



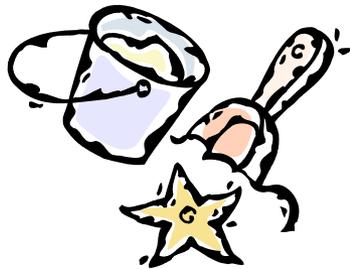
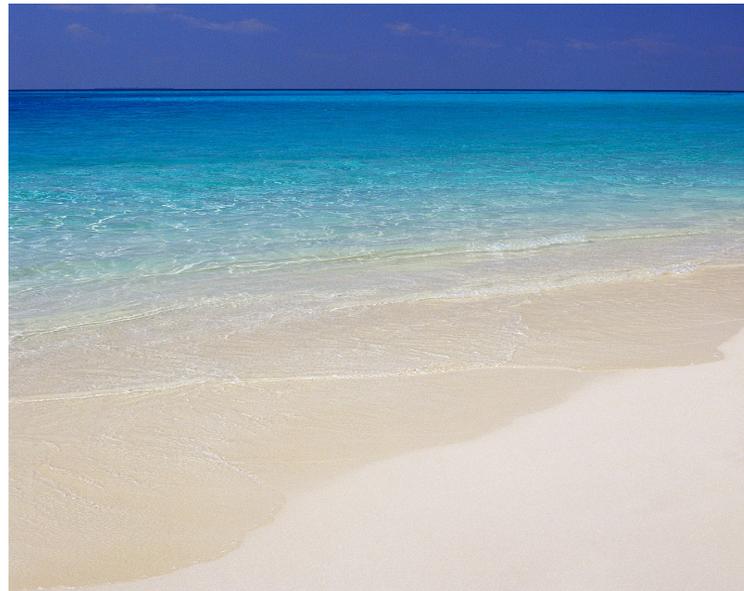
*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

August 12, 2009

# August





# ISOAG August 2009 Agenda

- |       |  |                         |
|-------|--|-------------------------|
| I.    | Welcome & Opening Remarks                                  | Peggy Ward, VITA        |
| II.   | Cyber Governance   | Dr. Kenneth Brancik, NG |
| III.  | Virginia.gov DNSSEC  | Eric Taylor, NG         |
| IV.   | Partnership Security Update                                | Don Kendrick, VITA      |
| V.    | 2009 COV Security Policy & Standard                        | John Green, VITA        |
| VI.   | Commonwealth Information Security Council                  | Peggy Ward, VITA        |
| VII.  | 2009 Commonwealth Security Data Points                     | Peggy Ward, VITA        |
| VIII. | Physical Security: Protecting Your Users and What They Use | Bob Baskette, VITA      |
| IX.   | COVITS 2009  | Peggy Ward, VITA        |
| X.    | Upcoming Events and Other Business                         | Peggy Ward, VITA        |



# **Cyber Governance**

*Managing the Integrated Governance, Risk  
Management and Compliance (iGRC)  
Process to reduce Cyber risks*

*Dr. Kenneth C. Brancik,  
CISM, CISSP, CISA, ITIL*

# Introduction - BIO

Northrop Grumman Information Systems  
(NGIS)

- **Advanced Technology Group (ATG)**
- **Principal Security Architect**

Director at VerizonBusiness Security  
Solutions (Trusted Security Advisor)

Former Federal Bank Regulator for  
approximately 15 years with the US  
Treasury (OCC) and the NY FED

Worked on Wall Street for several years in  
Auditing Technology Risk (Merrill Lynch &  
CITIGROUP)

Manager within PwC's Assurance and  
Business Advisory Services Line of Service  
for the Federal Sector

Published Author (Insider Threat)



The Role and Importance of the Cyber Governance Process

Security Assessments are an important component of Cyber Governance and should be performed on a continuous basis to reduce operational risk

Effective Identity and Access Management can reduce Cyber risks

INFOSEC Scorecards are an effective way of scoring Cyber hygiene and risk profile

Cyber Threat Modeling should address the entire Threat Landscape to address both internal and external attacks

Migrating from a Network Centric to a data centric security architecture requires a strong understanding of data flows

Regulatory compliance can be achieved in a cost effective manner, through an effective Cyber Governance Process

An understanding of the evolving Cyber threat vectors can aide in the decision-making process for the selection of an appropriate Defense in Depth Security Architecture

Developing security metrics can assist in measuring incremental improvements in Cyber defenses

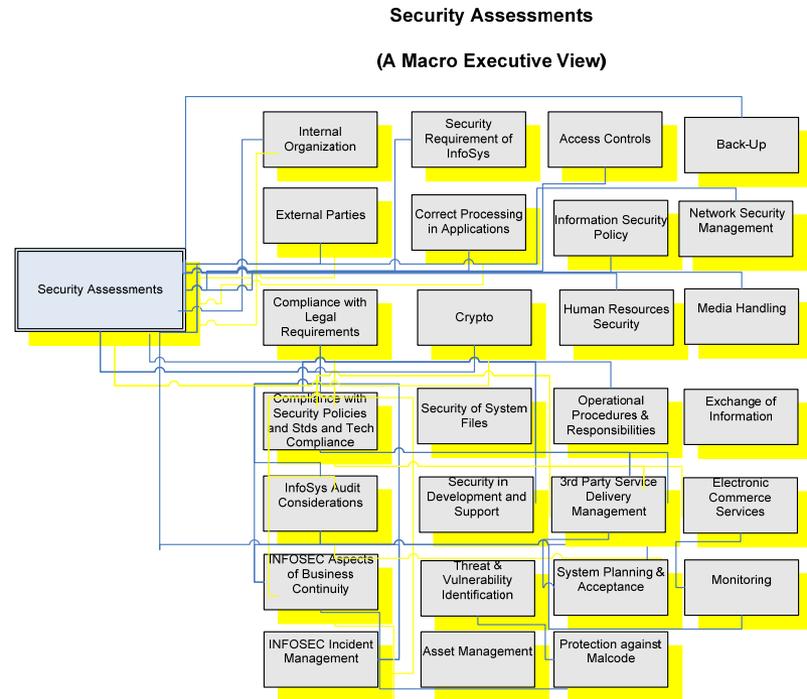
# Cyber Governance (Begins with a Security Assessment)

## A *MACRO* Taxonomy of *Security Assessments*

Cyber Governance: Includes an on-going process for Integrated Security Assessment (ISA), Risk Modeling / Mitigation, Solutioning and Performance Management

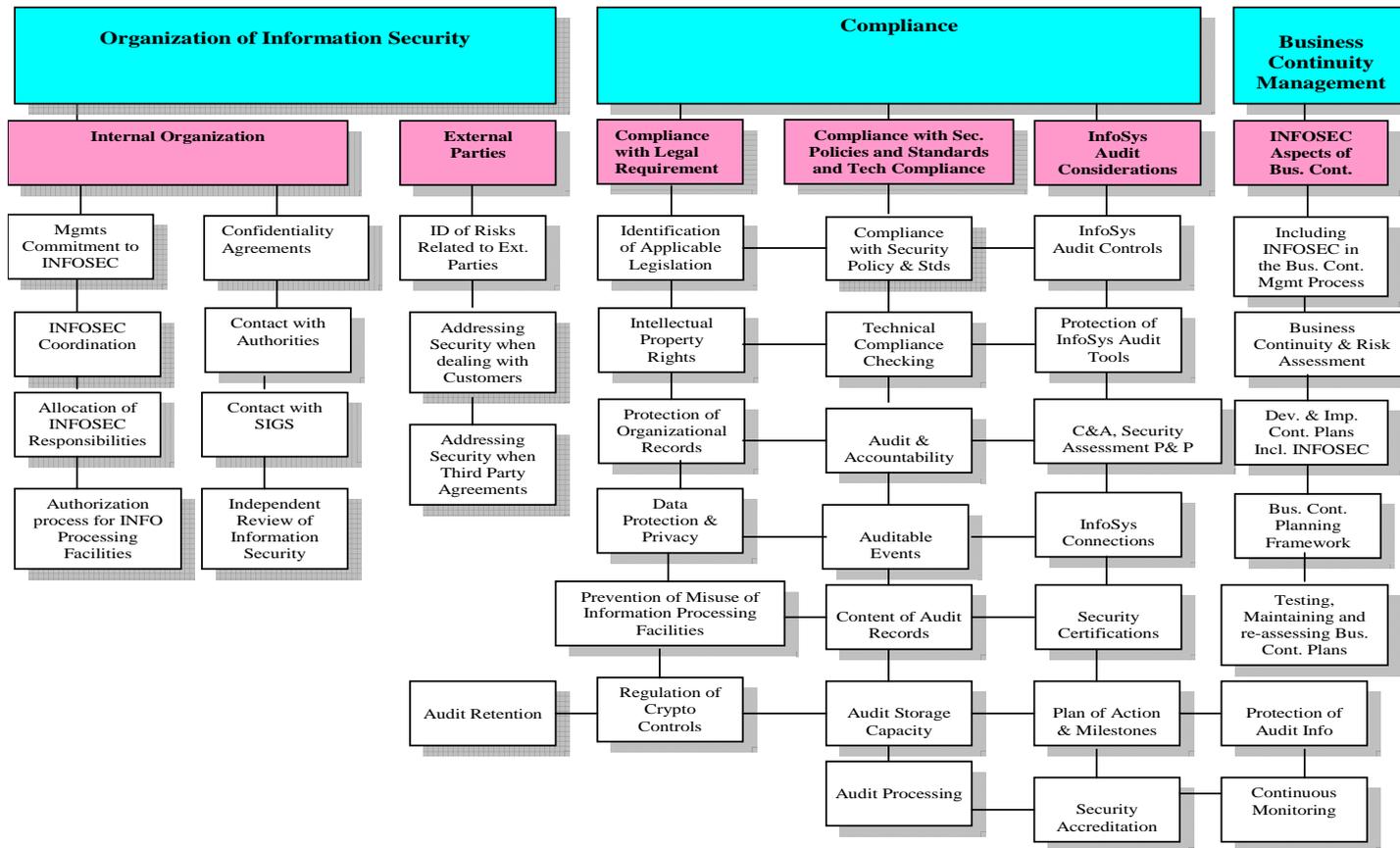
Key *Security Assessment* Risks include, but are not limited to the absence of effective controls over the following components:

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination



# A Micro Taxonomy of Security Assessments

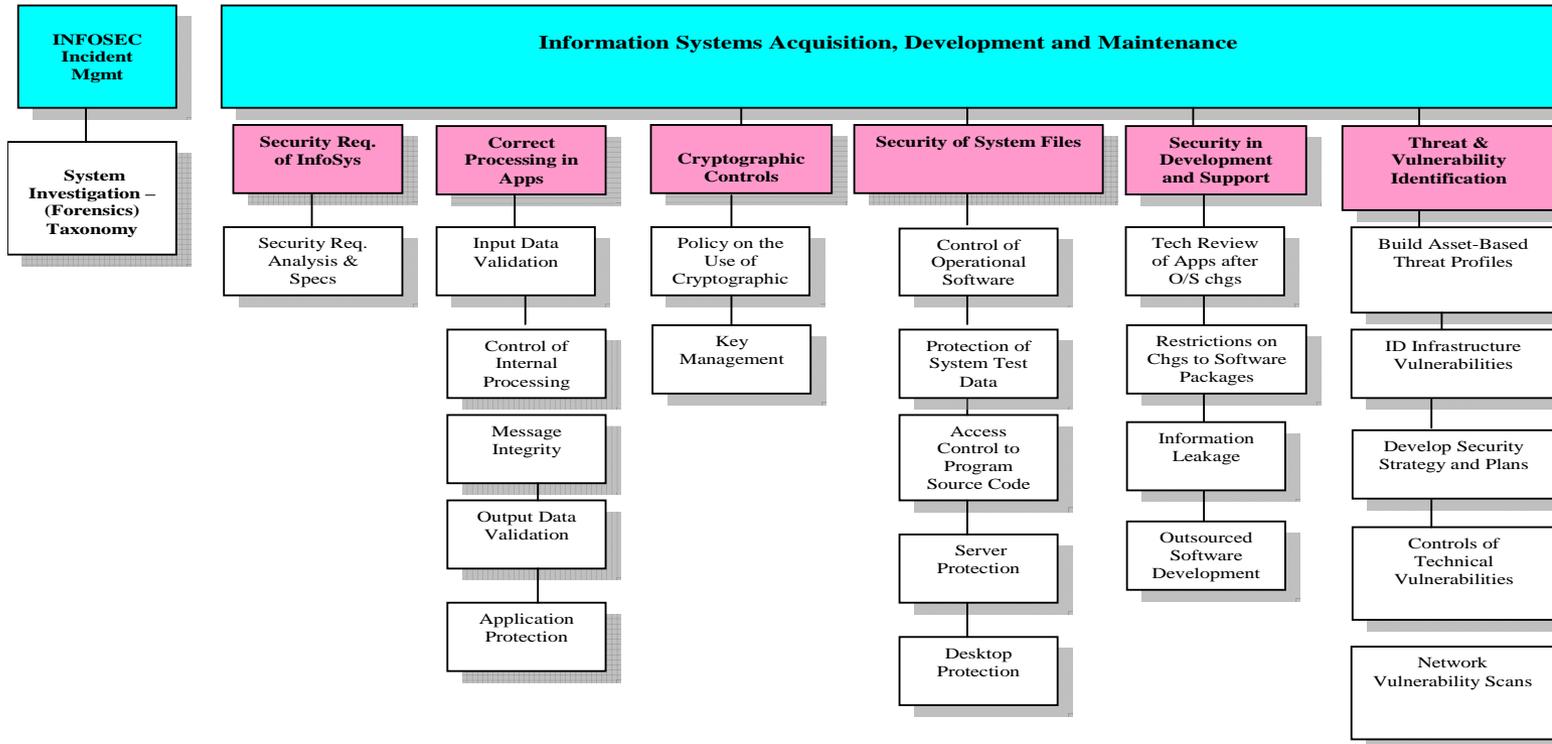
**Security Assessments  
Micro Taxonomy (An Operational View)  
Taxonomy (1 of 4)**



Security Assessments Taxonomy (1 of 4)

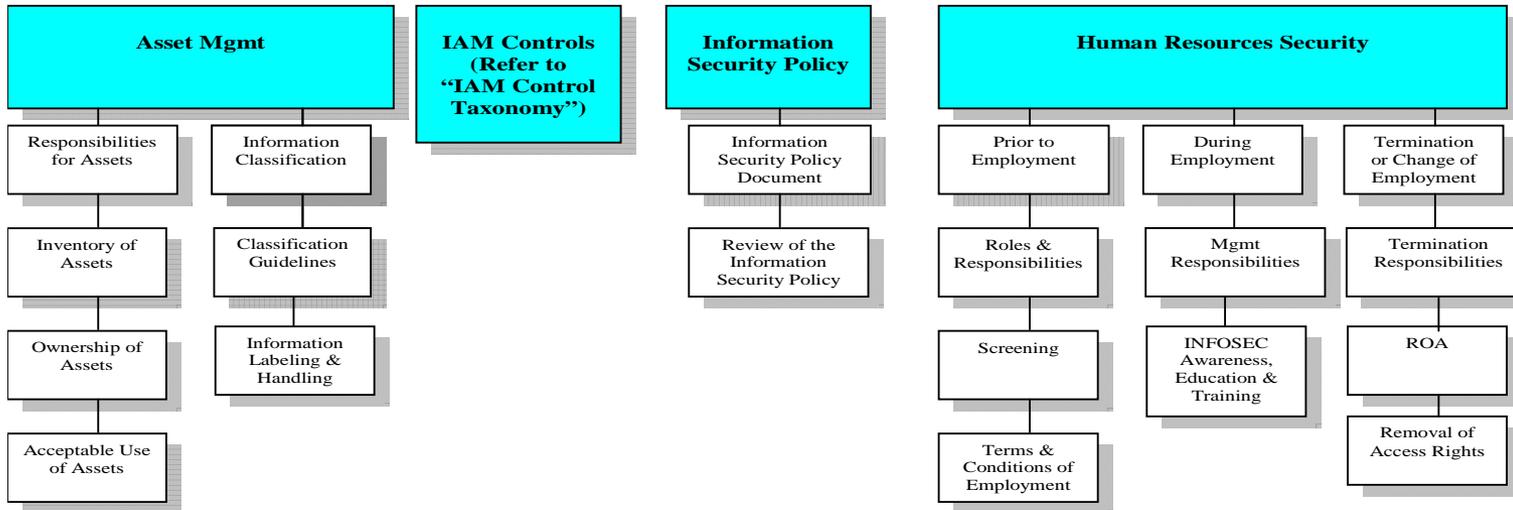
# A Micro Taxonomy of Security Assessments

**Security Assessments  
Micro Taxonomy (An Operational View)  
(2 of 4)**



# A Micro Taxonomy of Security Assessments

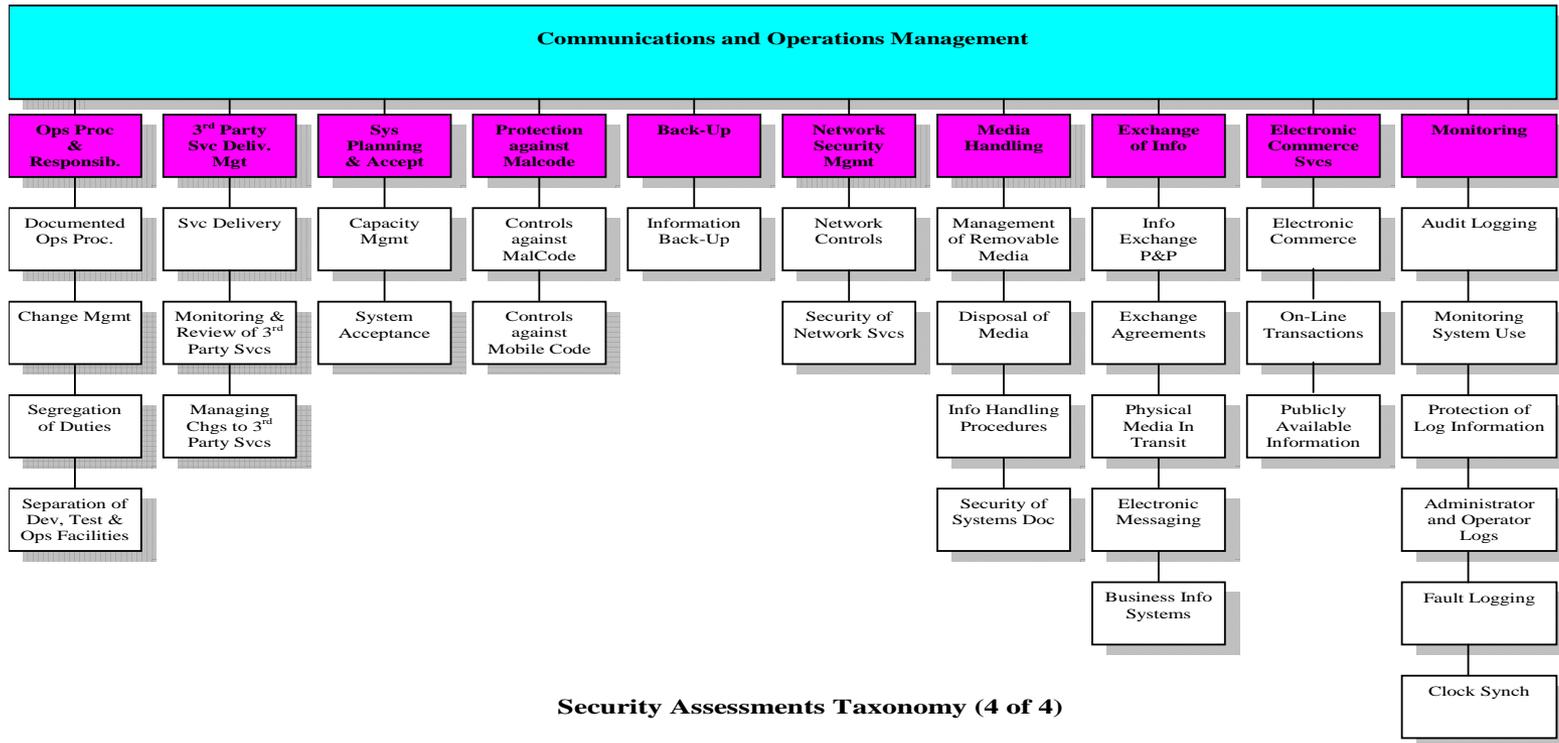
**Security Assessments  
Micro Taxonomy (An Operational View)  
(3 of 4)**



**Security Assessments Taxonomy (3 of 4)**

# A Micro Taxonomy of Security Assessments

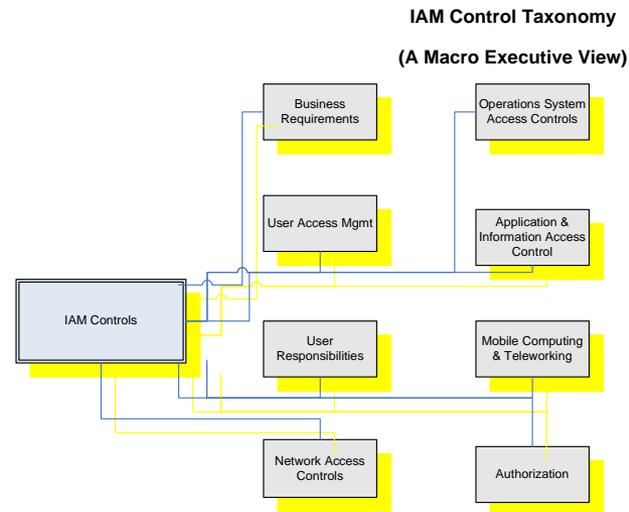
**Security Assessments  
Micro Taxonomy (An Operational View)  
(4 of 4)**



# A Macro Taxonomy of IAM

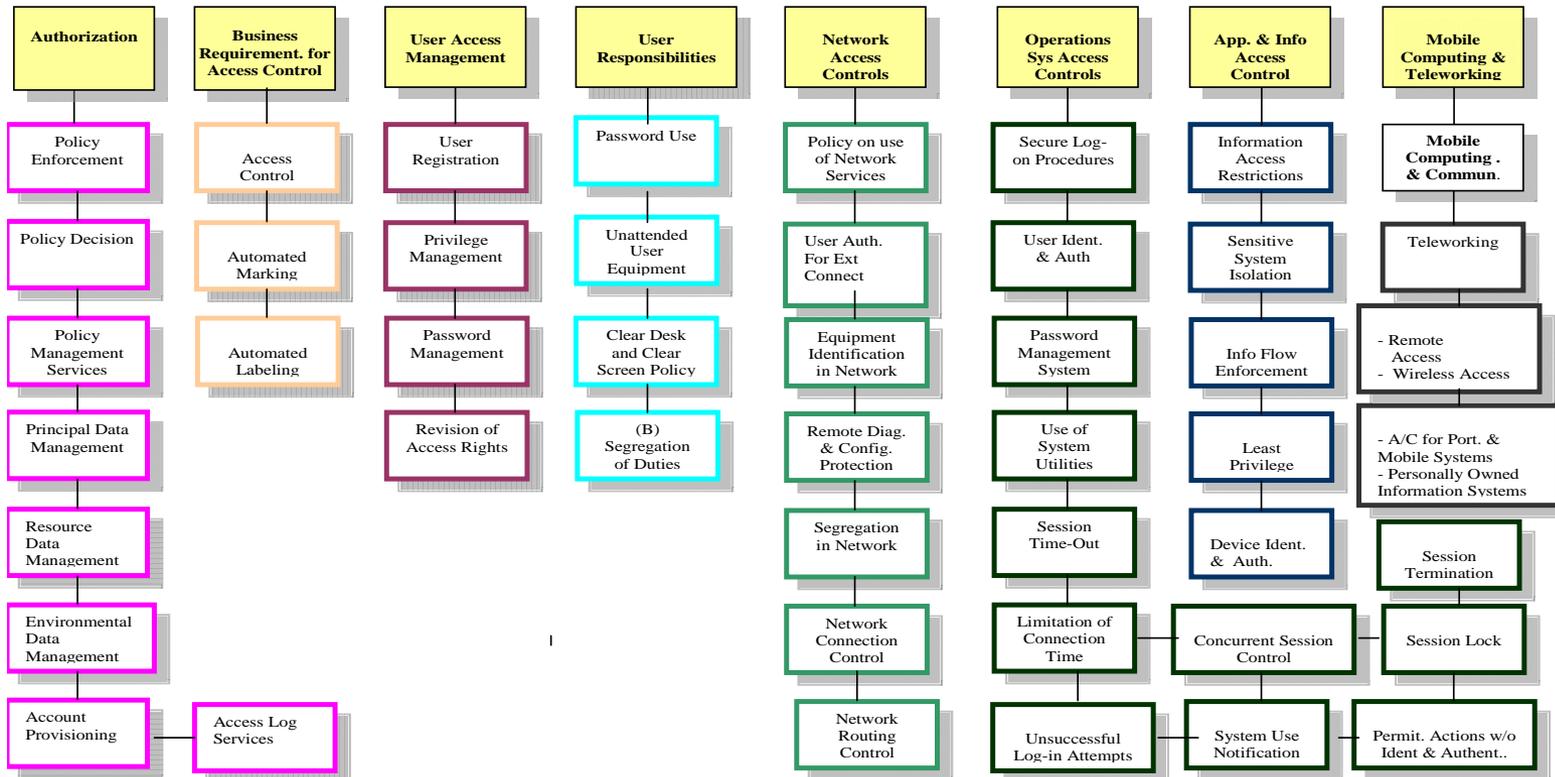
Key *Identity and Access Management (IAM)* Risks include, but are not limited to the absence of effective controls over the following components:

- User Management, Administration, and Maintenance systems
- User Provisioning and De-provisioning
- User Self Service and Self Registration
- Approval Workflows
- Web Access Management
- Enterprise Single Sign-On
- Identity Federation and Partner Access
- Role Based Access Control (RBAC) systems
- Credentialing Systems
- Digital Signing
- Encryption Systems
- Records Security and Data Privacy
- Audit and Reporting



# A Micro Taxonomy for IAM

**IAM  
Micro Taxonomy (An Operational View)**



# Cyber Governance – (Typical INFOSEC Scorecard)



<p>Security Policies, Standards and Procedures</p>	<ul style="list-style-type: none"> <li>• Organizations are faced with the challenge of developing integrated security policies, standards and procedures. Mapping documented guidance to compliance, audit and corporate level guidance is a significant challenge</li> </ul>
<p>Systems Development and Security Architecture</p>	<ul style="list-style-type: none"> <li>• While the software development industry is making efforts to secure the design and implementation of the software development and engineering processes, their still is no defacto standard for industry sound and best practices, however, this area is improving</li> </ul>
<p>Information Security Monitoring &amp; Data Sourcing</p>	<ul style="list-style-type: none"> <li>• The security event and information monitoring (SEIM) process is starting to mature, however, there is still a significant amount of work which remains in this area in terms of determining root cause analysis for breaches (external and internal) and the creation of actionable items for corrective action</li> </ul>
<p>Production Application Systems Security</p>	<ul style="list-style-type: none"> <li>• The primary emphasis has historically been on pre-implementation reviews vs production applications. Recently, there has been an increased regulatory oversight on assessing the processes and controls governing production applications and systems (i.e. SOX 404, introduction of new code and vulnerabilities to applications due to version changes and patch management)</li> </ul>
<p>Network Security</p>	<ul style="list-style-type: none"> <li>• CyberSecurity awareness within many organizations has generally improved over the past few years, however, information security architecture and design needs enhancements are needed to more effectively implement the Defense in Depth Model of layered security protection</li> </ul>
<p>User Authentication and Access Controls</p>	<ul style="list-style-type: none"> <li>• Many organizations are still placing too much reliance on the network controls vs the use of combined network and native application and systems controls for controlling user access</li> </ul>

# Cyber Governance – (Typical INFOSEC Scorecard)

<b>Vendor Management for Security</b>	<ul style="list-style-type: none"><li>• Challenges facing organizations in Vendor Management is maintaining transparency and on-going communication of key information between the software vendor and service provider</li></ul>
<b>Incident Response (Including Digital Forensics)</b>	<ul style="list-style-type: none"><li>• CyberSecurity Awareness and Preparedness has improved for many organizations in both the public and private sector, however, testing of the Incident Response Preparedness plan, which covers digital forensics and other areas are not being regulatory performed or performed at all.</li></ul>

***The Cyber Threat Modeling Needs to Factor many components: The results of the Security Risk Assessment, Vulnerabilities Identification, the Threat Landscape, Regulatory, Legal Compliance considerations and Industry Sound and Best Practices***

*There is a movement over the past few years for organizations to evolve from a Network to a Data Centric Model or “De-Perimeterization” for Cyber Risk Reduction and strengthening layered defenses for data privacy*

*De-Perimeterization (Data Centric Model) and “Control Point” identification*

*De-Perimeterization (Data Centric Model) and the Security Architecture*

De-Perimeterization (Data Centric Modeling)  
(A Nexus to Perimeter Security, Regulatory Compliance & Security Architecture)

The Nexus between the concept of De-Perimeterization, Regulatory Compliance & Security Architecture, lies within the identification and mapping of key data flows and "*Control Points*" within the enterprise and beyond

- *Perimeter Security*
- *Data flow*
- *Regulatory Compliance*
- *Security Architecture*

# The Traditional Network Centric Defense in Depth Layered Security Architecture Perimeter Protection

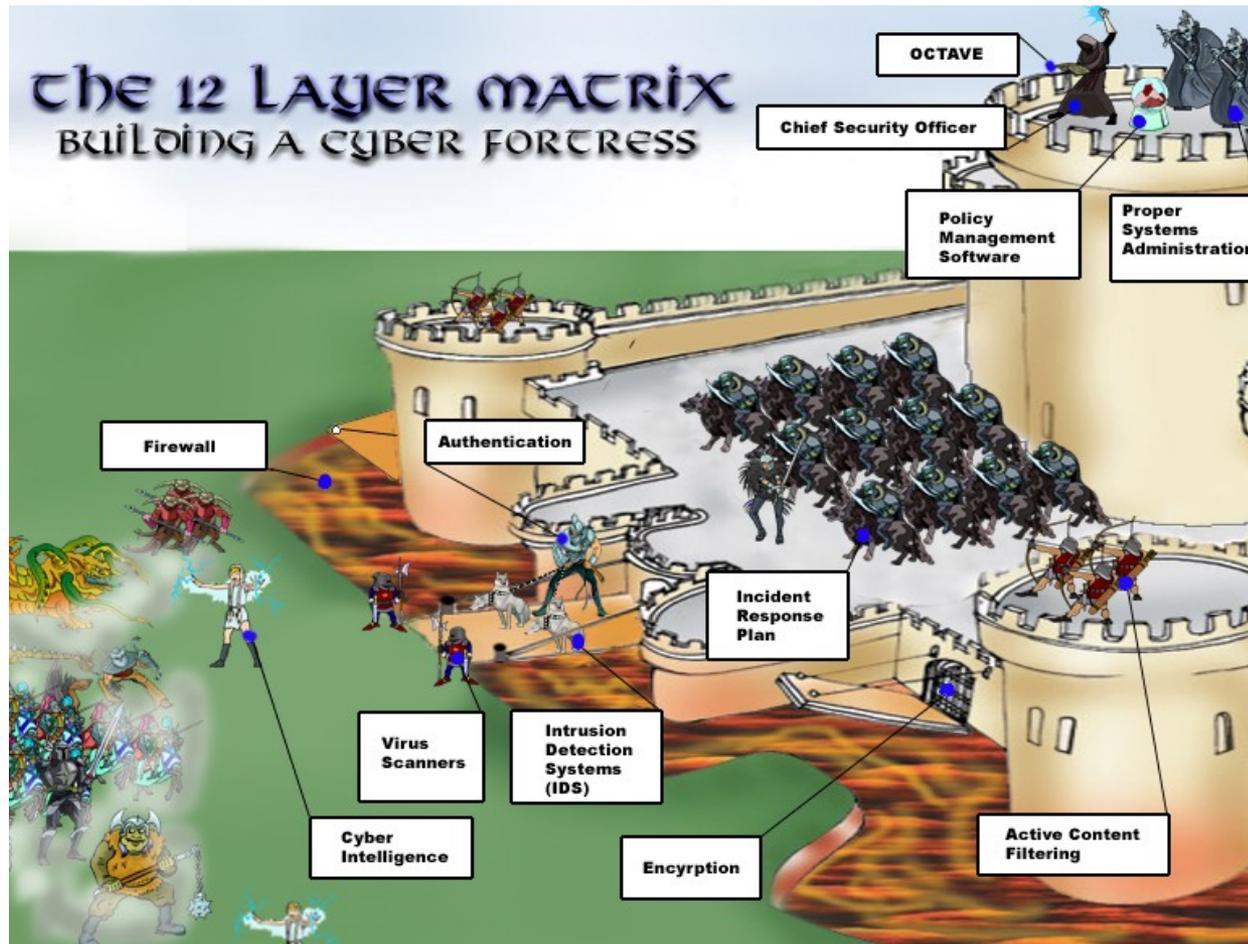


Diagram Courtesy of Tom Kellermann, VP Core Technologies

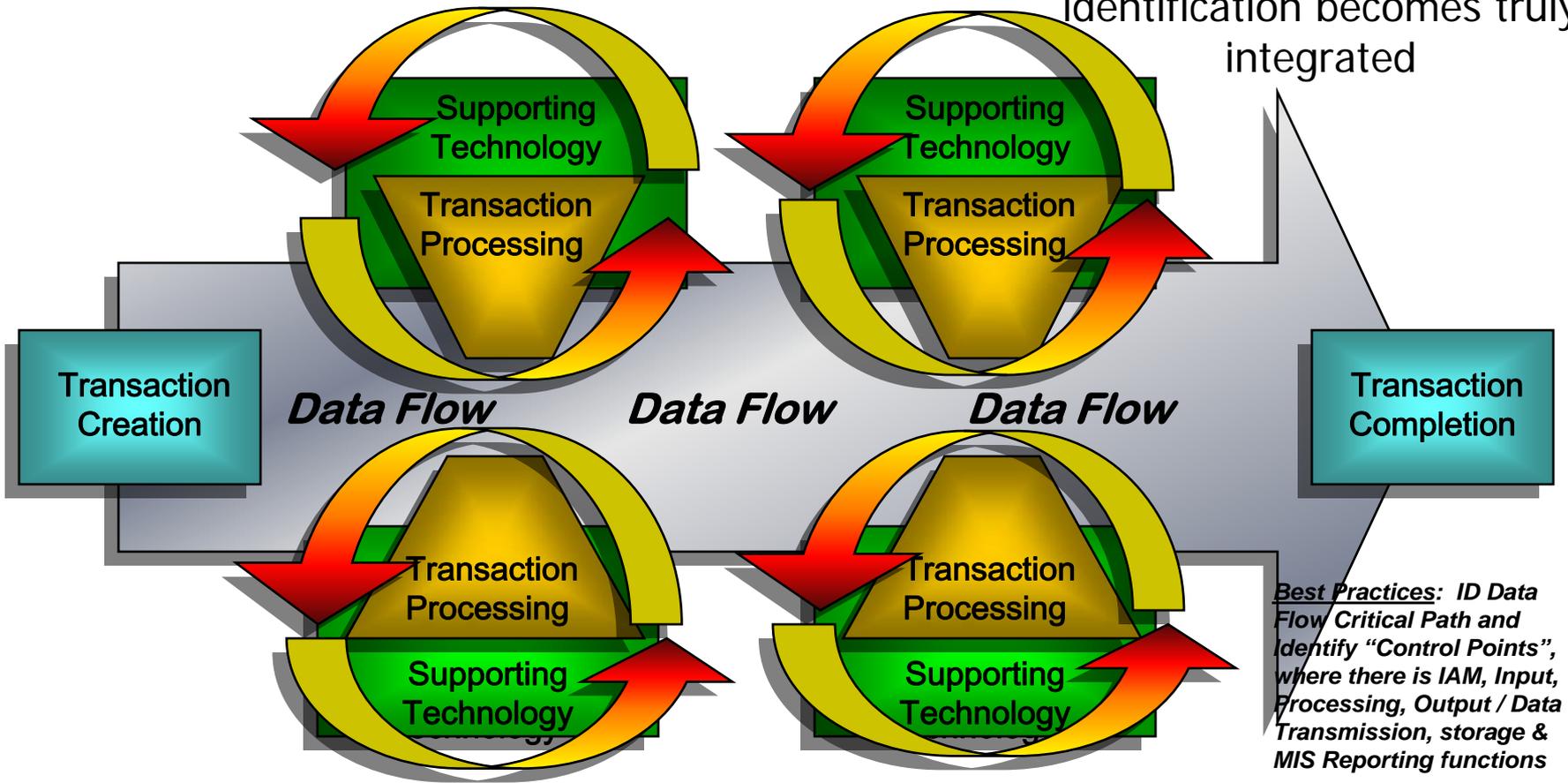
# The Progressive De-Perimeterization (Data Centric Modeling) Security Architecture Approach

## (Data Flow Mapping)

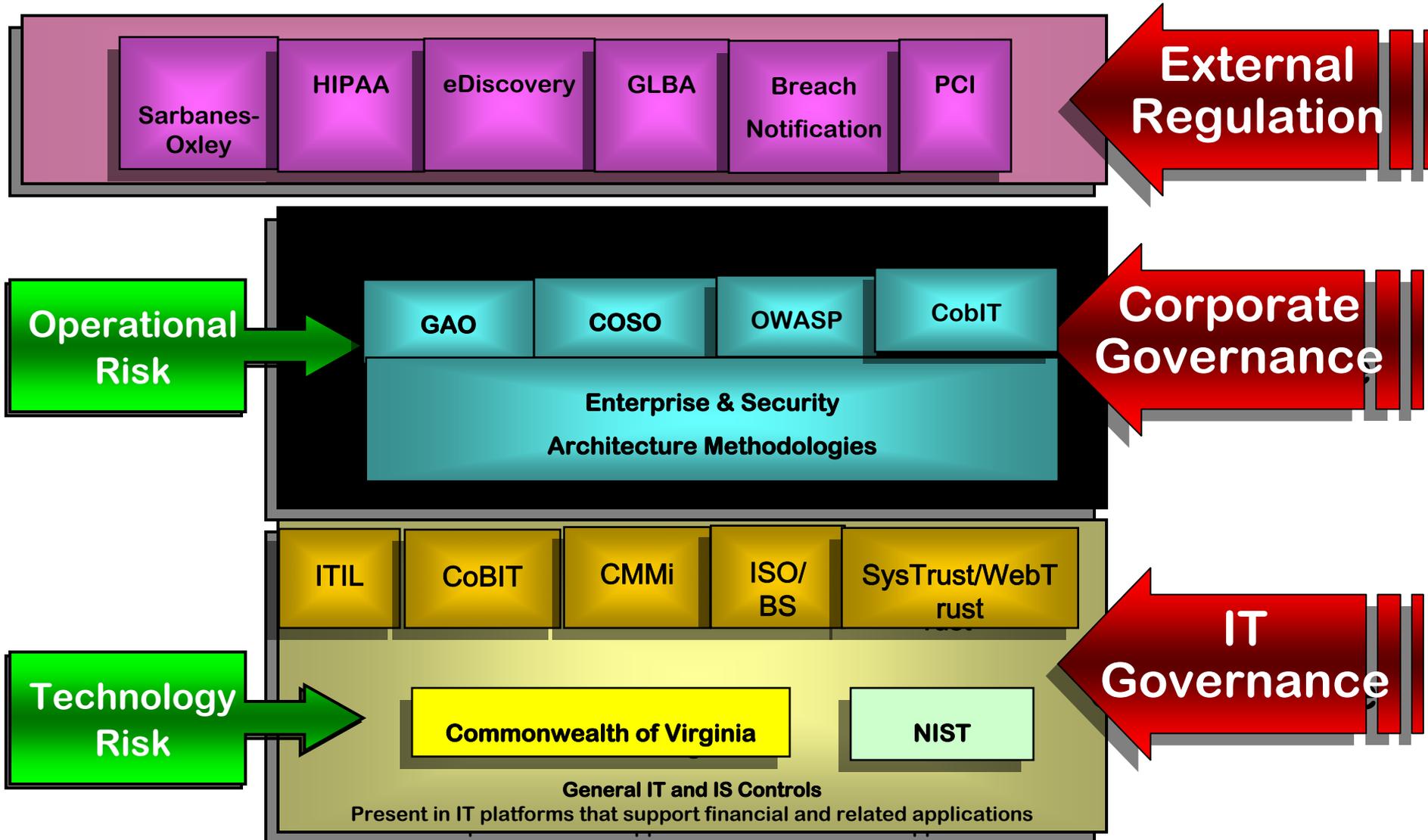
Business Process (Data)  
"flows horizontally"

Supporting Technology  
"flows vertically"

Where Data intersects  
technology, this is where  
operational risk  
identification becomes truly  
integrated



# De-Perimetretization (Data Centric Modeling) & Domestic Regulatory Compliance



## Vulnerabilities

- Backdoors and holes in the network perimeter
- Vulnerabilities in Common Protocols
- Attacks on Field Devices
- Database Attacks
- Man in the Middle Attacks
- Poorly Configured Firewalls
- Trusted Peer Utility Links

And many more!

# Cyber Threat Actors

Script Kiddie

Recreational Hacker

Cyber Activist

Organized Crime

Terrorist Organization

Nation-State

Insider Threat

**EXTERNAL Threats:** (The external attack vectors are the most commonly documented attacks of the three categories. The conventional attack pattern vectors have been memorialized primarily within MITRE's Common Attack Pattern Enumeration and Classification (CAPEC) repository and other data sources)

- Bot-network operators
- Criminal groups
- Foreign intelligence services
- Hackers
- Phishers
- Spammers
- Spyware/Malware
- Terrorists

**INTERNAL Threats:** (The Insider Threat component is one of the more elusive and insidious components of the Threat Landscape and represents a National Security concern given its implications on all sectors of the critical infrastructure. There is minimal data available in the public domain that provides credible data on this significant threat component. Consequently, the threat modeling process has long overlooked this significant component of the equation and has left many organizations unnecessarily exposed to this threat)

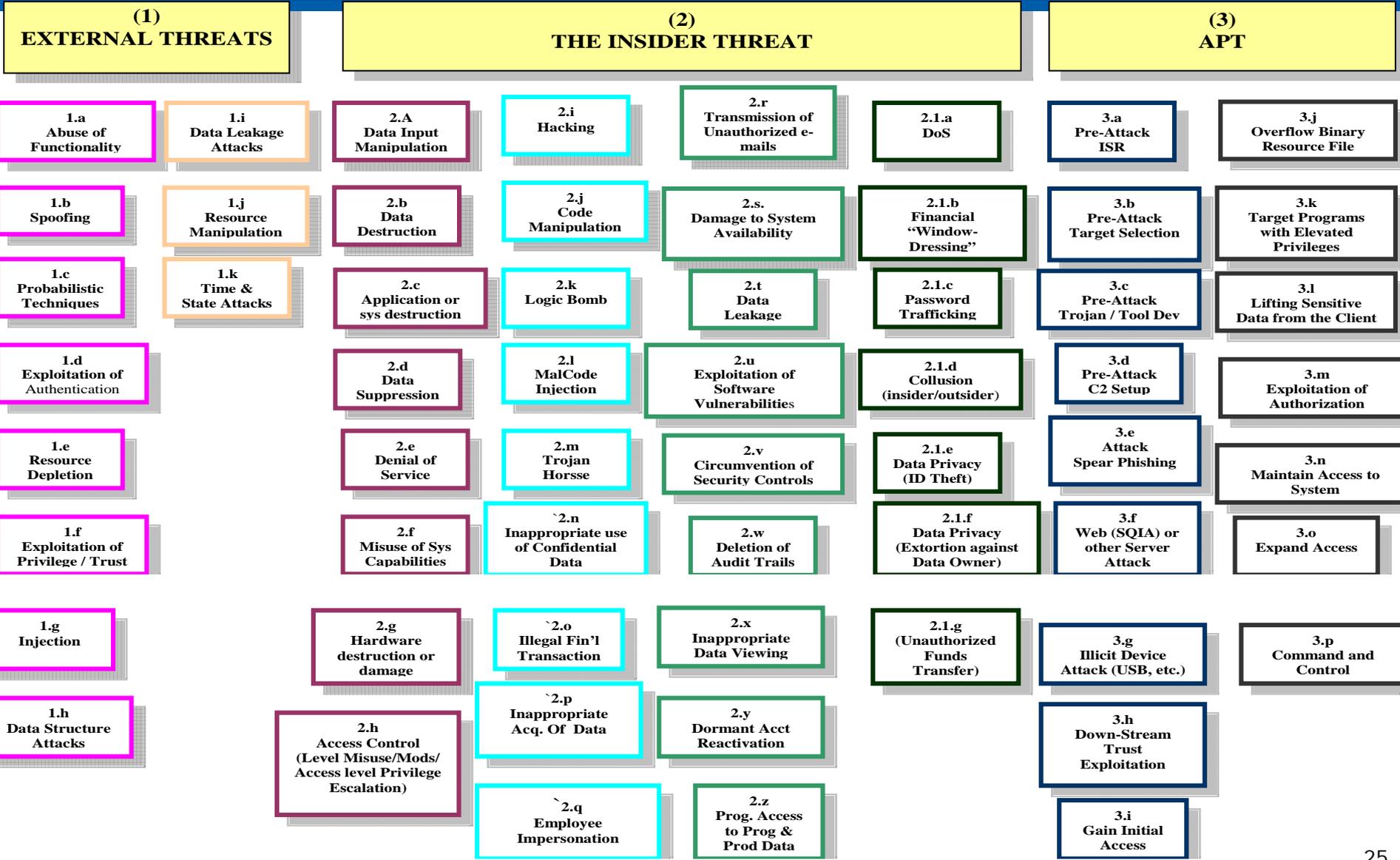
- Unauthorized System Access
- Inappropriate Use of Confidential Corporate Data stored in one computer
- Computer Data Manipulation
- Ease of Access into a Computer System
- Software Code Manipulation
- Misuse of System's Capabilities
- Inadequate Network Journaling for Forensic Purposes
- Illegal data transactions
- Loss of IPR

**APT: The APT is the most elusive of all the threat vectors and involves the combination of conventional network attacks used in combination with many other components (i.e. People, Processes and Technology) to create a complex modus operandi and APT attack scenarios**

**Common Conventional Network Attacks (Mitre's CAPEC) that can serve as the tip of the spear for more sophisticated attacks, involving people, processes and technology includes, but not limited to the following attacks:**

- **Blind SQL Injection - (7)**
- **SQL Injection (66)**
- **Client-side Injection-induced Buffer Overflow (14)**
- **Overflow Binary Resource File (44)**
- **Target Programs with Elevated Privileges (69)**
- **Lifting Sensitive Data from the Client (94) (category not pattern)**
- **Exploitation of Authorization (103) (category not pattern)**

# A Cyber Macro Taxonomy Of the Threat Landscape



The prevention and responding to improper disclosures of personal information is becoming a systemic concern both within both the public sector and throughout each segment of the Critical Infrastructure

In the public sector, the Government Accountability Office (GAO) testified to the Committee on Government Reform, House of Representatives on the issue of data privacy in the federal government.

- The GAO's June 8, 2006 publication on this testimony concluded that federal agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised.

The two key steps include:

- Develop a privacy impact assessment (PIA) (An analysis of how personal information is collected, stored, shared, and managed – whenever information technology is used to process personal information)
- Ensure that a robust information security program is in place, as required by the Federal Information Security Management Act of 2002 (FISMA)

## **GAO recommends that controls over privacy and security of personal information could be strengthened by:**

- Limiting the Collection of personal information (limits the opportunity for that information to be compromised)
- Limiting Data Retention (Retaining personal data longer than needed by regulation adds to the risk that the data will be compromised)
- Limit access to personal information and train personnel accordingly (Only individuals with a need to access databases of personal information should have such access, and controls should be in place to monitor that access)
- Consider using technological controls such as encryption when data needs to be stored on mobile devices (i.e. laptop computers)

## **International – Cross Border Risks**

- Safe Harbor – US and EU for data privacy protection
- APEC - US and members of the Asia Pacific region for data privacy protection

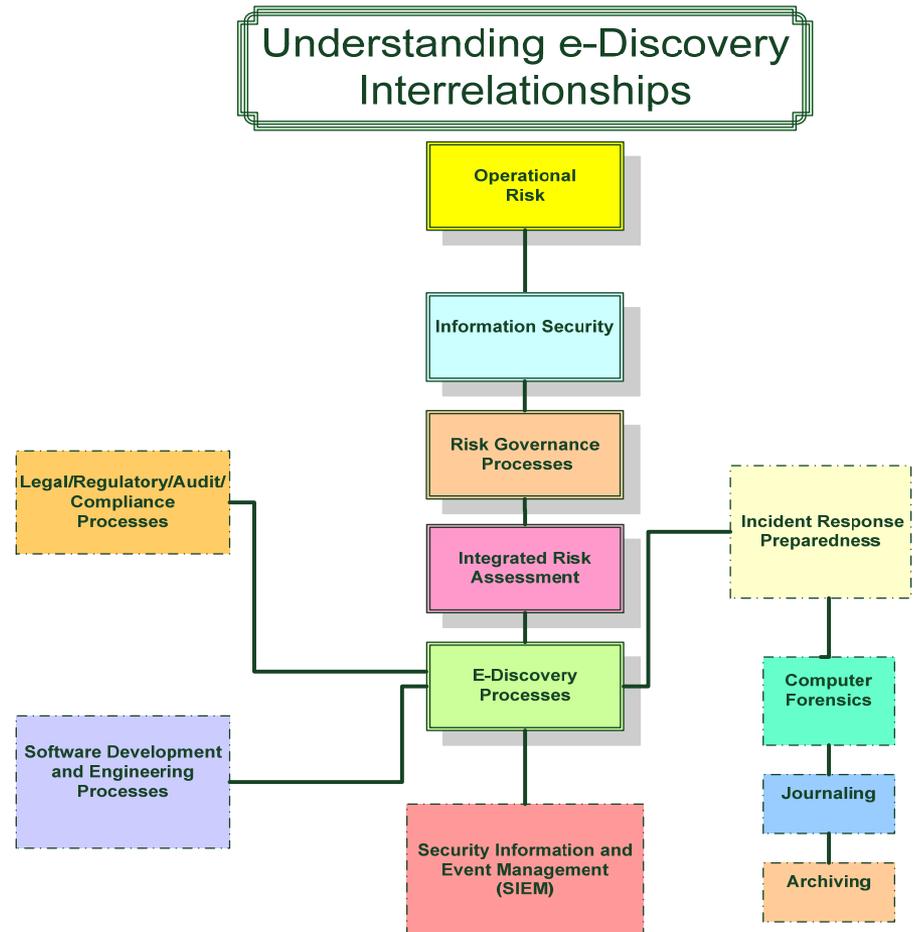
## Interest in Data Breach Notification Legislation Has Increased

- Federal laws to date have not required agencies to report security breaches to the public, although breach notification has played an important role in the context of security breaches in the private sector.
- Several bills have been introduced to Congress and the Senate such as the Data Accountability and Trust Act (DATA), which would establish a national requirement for companies that maintain personal information to notify the public of security breaches.

## Understanding E-Discovery Interrelationships

Putting all the pieces together

- The Parent process that drives E-Discovery is Operational Risk
  - The children of the parent process includes not only E-Discovery but all the other components of this process, such as:
    - Information Security
    - Risk Governance
    - Integrated Risk Assessment
    - Legal/Regulatory/Audit
    - Software Development and Engineering Processes
    - SIEM
    - Incident Response Preparedness
    - Computer Forensics
    - Journaling
    - Archiving



*eDiscovery* and *operational risks* can be reduced through an integrated risk assessment, threat analysis and privacy impact assessments which identify, measure, monitor and control the collection and storage of Electronically Stored Information (*ESI*)

*eDiscovery* and *operational risks* can be reduced through the implementation and testing of information security procedures which outline risk governance processes over Legal, Regulatory and Audit Processes, Software Development and Engineering, Security Information and Event Management (SIEM), Digital Forensics, Journaling and Archiving

---

Industry Sound and Best Practices: (ISO 27001 - 27005, NIST, ITIL, COBIT, SABSA, COV Security Requirements, DSS PCI, HIPPA, etc.)

Enterprise Risk Assessment (ERA) – (Cyber Vulnerabilities + Threats)

Threat Modeling

Compliance

Residual Risk Identification (Inherent Risk – Mitigating Controls) and Risk Acceptance

Economics (Costs and Performance Based Measurements to Identify incremental Security Improvements)

# Security Control Selection

(Based on the iGRC Processes)

## **Integrated Risk Assessment (IRA)**

- Classify and Rank Sensitive Data, Systems, and Applications
- Assess Threats and Vulnerabilities
- Assign Risk Ratings
- Develop an INFOSEC Risk Strategy:
  - Enterprise (EA) and Security Architecture (SA) Considerations
    - » Policies and Procedures
    - » Technology Design
    - » Outsourced Security Services
  - Develop a strategy that defines control objectives and establishes an implementation plan. The security strategy should include:
    - Appropriate consideration of prevention, detection, and response mechanisms
    - Implementation of the least permissions and least privileges concepts
- Security Controls Implementation:
  - Identify Cyber Base Practices for each component of Cyber Security & Integrate

# Cyber Controls Taxonomy

- ERM – (Enterprise Risk Management)**
- Systems Development & Acquisition**
- User Authentication & Access Controls**
- Security Assessments**
- Unified Threat Management**
- Management of Encryption Key & Digital Certificates**
- Event Correlation**
- System Patch Management**
- Supply Chain Vulnerabilities**
- Secure Mobile Computing**
- Information Security Monitoring**
- Security Outsourcing**
- Security Architecture**
- Network Security & IAM**
- Production Application Security**
- Information Classification**
- IDS & IPS**
- Incident Response & Preparedness**
- Digital Forensics**
- Diagnostic Testing**
- Information Asset Protection**
- Characterization of System & Data Flows**

## The 2009 CIS Security Metrics

- Incident Management
- Vulnerability Management
- Patch Management
- Application Security
- Configuration Management
- Financial Metrics
- Other

The User Requirements and Design of the Enterprise Security Architecture should be a tight integration of the entire Cyber Governance Process

Layered Defenses within the IT infrastructure should be a by-product of an Enterprise-Wide Cyber Governance Process

**IMPORTANT: The Cyber Risk Governance Process is on-going and iterative and so baking these processes into daily operational activities is the right RX for maintaining Good Cyber Hygiene!**

# THANK YOU!



## QUESTIONS?

Dr. Kenneth C. Brancik, CISM, CISSP, CISA, ITIL

Northrop Grumman Corporation

The Advanced Technology Group (ATG)

7575 Colshire Drive,

McLean, VA

(703) 883-8333 (Office)

[Kenneth.Brancik@ngc.com](mailto:Kenneth.Brancik@ngc.com)

***NORTHROP GRUMMAN***





# Virginia.gov DNSSEC



- **Objective**

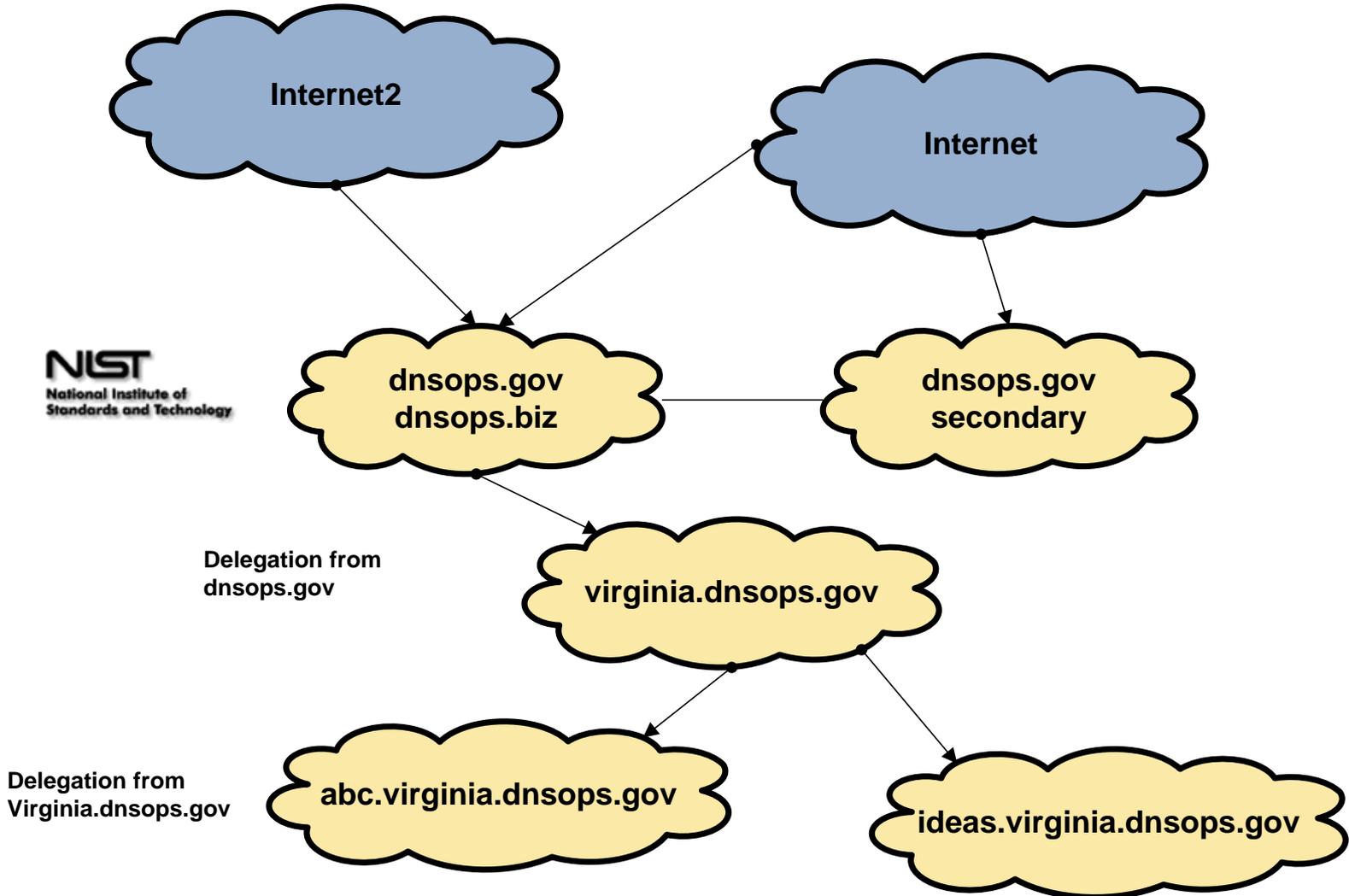
- Provide update on DNSSEC effort and specifically the pilot environment
- Request your participation in ensuring success

- **Agenda**

- Review DNSSEC requirements
- Explain DNSSEC testing and the SNIP
- Outline high level plan and milestones
- Discuss actions and next steps

- **On August 22, 2008, the Office of Management and Budget (OMB) released a memorandum requiring U.S. Federal Agencies to deploy DNSSEC across .gov sites**
  - The .gov root was signed in January 2009
  - All subdomains under .gov must be signed by December 2009.
- **DNS Security Extensions**
  - **Provides Authentication and Integrity**
    - Authentication of the origin
    - Helps to prevent spoofing
    - DNS Data integrity
  - **Uses public keys and signatures**
- **The IT Partnership has launched a project to ensure all Commonwealth sub-domains (virginia.gov) are signed by December 2009, and the test environment will soon be available**

- **The Secure Naming Infrastructure Pilot (SNIP) is a joint project involving NIST, SPARTA Inc, and the Dept. of Homeland Security.**
- **The main goal is to provide a test domain for participants to use and become familiar with the DNS Security Extensions (DNSSEC) and how they will affect current DNS operations.**
- **DNS operators will use a basic SNIP delegation from the SNIP domain (dnsops.gov) and attempt to mirror their current operational procedures.**



- **Virginia.dnsops.gov assigned and signed**
  - CTNGH03.Virginia.dnsops.gov

## Sub-Domain Participation

- *Pilot (Test environment) is optional but strongly recommended*
- *Production required*

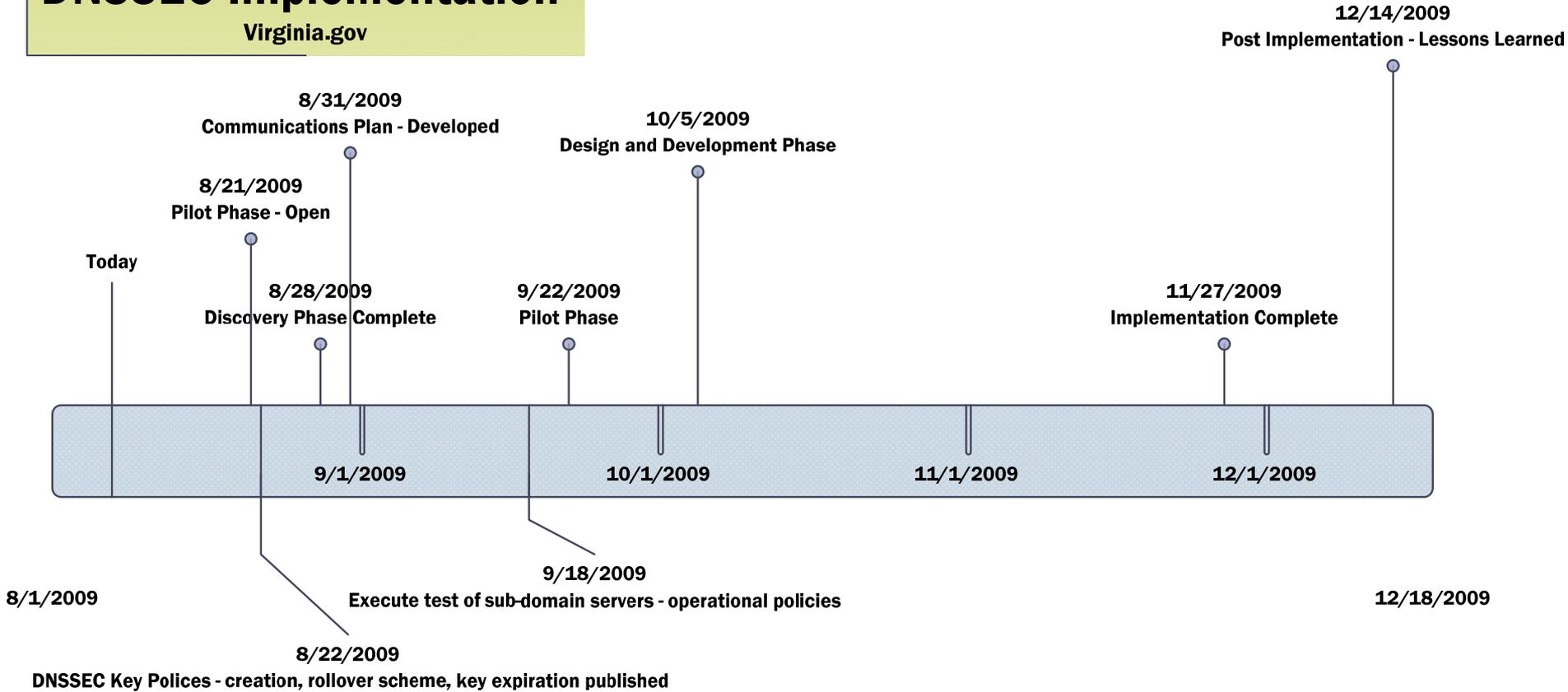
## Requirements

- **BIND 9.3.2 +**
- **Name Server Daemon (NSD) maintained by NLNet Labs**
- **Several Commercial Products and appliances**
  - **Must support - RFC4033, RFC4034, and RFC4035**
- **Full Support for DNSSEC will be introduced in Windows Server 2008 R2 and Windows 7.**
  - *Server 2003 has partial support of DNSSEC*
- **Registration of sub-domains is being done manually**
  - **Contact: [dnssec@vita.virginia.gov](mailto:dnssec@vita.virginia.gov)**

- **Discovery**
  - Parallel task with SNIP task
  - Communications will be published requesting information about the current DNS
- **Design and Development**
  - DNSSEC Key Policies - creation, rollover scheme, key expiration
  - Design and document operational processes and procedures
- **SNIP (Testing)**
  - Provides playground for testing your DNSSEC operations
- **Implementation**
  - Execute and monitor implementation process
  - Monitor and support

## DNSSEC Implementation

Virginia.gov



### Proposed Timeline

- **In-scope Agencies**

- Preferred option is to migrate existing DNS to CESC Enterprise DNS
- Partnership is responsible for completing implementation
- Project team will engage SD and Tower leads

- **Out-of-Scope Agencies**

- Encouraged to participate in pilot environment
- Required to participate in production environment

# In Scope Agencies



Subdomain	Authoritative Name Server	Inscope	Agency	Notes
dpor.virginia.gov	fw.dpor.virginia.gov.	Yes	DPOR	
oig.virginia.gov	dns.dmhmrzas.virginia.gov.	Yes	OIG	
abc.virginia.gov	dns.abc.virginia.gov.	Yes	ABC	
abc.virginia.gov	dns.abc.state.va.us.	Yes	ABC	
abc.virginia.gov	dns2.abc.virginia.gov.	Yes	ABC	
abc.virginia.gov	dns2.abc.state.va.us.	Yes	ABC	
dss.virginia.gov	bastille.dss.state.va.us.	Yes	DSS	
dss.virginia.gov	dssgate.dss.state.va.us.	Yes	DSS	
workcomp.virginia.gov	dns1.workcomp.virginia.gov.	Yes	CB	Virginia Workers' Compensation Commission
workcomp.virginia.gov	dns2.workcomp.virginia.gov.	Yes	CB	Virginia Workers' Compensation Commission
cicf.virginia.gov	dns1.cicf.virginia.gov.	Yes	CB	Criminal Injuries Compensation Fund
cicf.virginia.gov	dns2.cicf.virginia.gov.	Yes	CB	Criminal Injuries Compensation Fund
vsp.virginia.gov	ns1.vsp.virginia.gov.	Yes	VSP	
vsp.virginia.gov	ns2.vsp.virginia.gov.	Yes	VSP	
dmhmrsas.virginia.gov	dns.dmhmrzas.virginia.gov.	Yes	DMHMRSAS	
dmhmrsas.virginia.gov	dgsfirewall.dgs.virginia.gov.	Yes	DMHMRSAS	
vdh.virginia.gov	dns-ext-1.vdh.virginia.gov.	Yes	VDH	
vdh.virginia.gov	dns-ext-2.vdh.virginia.gov.	Yes	VDH	
vdh.virginia.gov	dns-ext-2.vdh.virginia.gov.	Yes	VDH	
schev.virginia.gov	dnrc1.principle.schev.edu.	Yes	SCHEV	
schev.virginia.gov	dnrc2.principle.schev.edu.	Yes	SCHEV	
dhrm.virginia.gov	ns1.dhrm.virginia.gov.	Yes	DHRM	
dhrm.virginia.gov	ns2.dhrm.virginia.gov.	Yes	DHRM	
cvc.virginia.gov	ns1.dhrm.virginia.gov.	Yes	DHRM	
cvc.virginia.gov	ns2.dhrm.virginia.gov.	Yes	DHRM	
www.drpt.virginia.gov	ns.cybersharks.net.	Yes	DRPT	
www.drpt.virginia.gov	ns2.cybersharks.net.	Yes	DRPT	
ftp.drpt.virginia.gov	ns.cybersharks.net.	Yes	DRPT	
ftp.drpt.virginia.gov	ns2.cybersharks.net.	Yes	DRPT	
olga.drpt.virginia.gov	ns.cybersharks.net.	Yes	DRPT	
olga.drpt.virginia.gov	ns2.cybersharks.net.	Yes	DRPT	

- Discovery Phase

Subdomain	Authoritative Name Server	Inscope	Agency	Notes
agencies.virginia.gov	ns1.agencies.virginia.gov.	TBD		Under Construction
agencies.virginia.gov	ns2.agencies.virginia.gov.	TBD		Under Construction
vcapride.virginia.gov	ns1.easy-cgi.com.	TBD		Valley Commuter Assistance Program (VCAP) related to NSVRC
vcapride.virginia.gov	ns2.easy-cgi.com.	TBD		Valley Commuter Assistance Program (VCAP) related to NSVRC
nsvrc.virginia.gov	ns1.easy-cgi.com.	TBD		Northern Shenandoah Valley Regional Commission (NSVRC) related to VCAP Virginia Association of Planning District Commissions
nsvrc.virginia.gov	ns2.easy-cgi.com.	TBD		Northern Shenandoah Valley Regional Commission (NSVRC) related to VCAP Virginia Association of Planning District Commissions
espl.virginia.gov	ns.intercom.net.	TBD		Eastern Shore Public Library
espl.virginia.gov	ns2.intercom.net.	TBD		Eastern Shore Public Library

# Out of Scope Agencies



Subdomain	Authoritative Name Server	Inscope	Agency	Notes
ideas.virginia.gov	dns1.midphase.com.	No	VEAP	
ideas.virginia.gov	dns2.midphase.com.	No	VEAP	
cgep.virginia.gov	uvaarpa.virginia.edu.	No		Commonwealth Graduate Engineering Program
cgep.virginia.gov	nom.virginia.edu.	No		Commonwealth Graduate Engineering Program
vi.virginia.gov	ns.vipnet.org.	No		Virginia Interactive
vi.virginia.gov	burr.ai.org.	No		Virginia Interactive
business.virginia.gov	ns.vipnet.org.	no		Virginia Interactive
business.virginia.gov	burr.ai.org.	no		Virginia Interactive

- <http://www.dnssec.net/>
- <http://www.dnsops.gov/>
- <http://www-x.antd.nist.gov/dnssec/>
- **NIST SP 800 81 - Secure Domain Name System (DNS) Deployment Guide**

# Questions





# Partnership Security Update

Don Kendrick

*Senior Manager of Security Operations*





# 2009 COV Security Policy & Standard Update

**John Green**

Deputy Chief Information Security Officer



# Policy, Standard & Guidelines Update



1. Collect comments & questions from the IS community during the year
2. Create draft of policy, standard or guideline (PSG) addressing comments...
3. Distribute draft to IS Council for review, input & feedback
4. Collect comments from IS Council, usually giving them a week or so to review
5. Review & address Council comments in the PSG
6. Send draft of PSG to ITIES Directorate for review & comment
7. Aggregate comments from ITIES, usually takes a week or so
8. Comments from ITIES are reviewed with CSRM management & addressed as appropriate
9. Draft of PSG is sent to ITIES for posting to Online Review Comment Application (ORCA)...
10. Gather comments from IS community (ORCA) for at least 30 days
11. Review & address ORCA comments
12. Create responses to comments from ORCA reviewers & distribute through ITIES
13. Send finalized version of PSG to ITIES who sends it to the CIO for approval.
14. If the CIO approves it goes to the ITIB for consideration & approval. If a standard or guideline there is a 5 day comment period & if a policy it must be approved at an ITIB meeting
15. Once approved it is posted to the web

Policy and Standard 

 = STATUS THIS MONTH

 = STATUS LAST MONTH



# Commonwealth Information Security Council

**Peggy Ward**  
Chief Information Security Officer



2009  
Commonwealth Security Annual Report

**Peggy Ward**  
Chief Information Security Officer





## § 2.2-2009

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

- C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.



# Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

**Acronyms:**

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

**ISO Designated: The Agency Head has**

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

**Attended IS Orientation:**

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



# Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

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

**Yes** - submitted a Security Audit Plan for the period of fiscal year 2009 - 2011 for systems classified as sensitive based on confidentiality, integrity or availability

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

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

**Expired** –submitted a Security Audit Plan on file that does not contain the current three year period FY 2009 – FY 2011

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

**Corrective Action Plans Received: The Agency Head or designee has**

**Yes** - submitted an adequate Corrective Action Plan or notification of no findings for Security Audits scheduled to have been completed

**Some** - submitted an adequate Corrective Action Plan or notification of no findings for some, but NOT all Security Audits scheduled to have been completed

**No** - NOT submitted any adequate Corrective Action Plans or notification of no findings for Security Audits scheduled to have been completed

**Not Due** - not had Security Audits scheduled to be completed

**N/A** - not submitted a Security Audit Plan so not applicable

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



# Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates
Agency XYZ	Yes	10	Yes	Yes	Yes

**Quarterly Updates: The Agency Head or designee has**

**Yes** - submitted adequate quarterly status updates for all corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**Some** - submitted adequate quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**No** - not submitted ANY quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**Not Due** - no open Security Audit findings

**N/A** - not submitted a Security Audit Plan or a Corrective Action Plan that was due

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



## FAQ!

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

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



# Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Human Rights Council	Yes	0	No	N/A	N/A
Dept. of General Services	Yes	0	Expired	No	N/A
Dept. of Human Res. Mgmt	Yes	0	Expired	No	N/A
Dept. Min. Bus. Enterprise	Yes	1	Pending	Pending	N/A
Employee Dispute Resolution	Yes	3	Expired	Not Due	Not Due
Compensation Board	Yes	1	Expired	No	N/A
State Board of Elections	Yes	1	Expired	No	N/A



# Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Forestry	Yes	1	Expired	Not Due	Not Due
Va. Dept. of Ag. & Cons. Serv.	Yes	30	Yes	Yes	Yes



# Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept of Business Assistance	Yes	2	Yes	Not Due	Not Due
Board of Accountancy	Yes	0	Yes	Yes	Not Due
Dept. of Housing & Community Development	Yes	1	Pending	Some	No
Dept. of Mines, Minerals & Energy	Yes	1	Yes	Yes	Yes
Dept. of Labor & Industry	Yes	3	No	N/A	N/A
Dept. of Professional & Occupational Regulation	Yes	1	Pending	No	N/A
Tobacco Indemnification Commission	Yes	1	No	N/A	N/A
Va. Employment Commission	Yes	2	Expired	Some	Yes
Va. Economic Development Partnership	Yes	0	No	N/A	N/A
Va. Housing Development Authority	No	1	No	N/A	N/A
Va. National Defense Industrial Authority	Yes	0	No	N/A	N/A
Va. Resources Authority	No	0	No	N/A	N/A
Va. Racing Commission	Yes	1	Yes	Pending	Pending



# Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Education	Expired	2	Pending	No	N/A
Frontier Culture Museum of Va.	Yes	0	No	N/A	N/A
Gunston Hall	Yes	0	No	N/A	N/A
Jamestown - Yorktown Foundation	Yes	1	Pending	Pending	N/A
Library of Va.	Yes	1	Expired	Not Due	Not Due
State Council of Higher Education for Va.	Yes	0	No	N/A	N/A
Science Museum of Va.	Yes	1	Pending	N/A	N/A
Va. Commission for the Arts	Yes	0	No	N/A	N/A
Va. Museum of Fine Arts	Yes	2	Pending	Yes	No



# Secretariat: Education (Cont'd)

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Christopher Newport University	Yes	0	Pending	No	N/A
George Mason University	Yes	1	Yes	Some	Yes
James Madison University	Yes	1	Yes	Yes	Some
Longwood University	Yes	1	Pending	Yes	Yes
Norfolk State University	Yes	2	Yes	No	N/A
Old Dominion University	Yes	0	Pending	Yes	YES
Radford University	Yes	0	Yes	Yes	Yes
University of Mary Washington	Yes	1	Yes	Not Due	Not Due
Va. Community College System	Yes	43	Pending	YES	YES
Virginia Military Institute	Yes	0	Expired	No	N/A
Virginia State University	Yes	3	Yes	Not Due	Not Due



# Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Accounts	Yes	4	Yes	No	N/A
Dept. of Planning & Budget	Yes	1	Yes	No	N/A
Dept. of Taxation	Yes	0	Yes	Pending	Some
Dept. of Treasury	Yes	3	Yes	Pending	Some



# Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Health Professions	Yes	2	Yes	Not Due	Not Due
Dept. of Medical Assistance Services	Yes	4	Yes	Yes	Yes
Department of Behavioral Health and Developmental Services <del>DMHMRSAS</del>	Yes	22	Yes	No	N/A
Dept. of Rehabilitative Services	Yes	0	Pending	Pending	N/A
Dept. of Social Services	Yes	1	Expired	No	N/A
Virginia Foundation for Healthy Youth <del>TSF</del>	Yes	1	No	N/A	N/A
Va. Dept. for the Aging	Yes	0	Yes	Not Due	Not Due
Va. Dept. of Health	Yes	3	Yes	Yes	Yes



# Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Conservation & Recreation	Yes	2	YES	YES	YES
Dept. of Environmental Quality	Yes	4	Pending	Some	Pending
Dept of Game & Inland Fisheries	Yes	3	Expired	Some	Some
Dept. of Historic Resources	Yes	2	Expired	No	No
Marine Resources Commission	Yes	3	Yes	Yes	Yes
Va. Museum of Natural History	Yes	1	No	N/A	N/A



# Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Alcoholic Beverage Control	Yes	4	Yes	YES	YES
Commonwealth's Attorney's Services Council	Yes	0	No	N/A	N/A
Dept. of Criminal Justice Services	Yes	2	Pending	Pending	Not Due
Dept. of Fire Programs	Yes	2	Yes	Not Due	Not Due
Dept. of Forensic Science	Yes	1	Expired	No	N/A
Dept. of Juvenile Justice	Yes	3	Pending	No	N/A
Dept. of Military Affairs	Expired	1	No	N/A	N/A
Dept. of Corrections	Yes	2	Expired	Some	No
Dept. of Correctional Education	Yes	1	Yes	Not Due	Not Due
Dept. of Veterans Services	Yes	0	No	N/A	N/A
Va. Dept. of Emergency Management	Yes	2	No	N/A	N/A
Va. State Police	Yes	3	Yes	Yes	Not Due



# Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
The Ctr for Innovative Tech.	Yes	1	Expired	No	N/A
Va. Info. Technologies Agency	Yes	30	Yes	Not Due	Not Due



# Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Motor Vehicles	Yes	2	Yes	Not Due	Not Due
Dept. of Aviation	Yes	3	No	N/A	N/A
Dept. of Rail & Public Trans.	Yes	0	YES	Not Due	Not Due
Motor Vehicle Dealers Board	Yes	0	Pending	N/A	N/A
Va. Dept. Of Transportation	Yes	5	Yes	Pending	Pending



# Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Indigent Defense Commission	Yes	4	Expired	Pending	N/A
State Lottery Dept.	Yes	2	No	N/A	N/A
State Corporation Commission	Yes	3	Yes	Not Due	Not Due
Va. College Savings Plan	Yes	3	Yes	No	N/A
Va. Office for Protection & Advocacy	Yes	1	Exception	Exception	Not Due
Va. Retirement System	Yes	2	Yes	No	N/A
Va. Workers' Compensation Commission	Yes	3	Exception	Exception	Not Due



# Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Office of the Governor	Yes	1	Exception	Exception	Not Due
Office of the Attorney General	Yes	0	Yes	Not Due	Not Due



# Physical Security: Protecting Your Users and What They Use

Bob Baskette:  
CISSP-ISSAP CCNP/CCDP  
Commonwealth Security Incident  
Management Engineer



## COV ITRM SEC 501-01 Facility Requirements

Commensurate with sensitivity and risk, each agency shall or shall require that its service provider document facilities security practices.

- Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).
- Design safeguards to protect against human, natural, and environmental risks.
- Require appropriate environmental controls such as electric power, heating, fire suppression, ventilation, air-conditioning and air purification, as required by the IT systems and data.
- Protect against physical access by unauthorized personnel.
- Control physical access to essential computer hardware, wiring, displays, and networks by the principle of least privilege.
- Provide a system of monitoring and auditing physical access to sensitive IT systems.
- Require that the ISO periodically review the list of persons allowed physical access to sensitive IT systems.



## Physical Security Tenants

- Addresses the physical protection of the resources of an organization.
- Must include the people, data, facilities, equipment, and Information Systems.
- Examines how elements of the physical environment and supporting infrastructure affect the confidentiality, integrity, and availability of information systems.
- Primary consideration is that nothing should impede Life-Safety goals.



## Physical Security Goals

- Physical Security Program should comprise safety and security mechanisms.
- Safety is the protection life and assets from fire, natural disasters, and accidents.
- Security is the protection against vandalism, theft, and attacks by people.
- President's Commission on Critical Infrastructure Protection requires organizations that are part of the national critical infrastructure to have adequate protection mechanisms in place.



# Physical Security Threat Categories

- Man-Made Threats
- Natural environmental threats
- Supply system threats
- Politically motivated threats



# Man-Made Physical Threats

- Sabotage
- Vandalism
- War
- Strike
- Unauthorized access
- Explosives
- Errors or accidents
- Fraud
- Theft



# Natural Physical Threats

- Floods
- Earthquakes
- Storms
- Fires
- Extreme temperatures



# Environmental Physical Threats

- Temperature
- Gases
- Liquid
- Organisms
- Projectiles
- Earthquakes and other severe vibrations
- Lava
- Energy Anomalies



## Supply System Threats

- Power distribution outages
- Communication interruptions
- Water, steam, gas disruptions



# Politically Motivated Physical Threats

- Strikes
- Riots
- Terrorism

## Physical Security Program steps

- Identify team to build program.
  - Carry out Risk analysis.
  - Set acceptable risk level with management.
- Derive baseline from Acceptable Risk Level.
- Create countermeasure performance metrics.
- Identify and implement countermeasures.
- Provide continuous monitoring.



# Issues When Selecting a Facility

- Visibility
  - Surrounding terrain
  - Building markings and signs
  - Type of neighbors
  - Population of area
- Surrounding area and external entities
  - Crime rate, riots, terrorism attacks
  - Proximity to police, medical, and fire
- Accessibility
  - Road access
  - Traffic
  - Proximity to airports, trains
- Natural disasters



## Crime Prevention Through Environmental Design

- Discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.
- Deals mainly with the construction of the facility: internal and external design, and exterior components such as lighting and landscaping.
- The physical environment can be manipulated to create behavioral effects that will reduce crime and the fear of crime.
  - Install benches to encourage people to sit and watch.
  - Only install sidewalks where people should walk.
  - Install computer room in middle of building for protection.

## CPTED Categories

- Natural access controls
  - The guidance of people entering and leaving a space by the placement of doors, fences, lighting, and landscaping.
- Natural surveillance
  - Includes straight lines of sight, low landscaping, raised entrances used to make criminals feel uncomfortable by providing many ways observers could see them.

## CPTED Categories Continued

- Territorial Reinforcement
  - Creates physical designs that emphasize or extend the company's physical sphere of influence so legitimate users feel a sense of ownership of that space. Done via walls, fencing, landscaping, lighting, flags. Make the users proud of the environment and a sense of belonging.
- Activity Support
  - Planned activities for the area to be protected. Provides guidelines for how to use the area and get people to use the area properly



## Security Zones

Interior space should be divided into zones with different security levels.

- Controlled
- Restricted
- Public
- Sensitive

## CPTED verses Target Hardening

- Target Hardening differs from CPTED due to the fact that Target Hardening focuses on denying access through physical and artificial barriers.
  - Locks
  - Alarms
  - Fences
- Target Hardening will lead to restrictions on use, enjoyment, or aesthetics of the physical environment.



## Physical Security Program Control Categories

- Administrative
- Deterrence
- Delaying
- Detection

# Administrative Controls

- Facility Requirements Planning
  - Visibility = low visibility is better (be careful of sign/markers)
  - Local considerations = any hazards in area
  - Natural disasters = wind/flood/earthquakes
  - Transportation = excessive traffic
  - No Joint tenancy
  - External services relative proximity to police/fire/medical
- Secure Facility Management
  - Audit trails and Access Logs
  - Emergency Procedures



# Administrative Controls Continued

- Administrative Personnel controls
  - Pre-employment screening
  - Background checks on employment, references, education
  - Security clearance
  - Ongoing employee reviews



## Deterrent Controls

- Fencing
- Warning signs
- Security guards
- Dogs
- Man-Traps
- Exterior Lighting



# Fencing Information

## Fencing Types

- Extremely High Security
  - 3/8-inch mesh with 11-gauge wire
- Very High Security
  - 3/8-inch mesh with 9-gauge wire
- High Security
  - 1-inch mesh with 11-gauge wire
- Greater Security
  - 2-inch mesh with 9-gauge wire
- Normal Industrial security
  - 2-inch mesh with 6-gauge wire

# Fencing Information Continued

## Fencing Height requirements

- 3' to 4' = Deters casual trespassers
- 6' to 7' = Too hard to climb easily
- 8' with 3 strands of barbed wire = will deter most intruders
- PIDAS Fencing
  - Perimeter Intrusion Detection and Assessment System
  - Fencing that has sensors located in the wire mesh and at the base to detect events

## Gate Types

- Class I
  - Residential use
- Class II
  - Commercial use where general public has access
- Class III
  - Industrial use where limited access is granted
- Class IV
  - Restricted access



# Window Protection / Glazing Types

## Applied during manufacturing

- Standard
  - Cheapest and lowest level of protection
  - Residential use
- Tempered
  - Glass is heated and cooled rapidly
  - Increases strength 5-7 times
- Acrylic
  - Plastic (toxic when burned)
  - Polycarbonate acrylics are strongest glass
- Wired
  - Mesh of wire embedded between two sheets of glass
  - Prevents shattering



## Window Protection Continued

- Laminated
  - Plastic layer between two outer layers of glass
- Solar window film
  - Tinted to provide security
- Security film
  - Transparent film to increase strength



## Exterior Lighting Notes

Exterior Lighting should be at least 8'-high  
with 2' candlepower

Exterior Lighting types:

- Floodlights
- Streetlights
- Fresnel lighting
- Glare Protection
  - Pointing lights at in-bound persons and away from the guard/security personnel



# Surveillance Techniques

- Organized
  - Security guards
  - Guard Dogs
- Mechanical
  - CCTV
  - Card access readers
  - Responsive Area Illumination
    - IDS activated lighting
    - Used in combination with CCTV to allow fast verification of IDS event
- Natural Strategies
  - Straight line of sight
  - Low landscaping
  - Raised entrances



## Guard Drawbacks

- Availability
  - Cannot exist in some environments
- Reliability
  - Pre-employment screening not always effective
- Training
  - Susceptible to social engineering
  - out-of-date manuals
- Cost



## Delay Controls

- Locks
- Defense in depth
  - Establishment of Security Zones
  - Inspection points (Man-Traps)
- Access controls

# Mechanical Locks / Key-based

- Warded locks
  - Basic padlock with spring-loaded bolt with a notch cut in it
  - Wards are metal projections around the keyhole
- Tumbler locks
  - Have multiple metal pieces that must be aligned to allow bolt to move
  - Pin tumbler (Most common type of lock)
  - Wafer tumbler (Disk tumbler) (Uses wafers instead of pins) ( normally found on file cabinets)
  - Lever tumbler

# Code-based Locks

- Combination locks
  - Can be electrical or mechanical
  - Traditional mechanical combination locks use internal wheels
  - Electrical combination locks use a keypad
- Cipher locks
  - Programmable lock
  - Uses keypad and optional swipe card for access
  - The lock code can be changed/reprogrammed and specific user codes blocked
  - Can provide:
    - Door delay alarm if the door is held open
    - Key override
    - Master Keying
    - Hostage alarm/Panic code



# Lock Security Categories

- Lock strengths
  - Grade 1
    - Commercial and industrial use
  - Grade 2
    - Heavy-duty residential / light-duty commercial
  - Grade 3
    - Residential or consumer



## Lock Security Categories Continued

- The delay time provided by a lock should match the resistance of the door, door frame, and hinges.
- Lock cylinder categories
  - Low security
    - No pick or drill resistance
  - Medium security
    - A degree of pick resistance
    - Uses more complex notch combinations
  - High security
    - Pick resistance
    - Only used in Grade 1 and Grade 2 locks



# Locking Mechanism Types

- Fail-safe lock
  - Door defaults to unlocked on loss of power
- Fail-secure lock
  - Door remains locked on loss of power

## Detection Controls

- Intrusion detection systems should be deployed as both external and internal sensors
- IDS mechanisms operate on:
  - Sounds and vibrations
  - Motion
  - Microwave, Ultrasonic, Electrostatic, and Magnetic field variances
  - Electrical circuit
  - Beams of Light

## Electromechanical systems

- Detects break or change in a circuit
- Can be deployed on the exterior or in the interior of a building
- Types:
  - Electrical Circuits
    - Uses contact tape placed across windows/doors or pressure pads placed in front of doors/windows
    - Can also install fine wire mesh to detect breakage of walls or windows
  - Magnetic Switches
    - Uses change in magnetic field between opposing magnets to detect an opening



## Volumetric Systems

- More sensitive than Electromechanical Systems
- Detects changes in subtle environmental characteristics
- Best employed in the interior of a building

# Volumetric System Types

- Acoustic
  - Uses microphones installed in floors, walls, and ceilings
  - Cannot be installed in areas that are exposed to exterior sound sources or dynamic environments
- Seismic/Vibration
  - Used to detect forced entry
  - Normally installed on exterior walls or floors/ceilings of sensitive rooms
- Photoelectric
  - Detects change in light beam
  - Requires consistent illumination
  - Should only be used in rooms without windows
- Proximity detector / capacitance detector
  - Most objects emit a measurable magnetic field
  - Monitors the electrical field around an object

# Volumetric System Types Continued

- Wave-pattern motion detection
  - Uses a wave pattern sent over a sensitive area and reflected back to a receiver
  - A change in pattern indicates a change in the environment
  - Can use Ultrasonic, Microwave, and low frequency patterns
- Passive Infrared Detector
  - System that reacts to fluctuations of ambient light energy within its range.
  - Detect the change in temperature in object or environment



## Environmental / Life Safety Controls

- Electrical power
- Fire Detection and suppression
- HVAC

## Hot Topics

- Fire is the rapid oxidation of materials
  - Requires oxygen, heat, fuel
- Damaging Temperatures
  - Computer Systems 175-F
  - Magnetic Storage 100-F
  - Paper 350-F
- Store only the absolute minimum essential records, paper stock, inks, unused media in the computer room.
- Light-Frame construction can resist rapid oxidation for up to 30 minutes
- Heavy-Timber Frame construction can resist rapid oxidation for up to 1 hour

## Fire Suppression

- **When selecting a fire suppression system consider:**
  - Estimate rate of occurrence
  - Amount of damage potential
  - Types of fires
  - Portable extinguishers should be located within 50-feet of electrical equipment and near exits

## Fire Detection

- Fire Detection (detect thermal combustion or its by-products)
- Smoke-actuated
  - Used in ventilation systems
  - Photoelectric devices are triggered by variation in light
  - Ionization devices react to charged particles in smoke created by the radioactive material in the smoke
- Smoke detectors provide good early-warning
  - Can be used to alert prior to automated suppression release
  - Manually deal with smaller fires

# Fire Detection Continued

- Heat-sensing
  - Alerts when the temperature reaches a pre-set value or a rapid increase is detected
  - Fixed temperature value detection results in lower false positive
- Flame-actuated
  - Sees infrared energy of the flame or the pulsation of the flame
  - Have a very fast response time
  - Fairly expensive
- Sensors should be installed on and above ceilings and below raised floors



# Fire Suppression Equipment

- Class A
  - Common combustibles such as wood, cloth, paper, rubber, plastics
    - Water or soda acid
- Class B
  - Liquids / Petrol / Coolants
    - Gas (Halon or CO<sub>2</sub>) or soda acid
- Class C
  - Electrical equipment
    - Gas (Halon or CO<sub>2</sub>) or soda acid
- Class D
  - Metals
    - Dry powder
- Class K
  - Commercial kitchens
    - Wet chemicals

# Fire Suppression Notes

- Dry chemical composition
  - Sodium bicarbonate, potassium bicarbonate, and calcium carbonate will stop chemical combustion
  - Monoammonium phosphate will melt at low temperatures and excludes oxygen
- Water suppresses the temperature required to sustain the fire
- Foam floats on top of the surface of the material and excludes oxygen
- Soda Acid suppresses the fuel of the fire
- CO<sub>2</sub> suppresses/removes the availability of oxygen (use in unmanned facilities)



## Halon Information

- Halon uses a chemical reaction to suppress the fire
  - Mixes well with air
  - Spreads extremely fast
  - Does not leave a residue
  - Above 900-F will become a toxic mixture (hydrogen Fluoride)
  - Will also deplete ozone
  - Deadly in concentrations greater than 10-percent
- Halon 1211 is liquid (portable)
- Halon 1301 is gas (facility)



# Halon Replacements

- FM-200
- AF-S-111
- CEA-410
- FE-13
- Water
- Inergen
- Argon
- Argonite
- Inert gases or Halocarbon agents.



# Fire Extinguishing Systems

- Dry Pipe System
- Deluge
- Wet Pipe System
- Preaction



# Fire Extinguishing Systems Continued

## Dry Pipe System

- No standing water in pipe
- All water is held in a reserve tank by clapper valve
- Clapper valve is activated by smoke or fire sensors and is designed to suspend the water supply for a short period.
- Once activated, the clapper valve opens, the air is removed from the pipe and the water is released.



# Fire Extinguishing Systems Continued

## Deluge

- Variation on the Dry Pipe System
- Designed to deliver a large volume of water quickly
- Not considered appropriate for computer rooms

# Fire Extinguishing Systems Continued

## Wet Pipe System

- Deliver pipes always contains water
- Sprinkler releases water as soon as the sensor detects smoke or fire
- Is considered a closed-head system
- Most sprinkler head systems use a fusible link in the nozzle that melts at 165-F
- Is considered the most reliable fire suppression system
- The only operational issues is that the system can leak and the pipes can freeze



# Fire Extinguishing Systems Continued

## Preaction

- Recommended for computer rooms
- Hybrid of Wet/Dry Pipe systems
- Will fill pipe with water at first sign of increased heat
- Uses the fusible link to release the water
- Enables manual intervention before discharge of water
- Dry-Pipe and Pre-Action systems use pressurized air in pipe to keep valve closed and water in holding tank



## Fire Related Notes

- Fire extinguishers should be located within 50-feet of electrical equipment and near the exits
- Rate-of-rise temperature sensors provide shorter warning times than fixed temperature sensors, but can generate higher false positives
- Smoke particulate residue will corrode metal contact surfaces and must be removed with Freon or Freon-alcohol solvents
- Detectors should be located on and above drop ceilings and below raised floors

# Electrical Power definitions

- Ground
  - Pathway to earth to enable excessive voltage to dissipate
- Noise
  - Electromagnetic or frequency interference that disrupts power flow
  - Presence of electrical fluctuations in the system that is unintentional and interferes with the transmission of clean power
- Transient noise
  - Short duration of power line disruption

# Electromagnetic Interference

- Electromagnetic interference is caused by the generation of radiation from the charge differences among the three electrical wires
- Common-mode noise
  - Noise from the radiation generated by the charge difference between the hot and ground wires
- Traverse-mode noise
  - Noise from the radiation generated by the charge difference between the hot and neutral wires

# EMI Protection

- TEMPEST
  - Transient EM Pulse Emanation Standard
  - Developed by US and UK military
  - DoD standard to prevent EMI eavesdropping via heavy metal shielding
  - Can use a Faraday cage (outer metal coating on housing unit) to prevent EMI leakage
  - Very expensive to implement
  - Normally only used in highly secured areas
- Two alternatives to Tempest technology:
  - Use white noise (uniform spectrum of random electric signals distributed over the full spectrum)
  - Use a control zone concept



# Radio Frequency Interference

- Radio Frequency Interference noise is generated from radio waves or noise generated by the components of an electrical system such as radiating electrical cables, fluorescent lighting, or electrical space heaters.



## Electrical Noise protection

- Power line conditioning
- Proper grounding of system to earth
- Cable shielding
- Limiting exposure to magnets, fluorescent lights, electric motors, and space heaters

# Power Regulation Issues

- Spike
  - Momentary high voltage
- Surge
  - Prolonged high voltage
- In-Rush current
  - Initial surge of current required to start a load
- Transient
  - Short duration of line noise disturbances



# Power Regulation Issues Continued

- Fault
  - Momentary power outage
- Blackout
  - Prolonged or complete loss of power
- Sag/Dip
  - Momentary low voltage condition that can last from one cycle to a few seconds
- Brownout
  - Prolonged power supply that is below normal voltage

# Power Regulation Mechanisms

- UPS Types
  - On-line
    - Primary power passes through and charges batteries
    - UPS has power inverters that feed power to the data center
  - Standby
    - Stays inactive until failure
    - Will switch to battery on failure
- Metal oxide varistor = used in surge protectors to move the excess voltage to ground
- Constant-voltage transformers can be used to regulate fluctuations in power during brown out conditions

## Static Electricity Precautions:

- Use antistatic spray to treat surfaces
- Use antistatic tables and floor mats
- Data Centers should have antistatic flooring
- Data Centers should have properly grounded power systems
- Use HVAC systems to control the level of humidity in the Data Center
- Humidity should be between 40 and 60 percent.
  - $< 40\%$  = static electricity / 20,000 volts possible
  - $> 60\%$  = condensation on parts / corrosion of connections



# Data Center Notes

- Data Centers should have two doors:
  - Controlled access for entry
  - Locked door with panic bar for emergency exit
- Data Centers must utilize positive air pressure
- Data Centers need water detectors under floors and above ceilings
- Data Centers should have a power feed from two separate substations if possible
- Data Centers should have a separate power feed from the rest of the building
- Data Center doors should open out / use 3-pin hinges
- Avoid internal partitions in secure areas (can pop ceiling tiles and climb over)



# Secure Media Storage (Safes)

- Safe types
  - Wall
  - Floor
  - Chest
  - Depositories
  - Vaults
- Passive relocking safes have extra bolts that fall into place if tampering occurs
- Thermal relocking safes have extra bolts that fall into place if a certain temperature is reached



## Collusion can defeat Physical Controls

### Collusion controls

- Separation of duties
- Pre-employment background check
- Rotation of duties
- Supervision



## Final Thoughts

- Physical Security, like other Security Disciplines, works best in layers moving from the perimeter to the asset.
- Acceptable Risk Level should be derived from the laws and regulations with which the organization must comply and from the threat profile of the organization overall.
- Please reference COV ITRM SEC 501-01 and COV ITRM SEC 517-00 for more information on COV-specific requirements and guidelines.



# Questions???

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

Thank You!



# COVITS 2009

**Peggy Ward**

Chief Information Security &  
Internal Audit Officer





# 11<sup>th</sup> Annual COVITS

## Transparency, Participation & Collaboration

When: September 20-22, 2009

Where: Marriott – Williamsburg, Va.

### Keynote Speakers

Aneesh Chopra, Federal Chief Technology Officer

&

Jerry Mechling, Harvard School of Government

Register at <http://www.covits.org/>

Govt employees: \$99 / SWAM Members: \$99 (Must be certified by the DMBE)



# 11<sup>th</sup> Annual COVITS

Helpful sessions to provide guidance & collaboration on topics pertinent to today's IT challenges:

## Topics include:

- Stimulus/Recovery Review
- Legislator Panel: Challenges in Virginia
- Cloud Computing
- Security: Insider Threats and Outside Attacks
- Continuity of Government Operations
- Data Standardization and Governance
- Economics of Customer Service
- Social Networking and Government
- Open Source and Free Stuff: Appropriate for Government?
- Health IT: The Changes Ahead
- Broadband across the Commonwealth



## Governor's Technology Awards

Winners will be announced at a special ceremony during COVITS 2009.

This awards program honors outstanding achievements & recognizes innovative technology initiatives in the public sector throughout the Commonwealth of Virginia.

**! Winners will receive complimentary admission to COVITS !**

Enter at :

[http://www.covits.org/governor's\\_technology\\_awards/index.cfm](http://www.covits.org/governor's_technology_awards/index.cfm)

**Deadline for submissions is August 19, 2009.**



# COVITS Special Ceremony

## Award Categories

Online, Not in Line

Cross-Boundary Collaboration

IT as Efficiency Driver

Innovative Use of Technology in Local Government

Innovative Use of Technology in K-12 Education

Innovative Use of Technology in Higher Education

Best Private Sector Telework Initiative

Best Public Sector Telework Initiative



# Upcoming Events





# UPCOMING EVENTS! 9/9/09 ISOAG

Wednesday, September 9 From 1:00 – 4:00 pm

**NEW LOCATION!!! State Capitol, House Room 3**

**Tour of the Capitol at 12:00 for the first 50 who register for the tour!**

*Thank you to Alison Anderson, DPB, for coordinating!*

**Keynotes:**

**Critical Infrastructure – Mike McCallister, OCP**

**Identity Theft Program – Steve Werby, VCU**



## UPCOMING EVENTS! Future 2009 ISOAG's

From 1:00 – 4:00 pm at CESC

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

**Tuesday -**                      **October 6**

**Wednesday -**                **November 4**

**Wednesday -**                **December 9**



# Information Security System Association

ISSA meets on the second Wednesday of every month

- **DATE:** Wednesday September 16th
- **LOCATION:** Hondo's, The Shoppes at Innsbrook  
4024-C Cox Road, Glen Allen, VA (directions at [http://www.hondosprime.com/get\\_directions.shtml](http://www.hondosprime.com/get_directions.shtml))
- **Topic:** "Nine Proven Software Security Best Practices – Building Security in maturity Model (BSIMM)"
- **TIME:** 11:30 - 1:30pm. Presentation starts at 11:45 & Lunch served at 12.
- **COST:** ISSA members: \$10 & Non-Members: \$20



# UPCOMING EVENTS: MS-ISAC Webcast

## National Webcast!

Wednesday, August 19, 2009, 2:00 to 3:00 p.m.

Topic: Security of Social Networking Sites/Web 2.0

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

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



## UPCOMING EVENTS - CIO-CAO Mtg.

### CIO-CAO Communications Meeting:

**Tuesday, August 25**

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

**Location:** Perimeter Center  
9960 Mayland Drive  
Richmond, VA



## FACTA Red Flag Requirements \*NEW DATE

Implementation Date: **November 1<sup>st</sup>, 2009**

Announcement at: <http://www.ftc.gov/opa/2009/07/redflag.shtm>

Are you aware of the red flag requirements in the Fair and Accurate Credit Transactions Act (FACTA) of 2003?

Please read carefully as it is not only banks and financial institutions!

<http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>



Any Other Business ???????



# ADJOURN

**THANK YOU FOR ATTENDING!!**

