples of webinars offered:

[\\*Technology & Management Directions of Smart Phones & Tablets](#)

[\\*Trends Driving Your Mobile Strategy Now Thru 2015](#)

[\\*iPad & Beyond: The Media Tablet In Business](#)

[\\*How Cloud Sourcing Is Changing The IT Services Market](#)

Visit the link to Gartner\* below to see the full listing of the topics offered and take advantage of these educational opportunities.

\* <http://my.gartner.com/portal/server.pt?open=512&objID=202&mode=2&PageID=3428358&webinarAction=webinarsGotoPage&webinarType=upcoming&page=2>



# Information Security System Association

## ISSA

**DATE:** Wednesday, April 13, 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:** Randy Trzeciak, CERT Inside Threat Team Lead

**TOPIC:** Risk Mitigation Strategies:

Lessons Learned from Actual Insider Attacks



# AITR Meeting

***Wednesday, April 13th***

*8:30 am – 9:00 am: Networking*

*9:00 am: Meeting start*

***Location: CESC***



## MS-ISAC

### *National Webcast Initiative*

Thursday, April 21  
2:00 pm – 3:00 pm EDT

Topic: *Data Life Cycle Management*

Visit MS-ISAC web for more information:

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



# Internet Security Training Workshop

Virginia Tech & SANS Institute are pleased to offer this 6-day SANS program

*<http://www.cpe.vt.edu/isect/>*

*May 17 – 22, 2011*

*Torgersen Hall at Virginia Tech  
Blacksburg, VA*

## Who Should Attend:

- *Penetration testers*
- *Ethical hackers*
- *Auditors who need to build deeper technical skills*
- *Security personnel whose job involves assessing target networks & systems to find security vulnerabilities*

- **Special pricing is available for any faculty/staff from any accredited EDU site (K-12, community college or higher education institution) or member of law enforcement. Commercial or Government employees are also welcome to attend.**

**\*\* If you wish to receive additional information about this program, please contact Randy Marchany, IT Security Lab, Virginia Tech by e-mail at [marchany@vt.edu](mailto:marchany@vt.edu)**



## Future ISOAG's

**From 1:00 – 4:00 pm at CESC**

**Wednesday - May 4, 2011**

**Wednesday - June 1, 2011**

***ISOAG will be held the 1<sup>st</sup> Wednesday of each month in 2011***



# Future IS Orientation Sessions

Tuesday - May 10, 2011  
(CESC)

9:00 – 11:30a

Tuesday - July 12, 2011  
(CESC)

1:00 – 3:30p

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



# ISOAG-Partnership Update

*IT Infrastructure Partnership Team  
Bob Baskette*

April 6, 2011



**NORTHROP GRUMMAN**



# ADJOURN

THANK YOU FOR ATTENDING

