



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

April 22, 2010



# ISOAG April 2010 Agenda

- |      |   |   |
|------|---|---|
| I.   | Welcome & Opening Remarks   | John Green, VITA  |
| II.  | Understanding an Evolving Threat Landscape through Targeted Attacks (Hydraq/Aurora) | Matthew Steele, Symantec                                |
| III. | Wide Open Wireless: How to Lose Data at the Speed of Light                          | Bob Baskette, VITA<br>Eric Taylor, NG                   |
| IV.  | 2010 General Assembly Update  | John Green, VITA  |
| V.   | Upcoming Events & Other Business  | John Green, VITA  |
| VI.  | Partnership Update  | Don Kendrick, VITA<br>Craig Drain, NG<br>Tony Shoot, NG |



# Understanding an Evolving Threat Landscape through Targeted Attacks (Hydraq/Aurora)

**Matthew Steele**

Director, Strategic Technology

# Agenda

## Definition

- Mass vs Targeted
- History & Economy

## Methodology

- Breakdown
- Summary

## Solutions

- Solutions & Challenges
- Awareness & Optimization
- Best Practices

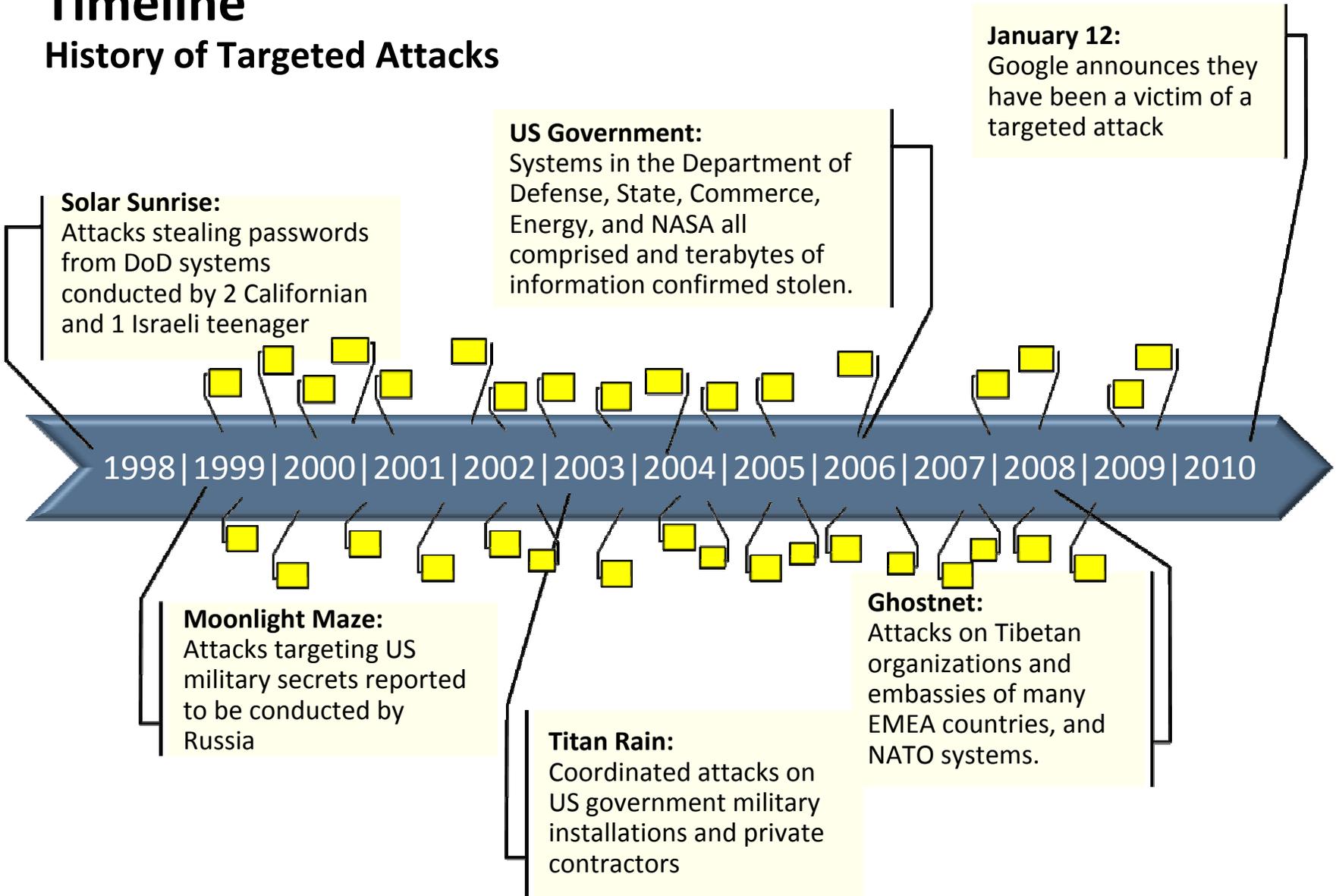
# Targeted Attacks

# Mass Attacks vs. Targeted Attacks

Phase	Mass Attack	Targeted Attack
<b>Incursion</b>	Generic social engineering By-chance infection	Handcrafted and personalized methods of delivery
<b>Discovery</b>	Typically no discovery, assumes content is in a pre-defined and predictable location	Examination of the infected resource, monitoring of the user to determine additional accessible resources, and network enumeration
<b>Capture</b>	Pre-defined specific data or data that matches a pre-defined pattern such as a credit card number	Manual analysis and inspection of the data
<b>Exfiltration</b>	Information sent to a dump site often with little protection; dump site serves as long term storage	Information sent back directly to the attacker and not stored in a known location for an extended period

# Timeline

## History of Targeted Attacks



# Underground Economy – Stolen Data

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	\$0.06–\$30
2	2	Bank account credentials	19%	17%	\$10–\$1000
3	9	Email accounts	5%	4%	\$0.10–\$100
4	3	Email addresses	5%	6%	\$0.33/MB–\$100/MB
5	12	Proxies	4%	3%	\$0.16–\$20
6	4	Full identity	4%	6%	\$0.70–\$60
7	6	Mailers	3%	5%	\$2–\$40
8	5	Cash out	3%	5%	8%–50% or flat rate of \$200–\$2000 per item
9	17	Shell scripts	3%	2%	\$2–\$20
10	8	Scams	3%	5%	\$3–\$40/week for hosting, \$2–\$20 design

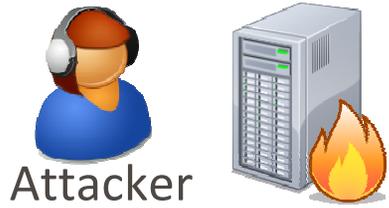
# Underground Economy – Stealing Data

Attack Kit Type	Average Price	Price Range
Botnet	\$225	\$150-\$300
Autorooter	\$70	\$40-\$100
SQL injection tools	\$63	\$15-\$150
Shopadmin exploiter	\$33	\$20-\$45
RFI scanner	\$26	\$5-\$100
LFI scanner	\$23	\$15-\$30
XSS scanner	\$20	\$10-\$30

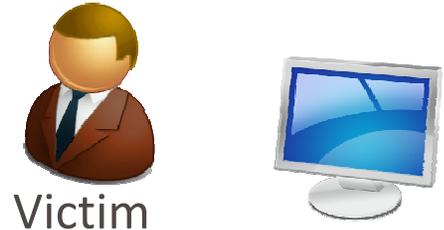
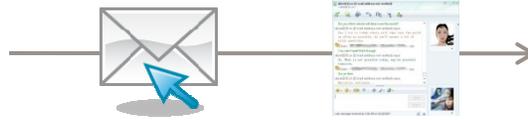
# Methodology

# Attack Methodology

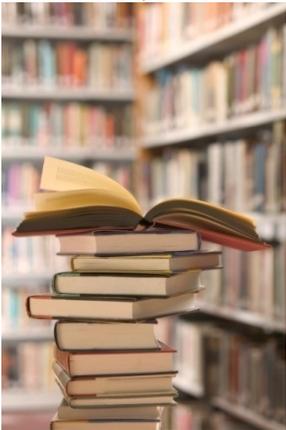
① Targeted socially engineered attack begins via email, IM, etc.



Attacker



Victim



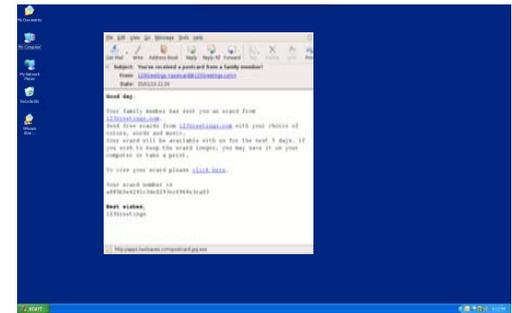
Good day.

Your family member has sent you an ecard from [123Greetings.com](http://123Greetings.com).  
Send free ecards from [123Greetings.com](http://123Greetings.com) with your choice of colors, words and music.  
Your ecard will be available with us for the next 5 days. If you wish to keep the ecard longer, you may save it on your computer or take a print.

To view your ecard please [click here](#).

Your ecard number is  
a885b5e6291c3de8293ec6968e3ca03

Best wishes,  
123Greetings

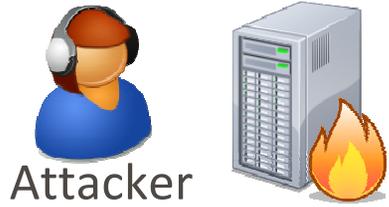


postcard.jpg.exe

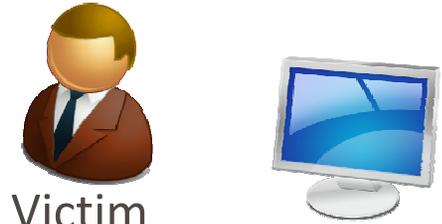
<http://apps.twooaves.com/postcard.jpg.exe>

# Attack Methodology

- 1 Targeted socially engineered attack begins, via email, IM, etc.



Attacker

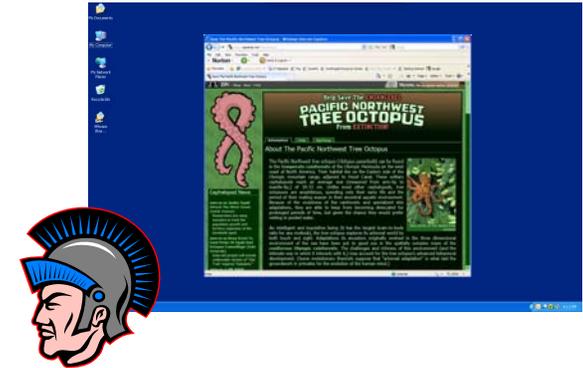
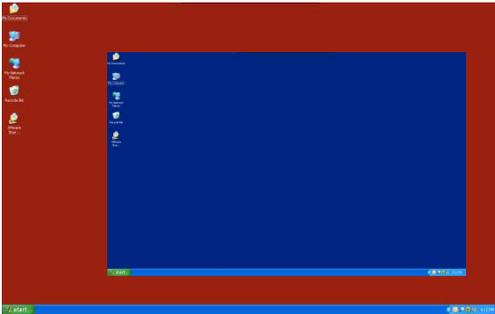


Victim

- 2 Victim unwittingly visits malicious server

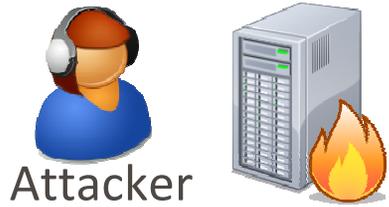


- 3 Vulnerability exploited, malicious payload delivered



# Attack Methodology

- 1 Targeted socially engineered attack begins, via email, IM, etc.



Attacker



Victim

- 2 Victim unwittingly visits malicious server



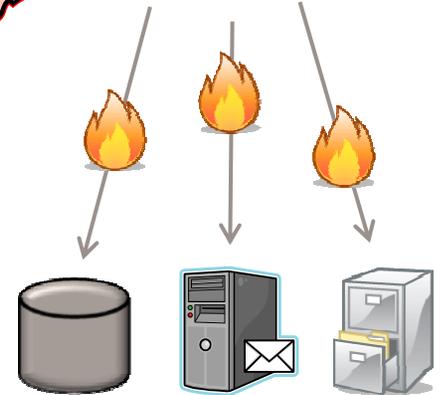
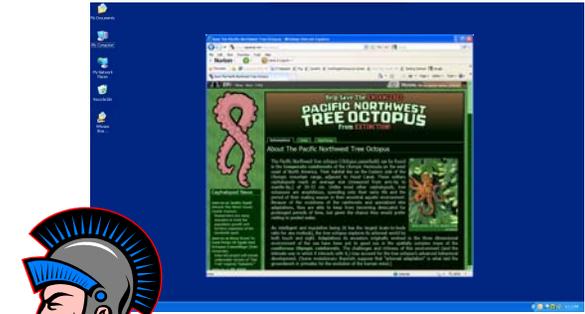
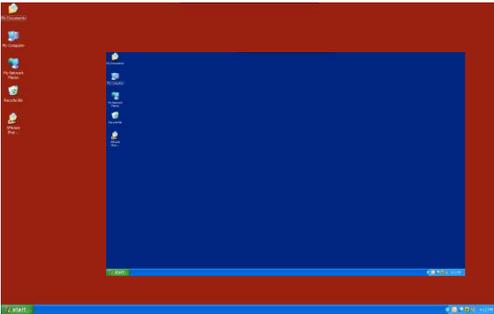
- 3 Vulnerability exploited, malicious payload delivered



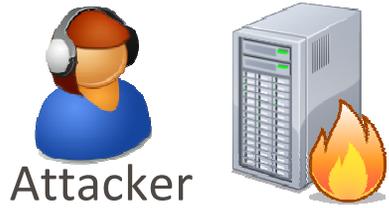
- 4 Malware "phones home" remote control established



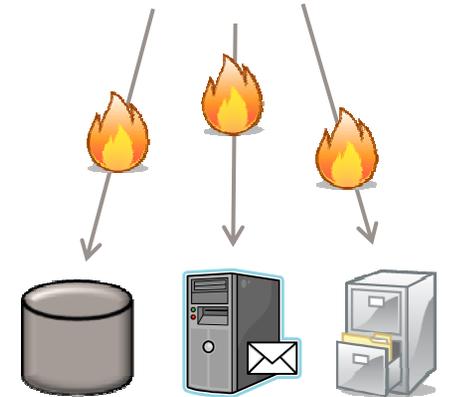
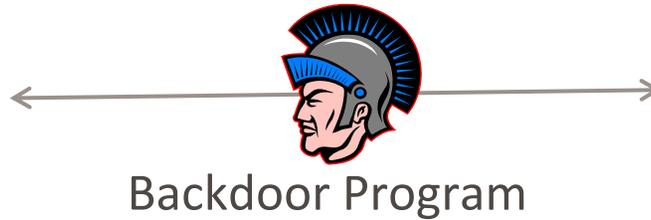
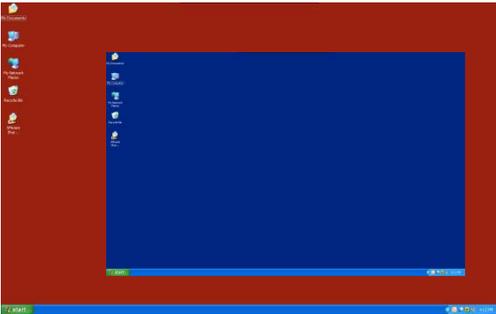
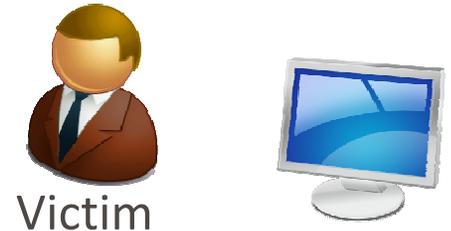
- 5 Confidential information stolen, computer becomes platform for additional exploits



# Attack Methodology



Rinse -> Wash -> Repeat

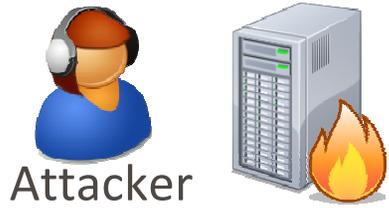


# Targeted Attack Summary

- Targeted attacks similar to Hydraq have been occurring for at least a decade
- The majority of the attacks leverage vulnerabilities for which a patch has already exists
- Attacks are personalized to the victim
- Email is primary tool for social engineering
- Web/http is primary delivery mechanism for malicious code (this includes hyper links in email)
- End points (Laptop, Desktops even mobile devices) once breached become platforms for malicious activity and code propagation.

# Solutions and Best Practices

# Technology Solutions



Attacker

Anti Spam / Fraud



SIEM

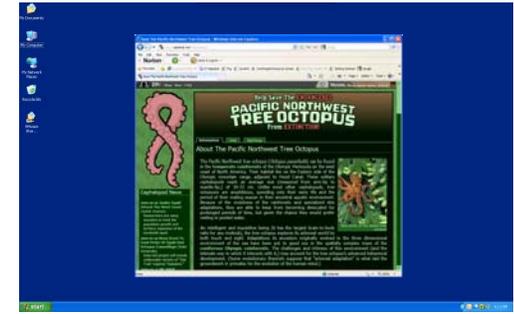
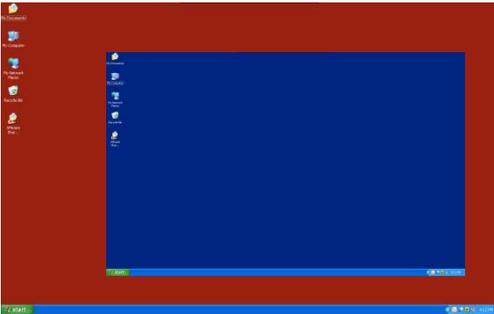


Victim

IDS/IPS URL Filters AV/Exploit



Backdoor Program



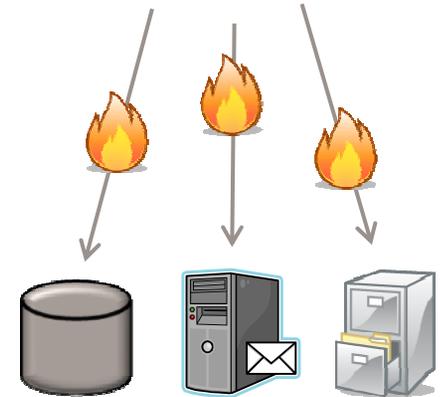
Firewall, Behavior Blocking, Reputation, DLP



Confidential Information



<http://your.stolen.info>



# Technical Challenges

Technology	Effectiveness	Reason
Email/IM SPAM Filtering	Weak	<ul style="list-style-type: none"> <li>Personalized emails to victims evade SPAM filters</li> </ul>
Anti-virus signature scanning	Weak	<ul style="list-style-type: none"> <li>Attackers can pre-scan executables with existing AV software, and modify until they are no longer detected</li> <li>Spaghetti code confuses heuristic scanning</li> </ul>
Intrusion Prevention Systems Firewalls	Moderate	<ul style="list-style-type: none"> <li>Most 0-day attacks evade IPS scanners</li> <li>Protocol anomaly detection may have blocked post-infection communications</li> </ul>
Browser Shield & Buffer Overflow Protection	High	<ul style="list-style-type: none"> <li>Doesn't require a-priori knowledge of the exploit</li> <li>Triggers on anomalies in execution path</li> </ul>
URL Blocking / Content Filtering	Weak	<ul style="list-style-type: none"> <li>Attacker-generated domains unknown to filter</li> <li>These domains were therefore typically allowed</li> </ul>
File Reputation Scanning	High	<ul style="list-style-type: none"> <li>Relies only on the community reputation of the file, which is typically low for personalized malware files</li> </ul>
Behavior Blocking	High	<ul style="list-style-type: none"> <li>Prevents malicious behaviors</li> </ul>
Data Leakage Protection	Moderate	<ul style="list-style-type: none"> <li>Network compromised, but sensitive data retained</li> </ul>

# Beyond Technology

## Awareness

(People)

- “You are part of the Problem and the Solution.”
- Weave education into regular routines. 15 minutes at a staff meeting. Pop ups on the screen.
- Engage your employees in prevention, performance, patches and signature updates.
- Promote a Situational Awareness.

## Optimization

(Process)

- “Speed is Safety”
- Time to resolution is critical in reducing risk exposure.
- Immediate Action Drill Analysis.
  - What parts of your process can be automated?
  - Can you trim Decision Tree?
- Boil your processes down using Availability vs. Security

# Best Practices

## Common Sense Security

- Apply latest security patches ASAP
- Start with Deny All then Allow, avoid granting Admin Rights where ever possible, Audit Privileges
- Limit Attack Surface by limiting allowable software

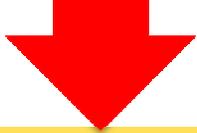
## Knowledge is Everything

- Review Access and DNS Logs
- Maintain Hardware and Software Asset Inventory
- Audit your Network (no unmanaged systems)
- Gather External Intelligence

**Questions?**

## Keep It Simple

IDENTIFY



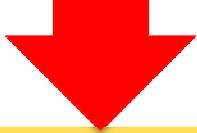
ISOLATE



REMEDiate

## Still Trying to Keep it Simple

Internal Monitoring, Global Intelligence, Correlation



Network Isolation, Application Control, Device Control



Clean, Update, Patch, Restore from Back Up



# Wide Open Wireless: How to Lose Data at the Speed of Light

Bob Baskette  
CISSP-ISSAP, CCNP/CCDP, RHCT  
Commonwealth Security Architect

## Wireless LAN Security

- The Institute of Electrical and Electronics Engineers standardized the security for wireless-based networks into two main components:
  - Encryption
  - Authentication
- IEEE Wireless Standard objective is to implement wireless LAN networks (an upper-layer feature) at Layer-2 and Layer-1 of the OSI model because they use standard interfaces into the IP layer-3
- Focuses on data privacy and access control



## WLAN Security

- Wi-Fi Alliance is a non-profit vendor-neutral organization that provides branding for 802.11-based technology known as Wi-Fi
- Wireless-based standards take advantage of the ISM band (Industrial, Scientific, and Medical radio spectrum that is deemed usable by the public)
- Most wireless products are shipped with an open-access policy (no security features enabled by default)



## Electronic Threats in a Wireless Network Environment

- Rogue Access Point
  - Provide Man-In-The-Middle attack platform
  - Spoofs a legitimate AP
  - Wireless client sends all traffic to rogue AP
  - Rogue AP copies all interesting traffic prior to sending to the legitimate destination
- Wireless sniffers/snoopers
  - Captures all traffic sent within a specific spectrum
  - Can store and extract information within the wireless network packets
  - Storage capacity only limited by available hard drive space
  - Can be tuned to monitor a specific computer or every computer in reception range
  - Wireless sniffing software can be downloaded from the Internet for free and runs under all major operating systems



## Electronic Threats in a Wireless Network Environment

- Ad-hoc access
  - Most operating systems support the concept of peer-to-peer/laptop-to-laptop/Ad-Hoc connections
  - Two laptops can communicate directly without the need for a wireless access point
  - Equivalent to allowing a malicious individual to connect an Ethernet cable to the laptop
  - Some operating systems support the concept of a wireless bridge which allows an Ad-hoc connected computer to use the Infrastructure connection to reach other networks. The malicious individual could use the Ad-Hoc connection to reach a private LAN



## Wired Equivalent Privacy

- WEP
- WEP was intended to provide confidentiality comparable to that of a traditional wired network since wireless networks broadcast messages using radio waves and therefore are much more susceptible to eavesdropping than wired networks
- WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity
- The basic WEP encryption method is to use the RC4 keystream XORed with the plaintext



# Wired Equivalent Privacy Authentication

- Open System authentication
  - The WLAN client does not provide any credentials to the Access Point during authentication
  - Any client, regardless of its WEP keys, can authenticate itself with the Access Point and attempt to associate to the network
  - No authentication will occur
  - The WEP keys are only used for encrypting the data frames
- Shared Key authentication
  - The WEP key is used for authentication
  - A four-way challenge-response handshake is used :
    - The client station sends an authentication request to the Access Point
    - The Access Point sends back a clear-text challenge
    - The client encrypts the challenge text using the configured WEP key and sends it back in an authentication request
    - The Access Point decrypts the challenge and compares it with the clear-text it had sent
  - After the authentication and association, the pre shared WEP key is also used for encrypting the data frames using RC4



## Wired Equivalent Privacy

- The 64-bit WEP installation uses a 40-bit key (AKA WEP-40)
  - The 40-bit key is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key
  - When the original WEP standard was developed, U.S. Government export restrictions on cryptographic technology limited the key size
- The 128-bit WEP installation uses a 104-bit key (AKA WEP-104)
  - The 104-bit key was permitted once the U.S. Government relaxed the export restrictions on cryptographic technology
  - The 104-bit key is concatenated with the the 24-bit IV to produce the final 128-bit WEP key
- Key size does not enhance the security provided by WEP
- Cracking a longer key requires interception of more packets, but there are active attacks that stimulate the necessary traffic



## Wired Equivalent Privacy Weakness

- Since the RC4 algorithm is a stream cipher, the same key must never be used twice
  - The purpose of the IV (transmitted as plain text) is to prevent any repetition in the key
  - A 24-bit IV is not long enough to ensure randomness on a busy network
  - A 24-bit IV allows a 50% probability the same IV will repeat after 5000 packets
  - It is possible to recover a 104-bit WEP key with probability 50% using only 40,000 captured packets
  - For 60,000 data packets, the success probability is about 80%
  - For 85,000 data packets, the success probability is about 95%
- In 2004 IEEE declared that both WEP-40 and WEP-104 "have been deprecated as they fail to meet their security goals"
- In 2008, Payment Card Industry (PCI) Data Security Standard (DSS) prohibits the use of the WEP as part of any credit-card processing after 30 June 2010



## Attack Tool Demonstration

- Break Time For Me
- Eric Taylor will now demonstrate how to attack weak Wireless configurations
- Attack Tools
  - Kismet - <http://www.kismetwireless.net/>
  - AirCrack-NG - <http://www.aircrack-ng.org/>
  - Karma - <http://trailofbits.com/karma/>



## Technologies to secure VLAN:

- Service Set Identifier
- MAC authentication
- WPA, WPA-2, 802.11
- 802.1x and EAP



## SSID

- Service Set Identifiers
- Arbitrary ID or name for a wireless LAN that logically segments the subsystem
- Provides basic access control mechanisms
- All wireless devices require attachment through the SSID to bind with the WLAN
- Not a true security mechanism, but can prevent unauthorized access to clients that do not know the valid SSID
- Recommended to disable the SSID beacon message/will break the Windows Wireless Zero Configuration feature



## MAC Authentication

- MAC address-based authentication
- Allows network access to Known MAC addresses (locally configured list of allowed addresses or external authentication server)
- Can be circumvented by using MAC spoofing
- MAC authentication is not specified in the 802.11 standard



## IEEE 802.11i

- Standard defines the core security standards for WLAN networks
- Provides stronger encryption, authentication, and key management
- Includes two new confidentiality protocols:
  - TKIP
  - AES



## IEEE 802.11i

- 802.11i standard includes two encryption enhancements for all Known WEP vulnerabilities:
- **Temporal Key Integrity Protocol**
  - TKIP
  - Software enhancement to the RC-4 based encryption algorithm
  - Adds measures such as per-packet keying (PPK), message integrity check (MIC), and broadcast key rotation
- **Advanced Encryption Standard**
  - AES-CCMP (Counter Mode with CBC-MAC = CCM)
  - AES is the encryption algorithm
  - CCM is the data privacy algorithm
  - Cipher Block Chaining Message Authentication Code
  - CBC-MAC component of CCMP provides data integrity and authentication



## Wi-Fi Protected Access

- **WPA**
  - Standard security solution from the Wi-Fi Alliance
  - Addresses all known WEP vulnerabilities in the original 802.11 standard
  - Uses TKIP for encryption
  - Based on RC-4 algorithm
  - Supports pre-shared key (PSK)
  - Supports 802.1x/EAP modes for authentication
  - PSK Verification works via a password or pass phrase on both the client and AP



## Wi-Fi Protected Access

- **WPA-2**
  - Wi-Fi interoperable implementation of the 802.11i standard
  - Provides stronger encryption mechanism through AES-CCMP
  - Supports PSK and 802.1x/EAP modes of operation for authentication



## Wi-Fi Protected Access

- **WPA and WPA-2 operation modes:**
  - Both provide encryption and authentication support
  - **Personal Mode**
    - Supports wireless products by using the PSK mode of operation for authentication
    - Pre-shared Key must be manually configured on the client and AP
    - Authentication server is not required
  - **Enterprise Mode**
    - Supports wireless products by using both the PSK and IEEE 802.1x/EAP modes of operation for authentication
    - AAA server using the RADIUS protocol is required when using 802.1x mode for authentication, key management, and centralized management of user credentials



## Wi-Fi Protected Access

- **Personal Mode**
  - WPA Authentication = PSK
  - WPA Encryption = TKIP/MIC
  - WPA-2 Authentication = PSK
  - WPA-2 AB Encryption = AES-CCMP
- **Enterprise Mode**
  - WPA Authentication 802.1x/EAP
  - WPA Encryption = TKIP/MIC
  - WPA-2 Authentication = 802.1x/EAP
  - WPA-2 Encryption = AES-CCMP



## IEEE 802.1x and EAP

- RFC 4017 EAP methods in WLAN authentication
- EAP provides
  - Universal authentication framework, not a specific authentication mechanism
  - Provides common functions and communication specifications for an authentication mechanism
  - EAP methods can be used in 802.1x solutions to provide identity-based network access control
  - Choosing the correct CAP mechanism depends on the client, the policy, and existing infrastructure:
    - Is there a Certificate Authority PKI available
    - What client platforms are supported
    - Are there any existing authentication servers



## Common EAP Methods

- EAP Message Digest 5 (EAP-MD5)
- EAP Transport Level Security (EAP-TLS)
- EAP Transport Level Security (EAP-TTLS)
- EAP Flexible Authentication via Secure Tunnel (EAP FAST)
- Protected EAP (PEAP)



## Questions???

For questions or more information, please contact:  
[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)

Thank You!



# General Assembly Legislation Session 2010

John Green  
Chief Information Security Officer



## HB518

**Freedom of Information Act; applicability; disclosure of criminal records; noncriminal incident information.**

Clarifies that the Virginia Information Technologies Agency (VITA) is not the custodian of records stored or maintained by VITA on behalf of other state public bodies. Such records, however, shall be provided by VITA upon the request of any state public body for which VITA stores or maintains such agency's records in with FOIA. However, other records of VITA shall be public records and subject to FOIA. The bill also expands the exemption for criminal investigative files and clarifies that noncriminal incident materials held by any state or local law-enforcement agencies are exempt from the mandatory disclosure provisions of FOIA. **Patron: Rust**

**Status:**

**04/11/10 Governor: Approved by Governor-Chapter 627 (effective 7/1/10)**



## HB 920

**Computer Crimes Act; definition of computer and computer network.**

Amends the definition of "computer" by adding cellular phones and other wireless telecommunications devices to the definition. The bill also clarifies that wired or wireless networks fall within the definition of "computer network." ***Patron: Bell***

***Status:***

***02/03/10 House: Passed by in Science and Technology with letter by voice vote***



## HB1015

**Secretary of Administration; telecommuting and alternative work schedules for state employees; effectiveness.**

Provides that the Secretary of Administration, in cooperation with the Secretary of Technology, shall measure the effectiveness of the comprehensive statewide telecommuting and alternative work schedule policy. The bill provides that the head of each agency shall report annually to the Secretary on the status of any programs or policies developed and implemented pursuant to this section. Any agency head failing to comply with the requirements of this section shall forfeit one percent of the moneys appropriated for the operation of the agency as provided in the appropriation act. The Secretary shall so notify the Comptroller, who shall take such moneys and deposit them into the Literary Fund. The bill also requires the Department of Human Resource Management to notify state employees by email, or other method deemed appropriate by the Department, of the statewide telecommuting and alternative work schedule policy. *Patron: Hugo*

***Status:***

***02/10/10 House: Continued to 2011 in Science and Technology by voice vote***



# HB1034

**Information Technology governance in the Commonwealth; the Secretary of Technology; the Chief Information Officer; the Information Technology Investment Board; the Information Technology Investment Council, established.**

The bill eliminates the Information Technology Investment Board (ITIB) and replaces it with the Information Technology Investment Council (ITIC), which is established as a policy council under the Governor with the power and duty to advise the Chief Information Officer (CIO) on: (i) development of all major information technology projects; (ii) strategies and standards regarding state agency use of information technology; and (iii) the development of enterprise applications, application budgets, and infrastructure expenditures. The ITIC also has the power and duty to approve the statewide four-year strategic plan developed by the CIO and approve statewide technical and data standards. The ITIC is composed of 10 agency representatives from each Cabinet Secretary, the Secretary of Technology, the CIO, the APA, and no more than two citizens, all to be appointed by the Governor. The Secretary of Technology serves as chair and the CIO as vice chair.

The bill requires the Secretary of Technology, in addition to existing duties, to develop criteria defining a "major information technology project" and, upon recommendation of the CIO, approve the procurement of such projects.

The bill grants the Governor the power to appoint the Chief Information Officer (CIO), who shall serve as the head of the Virginia Information Technologies Agency (VITA). The CIO reports to the Secretary of Technology and is responsible, through his role as head of VITA, for planning, developing, and procuring enterprise applications and infrastructure services. The CIO is also responsible for planning, developing, and soliciting contracts for major information technology projects. The CIO may enter such contracts only upon approval of the Secretary of Technology. The CIO may suspend a major information technology project but such project may only be terminated by the Secretary of Technology. The CIO appoints a Chief Applications Officer (CAO) subject to the approval of the Secretary of Technology. The CAO oversees, but the CIO approves, annual agency technology application budgets and expenditures.

This bill contains additional substantive changes to information technology governance in the Commonwealth as well as numerous technical changes. **Patron: Byron**

## **Status:**

**03/11/10 Governor: Acts of Assembly Chapter text (CHAP0136)**



## Changes to 2.2-2009

- Changes in HB1034 that affect information security in the Commonwealth:

§ 2.2-2009 C. The CIO shall *annually* report to the Governor, *the Secretary*, and General Assembly by December 2008 and annually thereafter, 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 and *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 the (i) Information Technology Investment Board *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 Information Technology Investment Board *CIO* may take action to suspend the public bodies *body's* information technology projects pursuant to subdivision 3 of § 2.2-2458 § 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.*



## Changes to 2.2-2009

- More changes in HB1034 that affect information security in the Commonwealth:

*§ 2.2-2009 H. The CIO shall also develop policies, procedures, and standards that shall address the creation and operation of a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps. All agencies in the Commonwealth shall cooperate with the CIO. Such cooperation includes, but is not limited to, (i) providing the CIO with information required to create and implement a Commonwealth risk management program; (ii) creating an agency risk management program; and (iii) complying with all other risk management activities.*



## HB1035/SB236

**Information Technology governance in the Commonwealth; the Chief Information Officer; the Information Technology Investment Board; the Department of Technology Management, established; the Information Technology Investment Council, established; and the Council on Technology Services, established.**

The bill eliminates the Information Technology Investment Board (ITIB) and replaces it with the Information Technology Investment Council (ITIC), which is established as a policy council under the Governor with the power and duty to (i) approve the recommended technology investment projects report prepared by the Project Management Division; (ii) approve plans for the development, maintenance, and replacement of enterprise and multiagency applications developed by the Council on Technology Services (COTS); and (iii) advise the Secretary of Technology on the termination of major information technology projects. The ITIC is comprised of each Cabinet Secretary, the Directors of the Senate Finance and House Appropriations Committees, and three non-legislative citizen members, all of whom to be appointed by the Governor. The Governor's Chief of Staff serves on the ITIC as chairman.

The bill grants the Governor the power to appoint the Chief Information Officer (CIO), who shall serve as the head of the Virginia Information Technologies Agency (VITA). The CIO reports to the Secretary of Technology and is responsible, through his role as head of VITA, for planning, developing, and procuring enterprise applications and infrastructure services.

The bill establishes the Department of Technology (DTM) with the power and duty to (i) develop regulations, standards, policies, and guidelines for management of information technology in the Commonwealth; (ii) oversee information technology security, procurements, projects, investments, planning, and budgeting; (iii) report on information technology status and trends in the Commonwealth; and (iv) in consultation with VITA, identify and plan for the information technology needs of the Commonwealth. The Department is led by a Director who is appointed by the Governor, confirmed by the General Assembly, and reports to the CIO. The Department includes the Project Management Division, the Virginia Geographic Information Network, and the Public Safety Communications Division, all of which were previously under the supervision and responsibility of VITA.



## HB1035/SB236 (con't)

The bill establishes the Council on Technology Services (COTS) as a policy council under the Governor with the power and duty to (i) advise the CIO on the application and infrastructure services provided by VITA; (ii) advise the Director of DTM on the development of information technology regulations, standards, policies, and guidelines; the list of recommended technology investment projects and proposed uses of state funds resulting from agency budget reviews; and (iii) develop, for approval by the ITIC, plans for the development, maintenance, and replacement of enterprise and multiagency applications. COTS is comprised of agency representatives from each of the Cabinet Secretaries and the legislative and judicial branches of state government.

The bill creates a new requirement that the Secretary of Technology develop a comprehensive statewide two-year strategic plan for information technology that addresses application and infrastructure needs, the use of information technology across state government, and information security issues. The Secretary is also responsible for the newly created DTM and shall coordinate and resolve any conflicts between DTM and VITA.

The bill contains several enactment clauses, including the provision that no additional funds from the general appropriation act passed by the 2010 Session of the General Assembly shall be used to implement the provisions of this act. Any additional funding necessary to implement the provisions of this act shall be provided from internal service funds maintained by VITA. This bill contains other substantive provisions and includes numerous technical changes necessary to update obsolete references. **Patron:** *Byron/Howell & Stosch*

**Status:**

**02/03/10 House: Incorporated by Science and Technology [\(HB1034-Byron\)](#) by voice vote**

**03/11/10 Governor: Acts of Assembly Chapter text (CHAP0145)**



## HB1039

### Notification of breach of medical information.

Requires notification to residents of the Commonwealth if their unredacted or unencrypted medical information or insurance information is the subject of a database breach. The notification required by this section would apply only to entities not subject to federal medical information database breach notification regulations. ***Patron: Byron***

### ***Status:***

*04/13/10 House: Governor's recommendation received by House*



## HB1144

**State employee telecommuting and alternative work schedule goals.**

Increases the target for eligible state employee participation in telecommuting and alternative work schedules to 40 percent in each respective program by January 1, 2012. ***Patron: Scott***

***Status:***

***02/10/10 House: Continued to 2011 in Science and Technology by voice vote***



## HB1207

### Computer trespass; penalty.

Expands the crime of computer trespass to include video and image capture software (screenshots) in addition to keyboard loggers. The provision does not apply to certain Internet, software, and hardware providers that provide network and data security services, technical assistance, or network management. The bill also authorizes recovery of damages in civil actions, including lost profits. ***Patron: Albo***

### ***Status:***

***03/08/10 Senate: Continued to 2011 in Finance (12-Y 0-N)***



# HB1361

**Computer and digital forensic services; exempt from regulation as a private security service business.**

Exempts from regulation as a private security service business any individual engaged in (i) computer or digital forensic services or in the acquisition, review, or analysis of digital or computer-based information, whether for purposes of obtaining or furnishing information for evidentiary or other purposes or for providing expert testimony before a court or (ii) network or system vulnerability testing, including network scans and risk assessment and analysis of computers connected to a network. ***Patron: Keam***

***Status:***

***02/10/10 House: Continued to 2011 in Courts of Justice by voice vote***



## SB242

### **Intellectual property created by state employees.**

Adds new reporting requirements for agencies that seek patent protection or seek to license or transfer any interest in intellectual property developed by state employees. The bill also makes several technical changes to the requirements of the intellectual property policy developed by the Secretary of Administration. To accommodate the technical changes, the bill also extends the reporting deadline for the Secretary of Administration in developing a statewide policy and guidelines.

***Patron: Watkins***

### ***Status:***

***03/03/10 House: Passed by in Science and Technology with letter by voice vote***



## SB332

### Virginia School for the Deaf and the Blind; VITA exemption.

Exempts the Virginia School for the Deaf and the Blind from provisions related to the Virginia Information Technologies Agency. *Patron: Hanger*

#### ***Status:***

***02/10/10 Senate: Continued to 2011 in General Laws and Technology (15-Y 0-N)***



## SB390/SB480

**Information Technology governance in the Commonwealth; Chief Information Officer and the Information Technology Investment Board; emergency.**

Eliminates the Information Technology Investment Board. In its place, the Governor will appoint the Chief Information Officer of the Commonwealth, subject to confirmation by the General Assembly. The bill contains an emergency clause. ***Patron: McDougle/Howell & Stosch***

***Status:***

***02/10/10 Senate: Incorporated by General Laws and Technology (SB236-Howell) (15-Y 0-N)***

***02/10/10 Senate: Incorporated by General Laws and Technology (SB236-Howell) (15-Y 0-N)***



# QUESTIONS?





# Upcoming Events





# Launch of CSRM Communications

- Webcasts
- ISO Collaboration Distribution List
- News postings on the CSRM Resource Center
- Twitter Announcements/Alerts
- ISO Sharepoint Portal?
  
- Focus on community, collaboration, and communication



## Future ISOAG's

From 1:00 – 4:00 pm at CESC

(please let us know if you want to host in the Richmond area!)

Wednesday - May 12, 2010

Wednesday - June 16, 2010 - @ DMV!  
*(Thank you Norm Hill for coordinating this!)*

Thursday - July 22, 2010



# Future IS Orientation Sessions

<b>Monday -</b>	<b>May 3, 2010</b>	<b>1:00 – 3:30 (CESC)</b>
<b>Tuesday -</b>	<b>July 6, 2010</b>	<b>1:00 – 3:30 (CESC)</b>
<b>Tuesday -</b>	<b>September 7, 2010</b>	<b>9:00 – 11:30 (CESC)</b>
<b>Monday -</b>	<b>November 1, 2010</b>	<b>1:00 – 3:30 (CESC)</b>



## DHS/FEMA State Cyber Security Training Program

The Adaptive Cyber-Security Training Online (ACT-Online) courses are now available on the TEEX Domestic Preparedness Campus. This training is designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure.

Cost is Free!! Students earn a DHS/FEMA Certificate of Completion along with Continuing Education Units (CEU) at the completion of each course.

No-Charge registration is available at the host site:

<http://www.teexwmdcampus.com>

*Thanks to Cameron Caffee, VDOT, for this information!*



# Information Security System Association

ISSA meets on the second Wednesday of every month

**DATE: Wednesday, May 12, 2010**

**LOCATION: Maggiano's Little Italy, 11800 W. Broad St.,  
#2204, Richmond/Short Pump Mall**

**TIME: 11:30 - 1:30pm. Presentation starts at 11:45 &  
Lunch served at 12.**

**PRESENTATION: Security Trends & Best Practices  
by Juniper**

**COST: ISSA Members: \$10 & Non-Members: \$20**



# SANS

Host: Virginia Tech

Ed Skoudis' Class - SEC 560 Network Pen Test & Ethical Hacking

Date: May 17-22, 2010

Cost: \$800 per person (regular price \$3550) for state and local government employees including LEO

Visit: [www.cpe.vt.edu/isect](http://www.cpe.vt.edu/isect)



## MS-ISAC Webcast

# National Webcast!

Wednesday, June 23, 2010, 2:00 to 3:00 p.m.

**Topic: Incident Response**

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



## Identity Theft Red Flags Rules Extended Until June 1, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until June 1, 2010. Read the FAQ at:  
<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



## Security Awareness Tools

For those of you here in Chester, we have Security Awareness Tools available for you!

Security Bookmarks!  
Security Brochures!  
Security Posters!  
*Duh's of Security DVD!*

- All of these tools and many more can be downloaded from the toolkit website

<http://www.vita.virginia.gov/security/default.aspx?id=5146>



Virginia Information Technologies Agency

Any Other Business ???????





# ISOAG-Partnership Update

*Don Kendrick*

*IT Infrastructure Partnership Team*

April 22, 2010



**NORTHROP GRUMMAN**

# Section Agenda

- Windows Patching Story
  - Agency Maintenance windows
  - Contract SLAs
  - How ISOs can support
- End User Services Software Roadmap
  - What is it
  - Quarterly Update
- Partnership Q & A



# Windows Patching Story

April 22, 2010



***NORTHROP GRUMMAN***

# Pre-Transformation

- No Centralized Enterprise Management System
  - Different tools for different Agencies/groups such as
    - Shavlik
    - Windows Server Update Service (WSUS)
    - Windows Update
    - Manual update processes
  - Is that resource patched or not?
    - No verification process for enterprise environment
    - No central compliance reporting ability for enterprise environment

# Current

- Altiris Enterprise Management System goes live 1 Sept 2009
  - One tool for all managed servers and workstations (WS) (includes Laptops); with Altiris agents installed.
  - Altiris agents start report to Altiris DB on missing patches since 1998
    - missing approx. 110K possible applicable patches on over 2900 servers
    - missing approx. 1.74M possibly applicable patches on over 43,000 workstations
  - Mission: Surge on eleven years of missing patches and maintain regular patching
    - Surge (Base-lined to Oct 2009: 92 and 88 percent of possibly applicable missing patches installed for WS and server, respectively. (as of 4/12/2010)
    - Regular (Patch Cycles since Nov 2009): 92 percent of 1 Million and 75 percent of 75K possibly applicable patches installed for WS and server, respectively. (as of 4/12/2010)

# Current

- During this effort:
  - Workstations (2,520,800 patches installed):
    - No Sev 1 or 2 tickets as a result
    - Eight to ten other tickets for network latency; root cause Altiris using bandwidth; rollouts postponed, realigned, and fulfilled; with the exception of one agency
    - Several unique resources at one Agency experienced conflicts between one patch from 2006 and the BIOS version; BIOS upgraded; issue resolved
    - One Agency will not allow Altiris package server connections—8% of outstanding patches
  - Servers (153,050 patches installed):
    - Two Sev 1 tickets; caused loss of functionality; resolved
    - Less than 8 other tickets; minor impact, resolved
    - Three Agencies delaying patching--68% of outstanding patches

# Future

- Central Enterprise Management System for Managed Resources
- One tool to patch them all. Consolidated approach
- Is that resource patched or not?
  - Hone patch verification process for enterprise environment compliance
  - Provide central compliance management reporting feedback for ITP and Agency ISOs
- Agency facilitation:
  - Work with Service Delivery personnel to provide consistent maintenance windows for patching effort
  - Work with Service Delivery personnel to establish pilot resource candidates for servers and workstations to ensure continuation of business functionality
  - Encourage Laptop users to connect into the network once every two weeks or more often as duties allow

# Patching SLAs

System Server Administration Service Level Requirements			
System Server Administration Task	Service Measure	Performance Target	Minimum Performance %
Deploy service / security patches / anti-virus updates necessary to fix/repair environment vulnerabilities	Elapsed Time	Upon receipt for VITA-directed HIGH risk vulnerability	95%
		24 hours for other HIGH risk vulnerability	
		48 hours for MEDIUM risk vulnerability	
		Within next maintenance window for LOW risk vulnerability	
		*Contingent on completion of systems assurance testing in accordance with VITA procedures	
	Formula	Number of requests completed within Performance Target / Total of all requests occurring during Measurement Interval	
	Measurement Interval	Measure Weekly, Report Monthly	
	Measurement Tool	HP ServiceCenter	

Northrop Grumman Proprietary Level I/Sensitive to VITA

## Your part...

- Need to define regular patching windows in alignment with vendor patch release schedules.
- Support the patching effort through designating pilot users, defining acceptance criteria, reducing FUD.
- Understand the shared risk environment.



# EUS Product Roadmaps

April 22, 2010

***NORTHROP GRUMMAN***

VITA Program

# Roadmaps, What are they?

- Used to provide planning insight for the program. Useful to the agencies to synchronize with agency development plans.
- Denotes operational readiness and availability for specific technologies.
- Specific agency implementation schedules are developed within the availability windows defined.
  - Communications and schedules to be facilitated through conversations with the AOM's.

# Intentionally Omitted

# Intentionally Omitted

# Intentionally Omitted



## Partnership Q & A

- Don Kendrick, Sr Manager, Security Operations and Architecture, VITA
- Craig Drain, Program Security Officer, NG
- Tony Shoot, Manager, Enterprise Architecture, NG

April 22, 2010



***NORTHROP GRUMMAN***



**ADJOURN**

**THANK YOU FOR ATTENDING**

