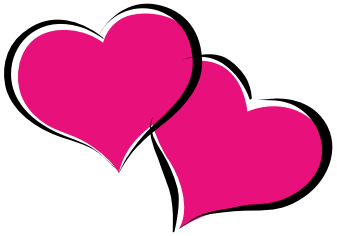
Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

February 6, 2008

February



Valentines Day!

President's Day!

Leap Year!

ISOAG February 2008 Agenda

I.	Welcome and Opening Remarks	Peggy Ward, (VITA)
II.	Fusion Center	William Tinsley, (VDEM)
III.	Security Management in the ITIL framework	Adriaan Van De Rijken, (NGC)
IV.	ITP Transformation Update	Chad Wirz, (VITA)
V.	CPE and Certification	Cathie Brown, (VITA)
VI.	At Risk! Securing Govt in a Digital World	NASCIO Video
VII.	Incident Management Process	Michael Watson, (VITA)
VIII.	General Assembly Legislation	Peggy Ward, (VITA)
IX.	Upcoming Events & Other Business	Peggy Ward, (VITA)

Virginia Fusion Center (VFC)

January 2008

VFC Location

- Located at VSP Administrative Headquarters
- Adjacent to the Virginia Emergency Operations Center (VEOC)

VFC Mission

- *Primary Mission:* Fuse together resources from local, state, and federal agencies and private industries to facilitate information collection, analysis, & sharing in order to prevent terrorist attacks and criminal activity.
- *Secondary Mission:* In support of VEOC, centralize information and resources to provide a coordinated and effective response in the event of an attack.

Superintendent's Advisory Board

- Meet semi-annually
- Receives and reviews reports submitted by Working Group
- Makes decisions regarding operational problems identified by Working Group
- Produces Annual Report to the Governor

Superintendent's Advisory Board

- Chaired by VSP Superintendent or his designee
- Co-chaired by VDEM State Coord. or designee
- Board Representatives include:
  - Department of Fire Programs
  - FBI and DHS
  - Office of Commonwealth Preparedness
  - Virginia National Guard
  - Police Chief's Association
  - Sheriff's Association

Working Group

- Chaired by F/Sgt Tinsley and Fred Vincent
- Meet quarterly
- In support of Superintendent's Advisory Board, makes recommendations regarding:
  - Operational problems or difficulties
  - Needs or enhancements of VFC
  - Policies and Procedures for security, information management, classification, and dissemination
  - Any other matters determined by the group and approved by the Steering Committee
- Produces reports to the Advisory board regarding activity and recommendations

Reporting Information to VFC

- Terrorism Hotline: 877-4VA-TIPS
- General Number: 804-674-2196
- Fax Number: 804-674-2983
- E-mail: vfc@vsp.virginia.gov

Fred Vincent

Special Assistant for Commonwealth Security

804.674.2911

fred.vincent@vdem.virginia.gov

Security Management in the ITIL framework

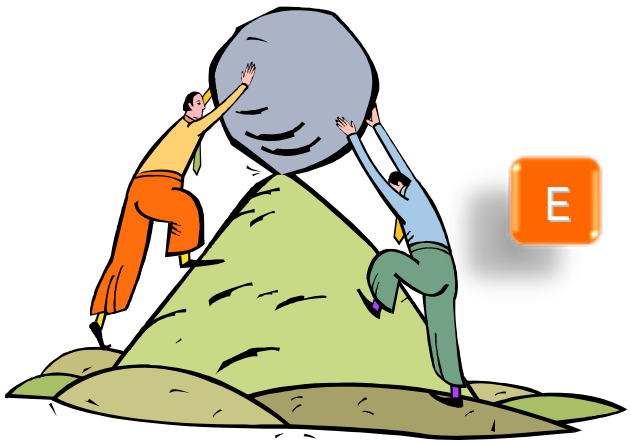
Adriaan Van De Rijken

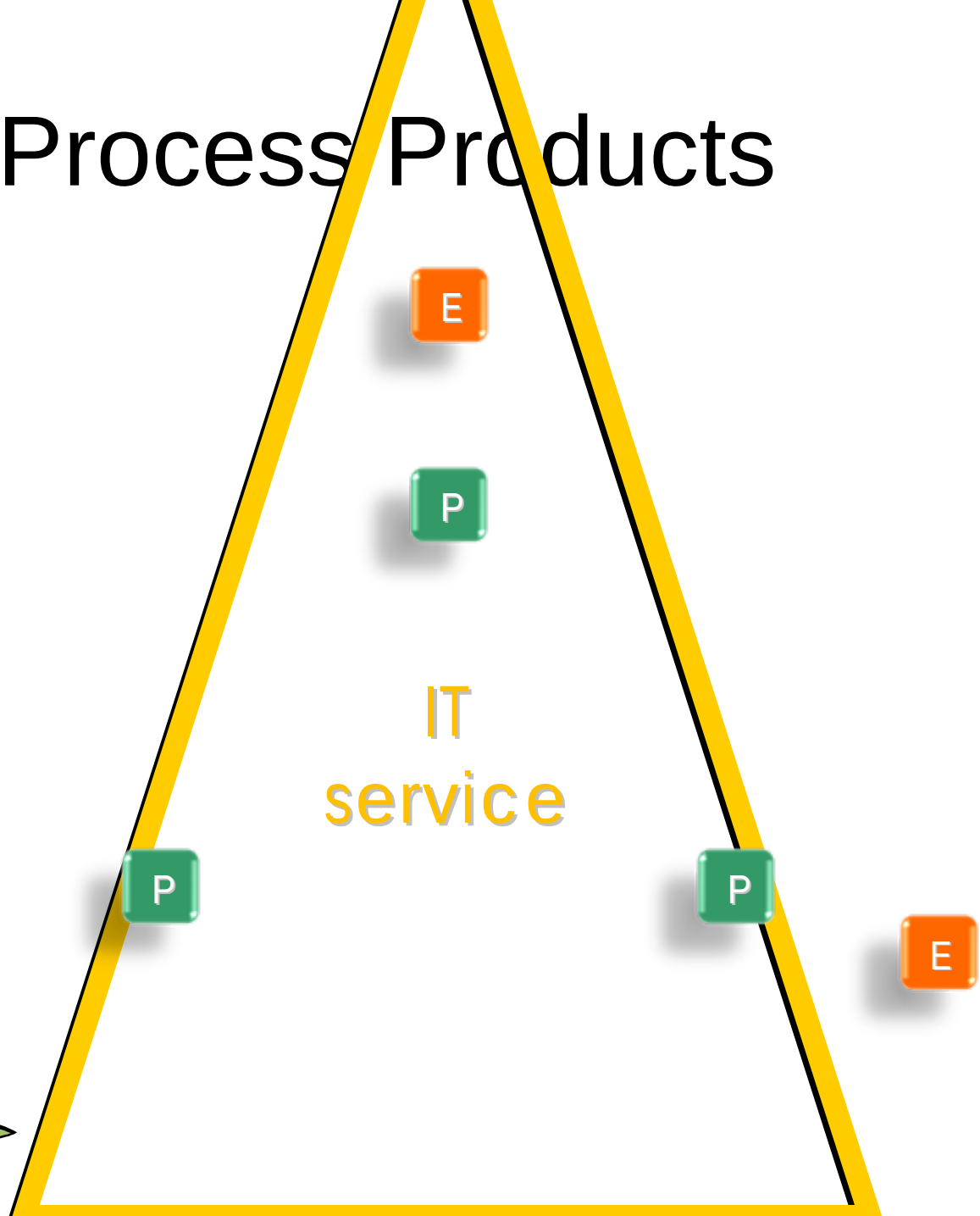
ITIL Service Lifecycle

Information Security Management

People Process Products

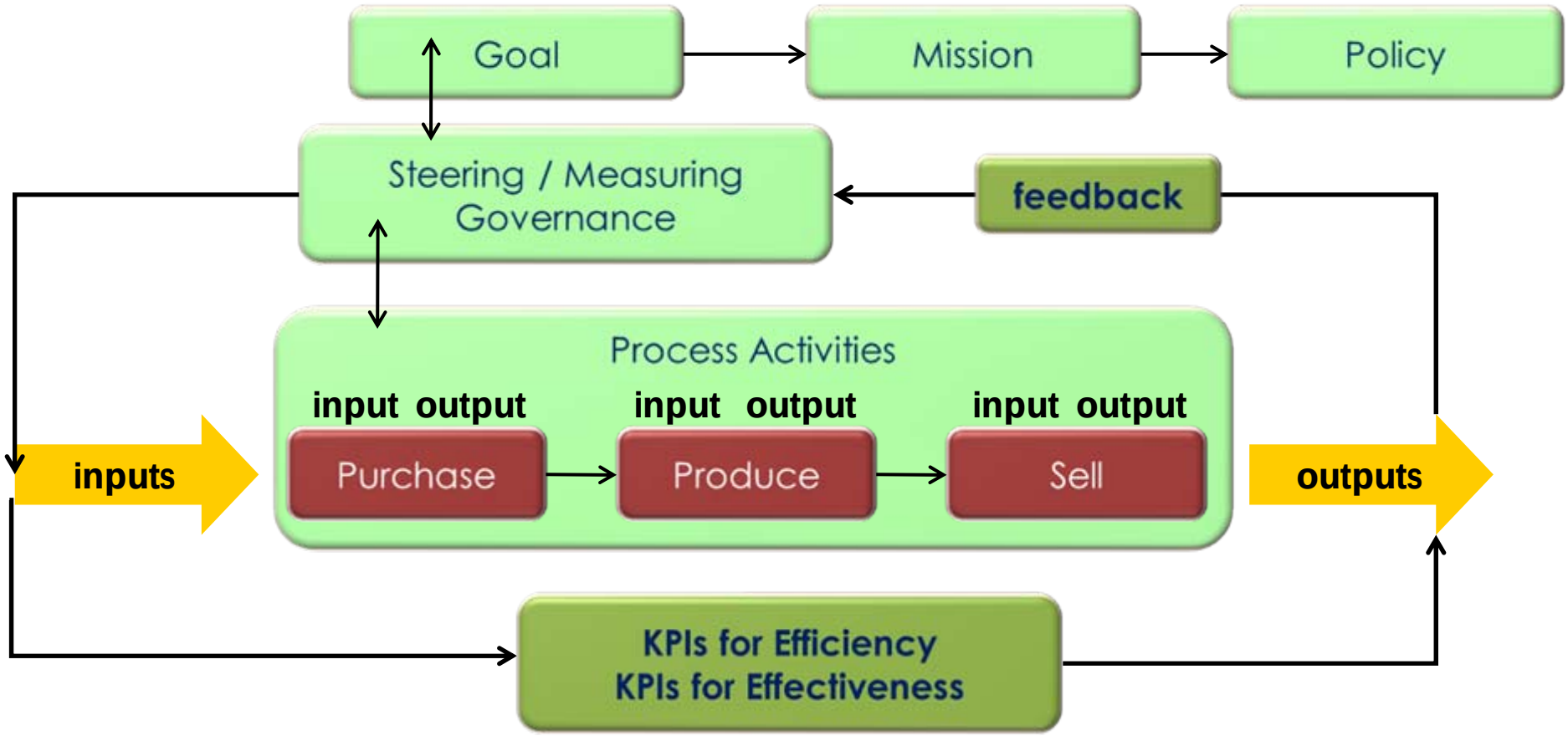
Find the balance between Flexibility and Stability

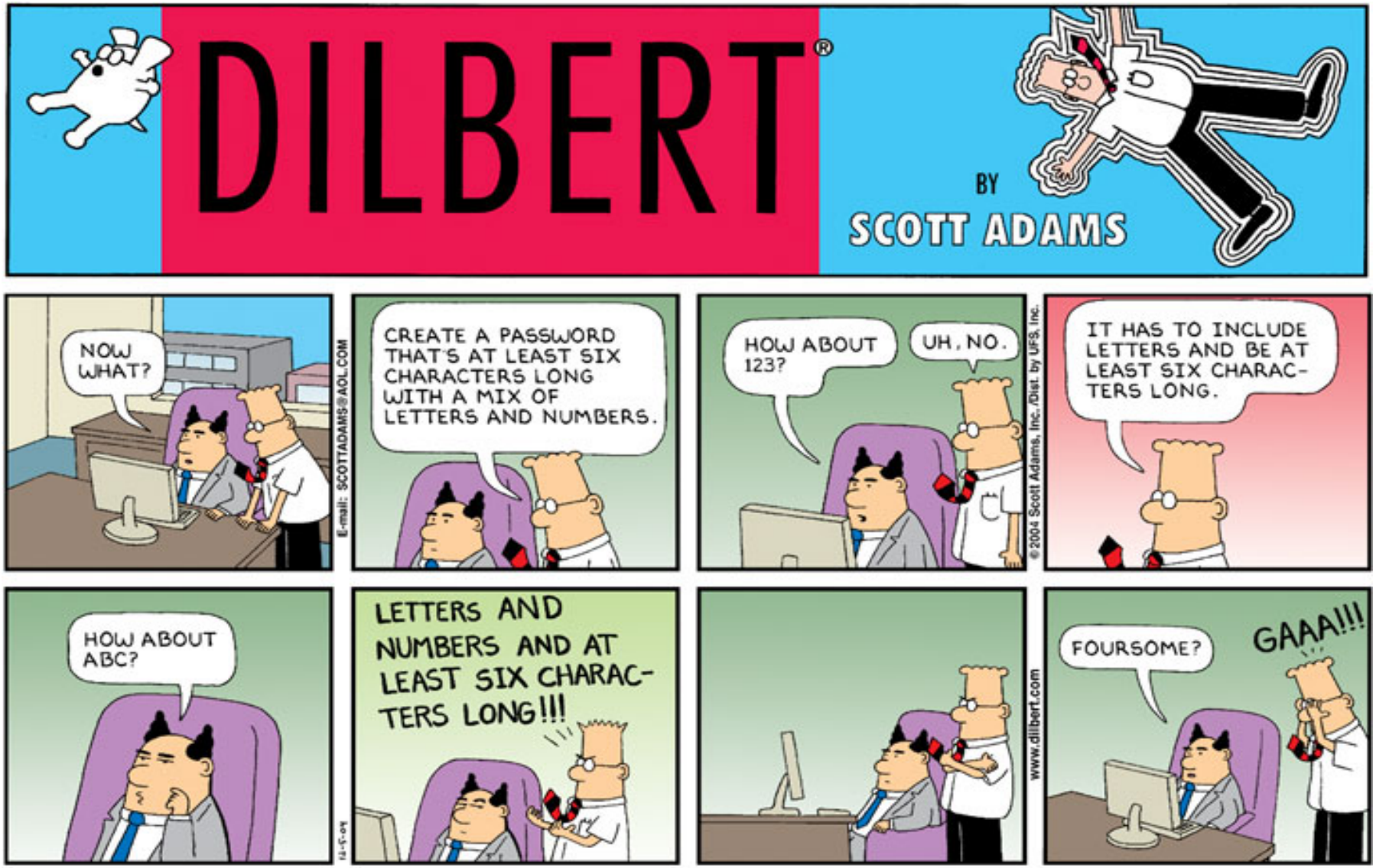




Tiers of Guidance

Process


Goal
Mission
Policy
Steering / Measuring
Governance
feedback
Process Activities
input output
input output
input output
inputs
Purchase
Produce
Sell
outputs
KPIs for Efficiency
KPIs for Effectiveness



© UFS, Inc.

Source: *Dilbert*, http://www.comics.com/comics/dilbert/archive/dilbert-20041205.html

Information Security Management Objectives

- Align IT Security with Business Security
- Provide focus for all aspects of IT security
- Manage all IT Security activities

Objectives are met when…

- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is complete, accurate and protected against unauthorized modification (integrity)

Objectives are met when…

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability)
- Business transactions, as well as information exchanges between enterprises, or with partners, can be trusted (authenticity and non-repudiation).
- Prioritization of confidentiality, integrity and availability are considered in the context of business and business processes.

Terminology

- Confidentiality
  Preventing unauthorized disclosure of information
- Integrity
  Preventing unauthorized modification of information
- Availability
  Having usable information available

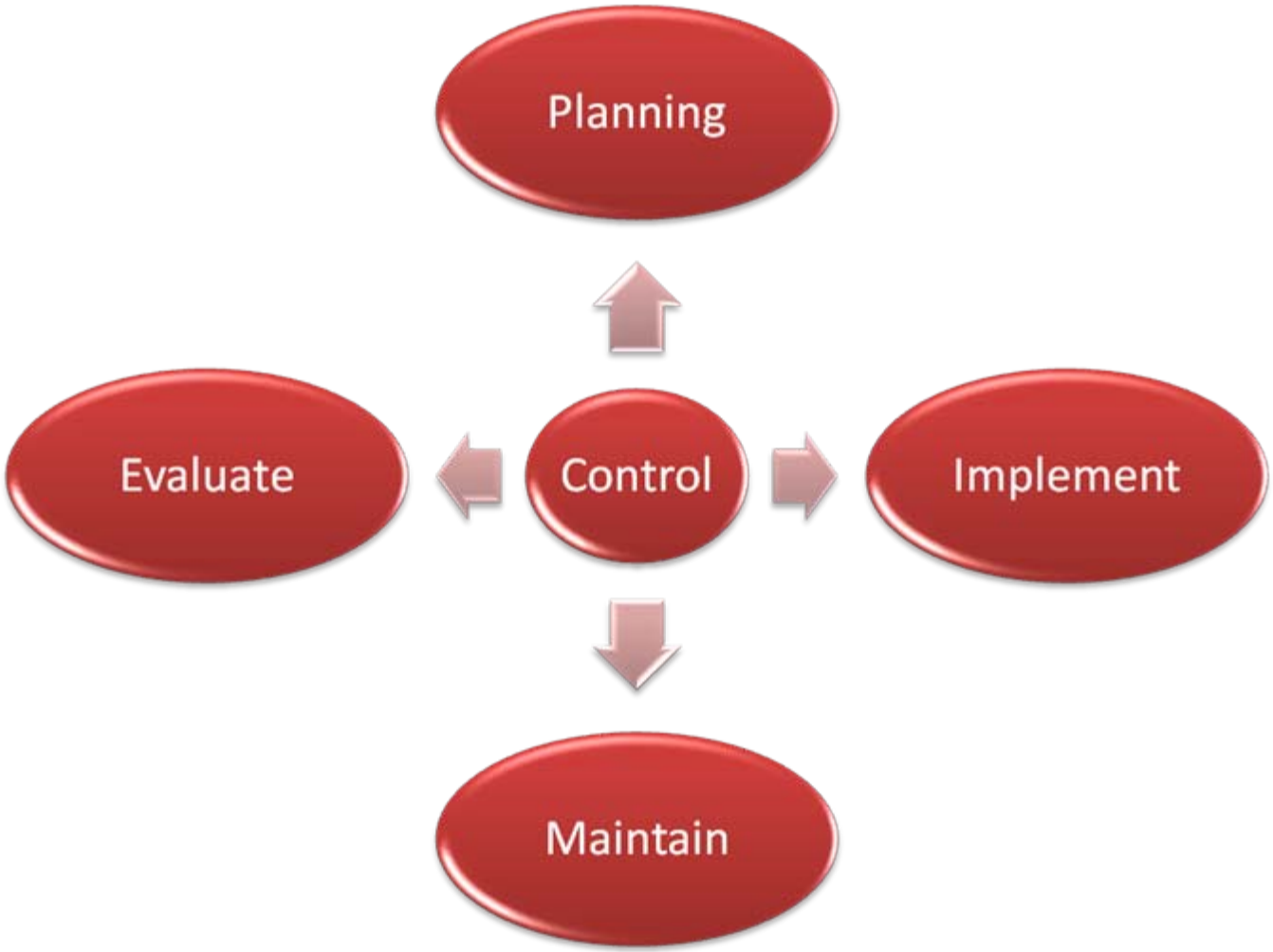
Terminology

- Authenticity
  Quality of being authoritative, valid, genuine
- Utility
  Usefulness of information
- Possession
  Act or condition of having or taking control of for your use and disposal

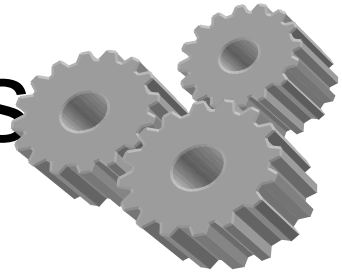
Information Security Manager Role

- Developing and maintaining the Information Security policy
- Ensure enforcement of Information Security policy
- Assisting Business Impact Analysis
- Perform Security risk analysis
- Monitor and manage security breaches

Information Security Management Concepts

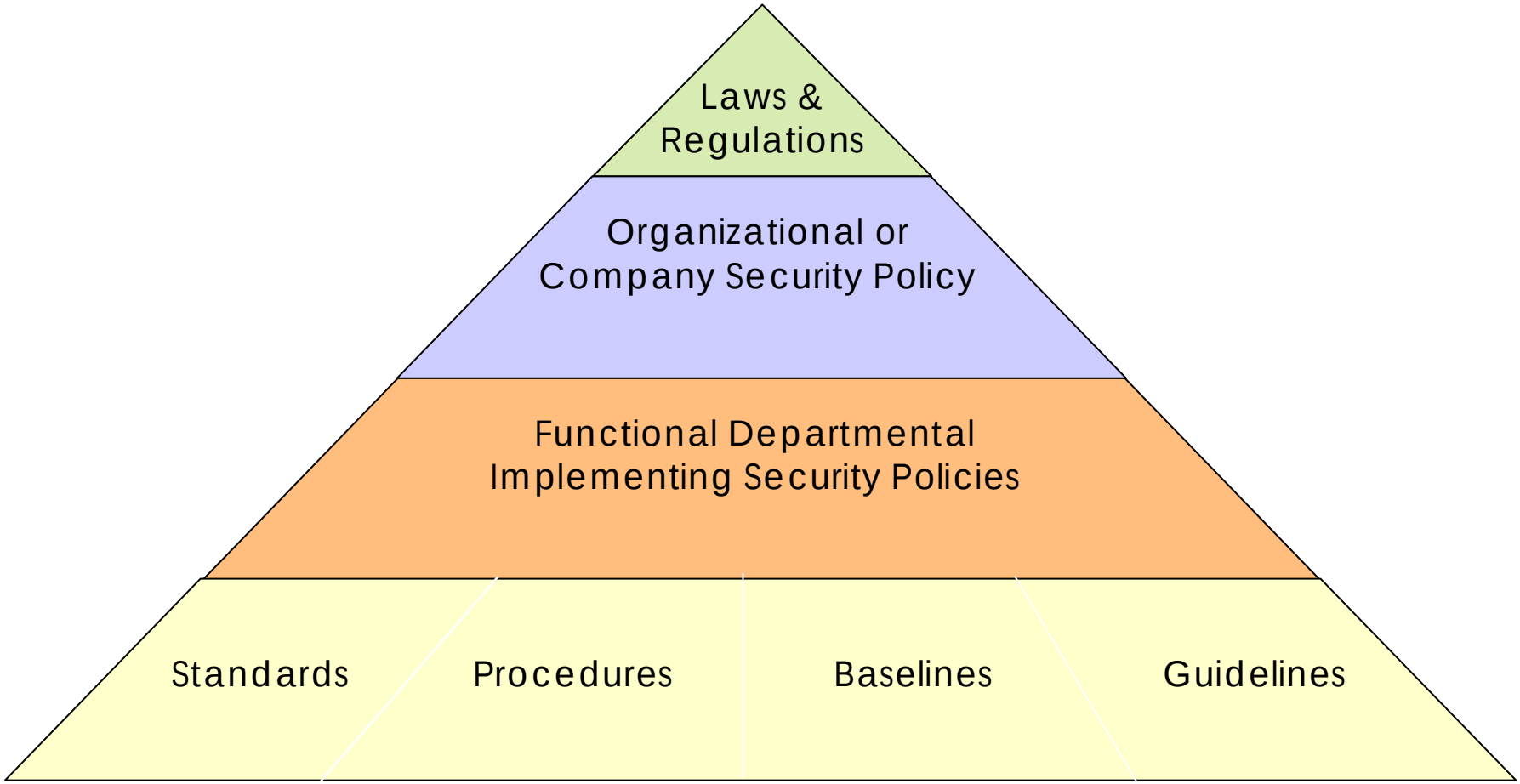


Baseline Controls



- Total Cost of Safeguard / Benefit Analysis
  - Is it cost effective?
  - Is it an effective safeguard?
  - Does it provide value?
  - Is it a complete solution?

Security Policy Pyramid



Service Desk/Incident Management

- Single Point of Contact
- Recognize Security Incidents
- Depending on Impact
  Follow other procedure
- Confidentiality
- Communication via Security Manager

Security Incidents

- Allow anonymous calls
- Use of standard form
- Escalation path
- Registration

Change Management

- Introduction of new measures for security in IT infrastructure
- Ensure current measures are adapted
- Implementation of changes can cause security incidents
- Utilize evaluation and control function of Change Management
- Security Manager in Change Advisory Board

Configuration Management

- IT components are provided with security classification
- Relationship with security measures or procedures
- Verification
- Reporting on IT components with security classification

Availability Management

- Ensure Security Policies are enforced in design of new or modified services (applications)

- Security = Law maker
- Availability = Law enforcer

Q&A

IT Infrastructure Partnership Program

Chad Wirz

February 6, 2008
ISO Meeting

INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Messaging Services

Enterprise Exchange/Outlook Email
Enterprise Collaboration Tools
Active Directory, DNS
$25M Investment

Desktop

Mass Desktop Refresh Projects
Network Printer Consolidation and Refresh
Enterprise Desktop Management Systems
$35M Investment

Help Desk

Enterprise Help Desk in Russell and Chesterfield Counties
Field Based Agents and Technicians for Level 3
Enterprise Help Desk System (Peregrine)
$10M Investment

Mainframe and Servers

New IBM and Unisys Mainframes in New Data Center
Consolidation and Refresh of Servers
Migration of servers to the Data Center
$50M Investment

Transformation

$270 Million Investment

Reliable, High Performance,
Enterprise-Wide IT Infrastructure

ITIL

"People – Processes – Tools"

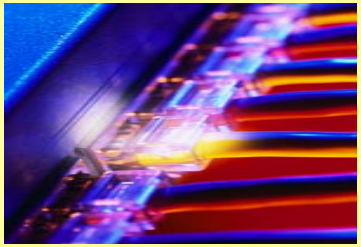
Security

Enterprise Security Operations Center
Computer Security Incident Response Center
Secure Internet Gateway
$10M Investment

Facilities Tier 3 and Tier 2

New Data Center/Office Building in Chesterfield
New Disaster Recovery Center and Help Desk
in Russell County
$60M Investment

Network



New Commonwealth-wide MPLS Core WAN
LAN upgrades to Local Switches/Routers as Needed
Network Re-addressing of IP, DHCP
$60M Investment

Voice / Video

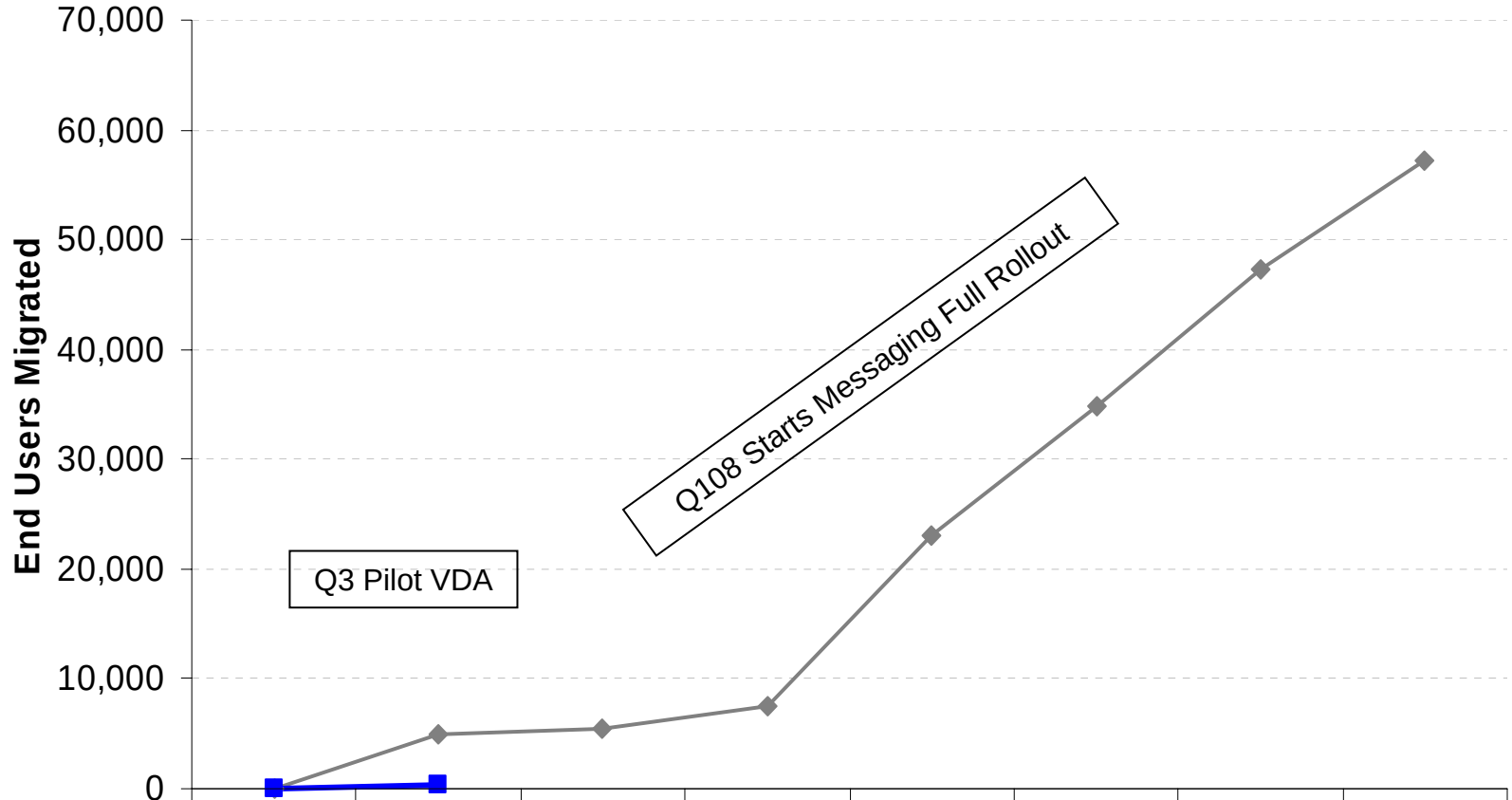
Voice over IP Network Optimized for
Voice and Video Traffic
$20M Investment

Directory Services & Messaging Security Standards

- Ease in verifying compliance for auditing purposes
- Monitored by CMOC and ESOC
- Protected by HIDS and NIDS
- SLAs are easily reported and verified
- Standardized support and repeatable processes for account management
- High availability and data center redundancy
- Can be leveraged for application authentication

Messaging quarterly run rate

Exchange End User Migration Approach

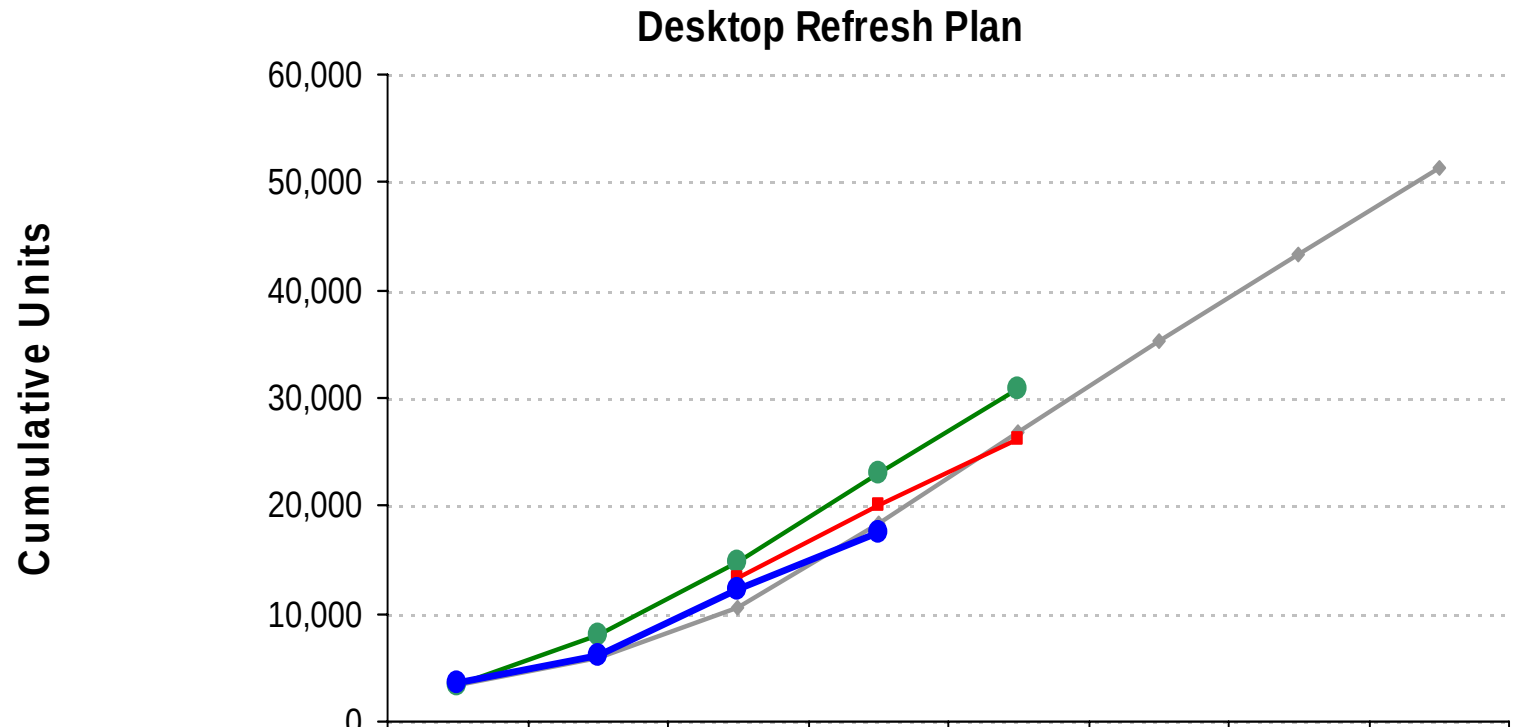


	Q3 CY07	Q4 CY07	Q1 CY08	Q2 CY08	Q3 CY08	Q4 CY08	Q1 CY09	Q2 CY09
Planned	50	4,989	5,401	7,562	23,097	34,855	47,213	57,213
Actual	50	339						

Desktop Security Standards

- Firewall
  - Deployed to prevent inbound attacks
  - If an agency has more restrictive tool, that tool will be left in place
- Local Admin Rights
  - Protection against unintentional modifications
  - Exceptions granted by the CISO (Peggy Ward) for a maximum of 1 year
- PC Encryption

Desktop quarterly run rate



	Apr 07	Jul 07	Oct 07	Jan 08	Apr 08	Jun 08	Oct 08	Mar 09
Baseline Target	3,484	5,984	10,484	18,484	26,884	35,284	43,284	51,284
Scheduled	3,484	7,984	14,792	23,111	30,746			
20% Rule Historical Dropoff			13,400	20,085	26,194			
Actuals	3,499	6,055	12,241	17,631				

Enterprise Solutions Center Security Standards

- RPB to CESC Move provides:
  - Building dedicated for the Commonwealth's consolidated data center (no commercial tenants)
  - Two power feeds off of separate power grids
  - UPS and on-site generator protection
  - Redundant water supply, cooling, electrical, and mechanical infrastructure
  - State of the art surveillance both internal and external
  - External parking areas
  - Additional levels of physical security for 'raised floor' access
  - State of the art fire/hazard detection
  - without commercial tenants
  - Infrastructure to support data center to data center backup for contingency purposes (CESC – SWESC)

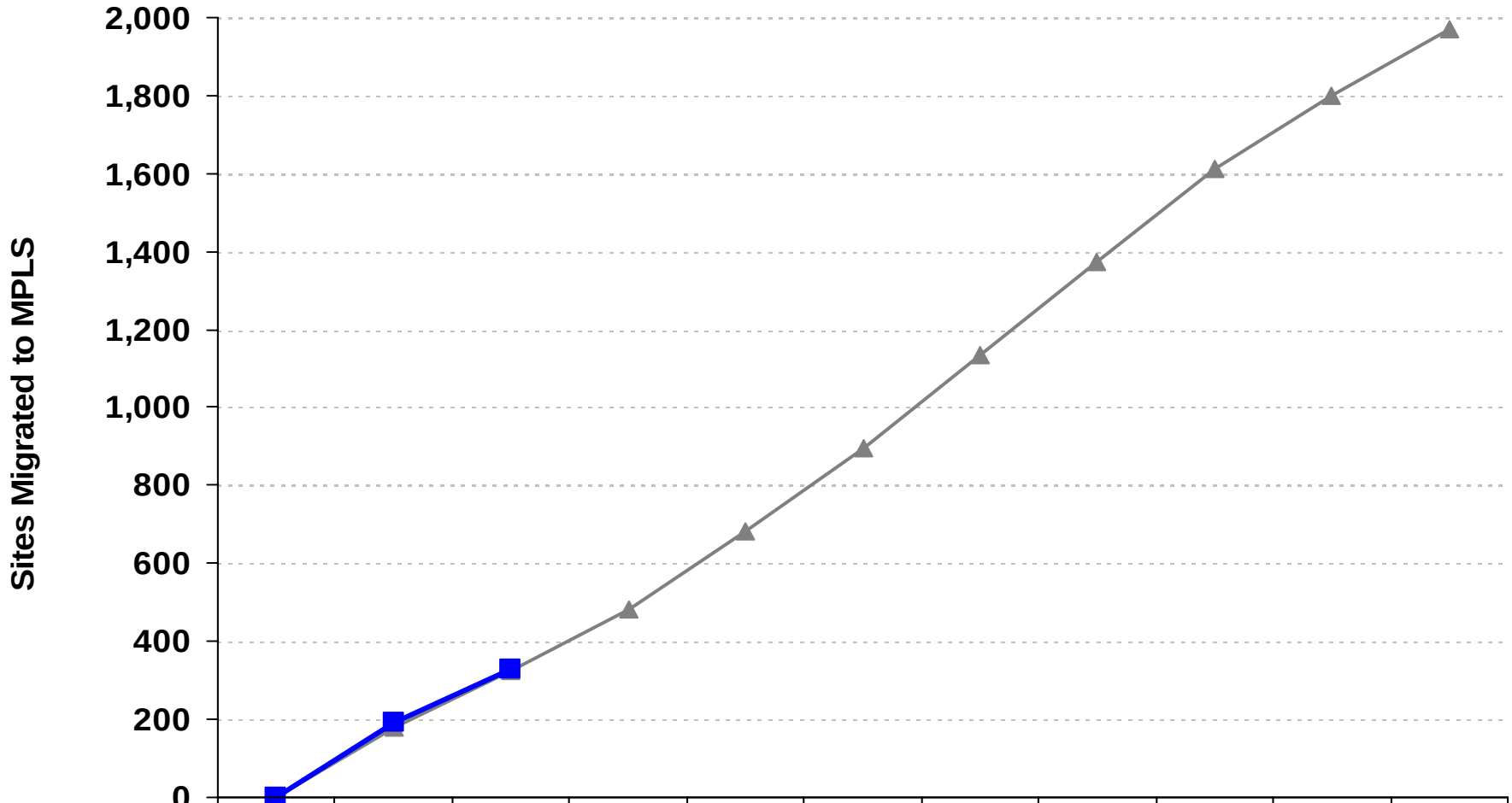
Enterprise Solution Center

- All Mainframe, Server, Network, etc. moved from Richmond Plaza Building to CESC
- Planning underway to analyze agency location equipment for relocation. (completion 06/09)
- SWESC commissioned

Network Security Standards

- **Network Transformation will create a more secure environment**
  - Review Firewall, blocked sites, and content filtering rules
  - Identify required remedial activities for firewalls, blocked sites, and content filtering.
  - Separate agency traffic with VRF (Virtual Route Forwarding) in the MPLS cloud
- **Benefits to the agency**
  - Internet Secure Gateway (ISG) comprised of several integral components that provide both user accessibility and security.
  - Standardized Security Architecture and Centralized Management of security devices.
  - Meet Commonwealth business and security requirements for firewall, blocked sites and content filtering standards.

Network migration



	Jul '07	Sep '07	Nov '07	Jan '08	Mar '08	May '08	Jul '08	Sep '08	Nov '08	Jan '09	Mar '09
Planned Migration	0	180	326	482	684	894	1,134	1,374	1,614	1,798	1,972
Actual Migration	0	190	328								

Virginia Information Technologies Agency

Security/Audit Certifications and CPE's

Cathie Brown

Deputy Chief Information Security Officer

Agenda

- Security/Audit Related Certifications
  - CISSP (ISC(2)
  - CISA/CISM (ISACA)
  - CPA (AICPA & BOA)
  - CIA (Institute of Internal Auditors)
  - GIAC (SANS)
- CPE's Continuing Professional Education
- Process for ISOAG Meetings

CISSP

- Certified Information System Security Professional
- Governed by the International Information Systems Security Certification Consortium (commonly known as (ISC)²)
- Approved by the U.S. Department of Defense (DoD) in both their Information Assurance Technical (IAT) and Managerial (IAM) categories
- Adopted as a baseline for the U.S. National Security Agency's ISSEP program

CISM

- Certified Information Security Manager
- Governed by ISACA (previously known as Information Systems Audit and Control Association, but now goes by its acronym only) www.isaca.org
- Uniquely targets information security management audience

CISA

- Certified Information Systems Auditor
- Also governed by ISACA
- Globally accepted standard of achievement among information systems (IS) audit, control and security professionals

CISA/CISM

- ANSI accredited both certifications under ISO/IEC 17024:2003 General requirements for bodies operating certification of persons
- ANSI/ISO/IEC 17024 intent is to ensure programs are following accepted standards and guidelines when producing certified individuals.

CPA

- Certified Public Accountant
- Governed by the American Institute of CPA's and the Virginia Board of Accountancy (BOA) www.boa.virginia.gov
- Statutory title of qualified accountants who are licensed to provide public attestation and auditing opinions on financial statements

CIA

- Certified Internal Auditor
- Governed by The Institute of Internal Auditors www.theiia.org
- Hallmark designation of internal audit
- The only globally accepted designation for internal auditors

GIAC

- Global Information Assurance Certification
- Governed by SANS Institute (SysAdmin, Audit, Network, Security) www.sans.org
- Accreditation by ANSI/ISO/IEC 17024:2003 Certification Accreditation Program

CPE Units

- "*Continuing Professional Education (CPE)*"
- Required to maintain most certifications
- Earned through activities such as:
  - Attending educational courses or seminars
  - Attending conferences (related to topic)
  - Being a member of an association and attending meetings
  - Completing college courses (related to topic)
  - Publishing articles or books (related to topic)
  - Self-study

CPE Units for ISOAG Attendance

- ISOAG Meetings qualify
- 50 min to 1 hr = 1 CPE Unit (depending on certification)
- Attendance must be recorded (sign-in and sign-out)
- Documentation about topics and speakers must be maintained
- Subject to audit by certification sponsor

How does this work?

- When registering online for ISOAG Meeting, check the box for CPE (beginning March, 2008)
- Sign in when you arrive
- Before you leave
  - Sign Out
  - Pick up Certificate
- We will email certificates to attendees via webconference
- Submit CPE Units to the sponsor of your certification

For additional information

- CISSP
  https://www.isc2.org/download/CISSP%20Recertification%20Guidelines.pdf
- CISA/CISM
  http://www.isaca.org/Template.cfm?Section=Certification&Template=/ContentManagement/ContentDisplay.cfm&ContentID=19934
- CPA
  http://www.boa.state.va.us/boardregulations.asp
- CIA
  http://www.theiia.org/certification/why-become-certified/certification-faq/?search=CPE&C=449&I=1022
- GIAC
  http://www.giac.org/certifications/

IT Security Audit Standard - change

Under 2.1 Planning for IT Security Audits:

Annually, each Agency shall develop/update an IT security audit plan for the government databases for which it is the Data Owner. The IT security audit plan shall be based on the Business Impact Analysis (BIA) and data classification performed by the Agency. Each Agency Head shall submit the Agency IT security audit plan to the CISO initially and whenever there is an update. However, the initial IT security audit plan shall be submitted to the CISO at the Agency's earliest convenience, but not later than 7 months after the effective date of this standard.

If the Audit Plan has not changed from previous submission, a notification to the CISO stating such is acceptable.

Virginia Information Technologies Agency

AT RISK! Securing Government in a Digital World

NASCIO

Virginia Information Technologies Agency

Security Incidents and You! Incident Handling in the COV

Michael Watson

Incident Management Director

What's an Incident and why do I care?

- What is a security incident anyway?
- A security incident occurred, now what?
- How can VITA help with the incident?
- What am I responsible for?
- How does this help?

As Defined on VITA Website

- Information Technology Security Incident
  - refers to an adverse event in an information system, network, and/or workstation, or the threat of the occurrence of such an event.
- Event
  - An event is any observable occurrence in a system, network, and/or workstation. Although natural disasters and other non-security related disasters (power outages) are also called events, Commonwealth Security is primarily interested in IT security related events. Events can many times indicate an information technology security incident is happening.

The Code says…

- All executive branch agencies including institutions of higher education are required to report information technology security incidents to VITA except for the UVA, Virginia Tech, and William and Mary.

- § 2.2-603. Authority of agency directors.
  - F. The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in § 2.2-2005, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence.

- ISO's are typically involved in reporting the incident.

The Standard says…

- SEC501 Section 9.4 Purpose –IT Security Incident Handling requirements identify the steps necessary to respond to suspected or known breaches to IT security safeguards.

- Each agency shall or shall require that its service provider document IT security incident handling practices that include the following components, at a minimum:
  - Designate an IT Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.
  - Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.
  - Implement proactive measures based on cyber attacks to defend against new forms of cyber attacks.
  - Establish IT security incident categorization and prioritization based on the immediate and potential adverse effect of the IT security incident and the sensitivity of affected IT systems and data.
  - Identify immediate mitigation procedures, including specific instructions, based on IT security incident categorization level, on whether or not to shut down or disconnect affected IT systems.

The Standard says more…

- SEC501 Section 9.4 –IT Security Incident Handling (continued):
  - Establish a process for reporting IT security incidents to the CISO. Executive branch agencies must establish a reporting process for IT security incidents in accordance with §2.2-603(F) of the Code of Virginia so as to report "to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence," "all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities."
  - Establish requirements for internal agency IT security incident recording and reporting requirements, including a template for the incident report.
  - Establish procedures for IT security incident investigation, preservation of evidence, and forensic analysis.
  - Report IT security incidents only through channels that have not been compromised.

Previous Guidance on what to report…

- An information technology security incident should be reported if the following conditions are met:
  - it was intentional and successful

    AND

  - it resulted in either:
    - exposure of legally protected data in Commonwealth databases, such as personally identifiable information, financial information protected by GLBA, or health information protected by HIPAA;

      OR

    - major disruption to normal agency activities carried out via Commonwealth data communications, such as network unavailability for all or significant portions of an agency due to a denial of service (DOS) attack.

New Guidance on what to Report

- An information technology security incident should be reported if the following conditions are met:
  - it resulted in:
    - A violation of Commonwealth Security's and/or the Agency's explicit or implied security policies.
      Examples of this include unauthorized access or use of a system or data.

      OR

    - Unauthorized exposure of Commonwealth data, such as personally identifiable information, financial information protected by GLBA, or health information protected by HIPAA;

      OR

    - Major disruption to normal agency activities. Often this case will occur via Commonwealth data communications. An example of a major disruption is network unavailability for all or significant portions of an agency due to a denial of service (DOS) attack.
- Determining if exposure of data occurred can be difficult. When in doubt or unable to determine what happened, report an incident.
  - We are here to help.
- For additional guidance and more information about incident reporting visit VITA's website

Now what do I do about it?

- Report the security incident within 24 hours
  - https://www.vita.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm
  - An email acknowledgement will be sent confirming receipt of the report.
- Be aware of digital evidence and forensics
- Plan ahead
  - Contact Information
  - Basic Supplies
  - Environment Information
- Ask for help
  - COV CSIRT Team is available

Doesn't NG handle this stuff?

- Maintaining the infrastructure vs. Maintaining the data
  - Only the agency (specifically the data owner), knows the data to be concerned about.
  - Any infrastructure incidents not related directly to an agency are reported to Commonwealth Incident Management.
    - Incidents directly related to an agency be reported to both the agency ISO and COV Incident Management.
- Current plans include NG providing COV Security with IDS reports and other network monitoring data.
  - In addition COV Security has monitoring equipment in place.

So what does COV Incident Mgmt do?

- What can COV Incident Management do to help?
  - CSIRT – Computer Security Incident Response Team
    - The primary function of the security incident management team is to help investigate security incidents and recommend appropriate action to be taken.
  - Security incident management also provides computer forensic services when necessary.
  - The team coordinates between the parties involved in an incident.
- Actual security incidents have an incident summary for documentation and tracking purposes.
  - Summaries help with trending
  - Helps determine if any weak areas of security within the Commonwealth exist.
  - Annual Report to Governor
    - Includes statistics such as number of incidents, how long it took to resolve them, and how long it took to report them.

Great! So what do you do when you're not handling incidents?

- Monitoring the Security Community
  - Evaluate data from various information sources.
    - Keylogging
    - Botnets
    - Log reviews
  - Investigating vulnerability announcements
    - Microsoft's security bulletins
    - Application vulnerabilities
    - Widespread cyber attacks
- Working to develop security communication throughout the Commonwealth
  - Create communication channels to handle cyber incidents that impact the COV

It would be great if…

- We are always looking to improve service!
  - Let us know if we can help
  - Ideas for new services
  - Areas that you would like more education on

VITASecurityServices@VITA.Virginia.Gov

Virginia Information Technologies Agency

General Assembly Legislation 2008 Session

Peggy Ward
Chief Information Security & Internal Audit Officer

HB 345

Credit reports; authorizes an individual to freeze access thereto

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb345

Credit reports; freezing access. Authorizes an individual to freeze access to his credit report. If a consumer has placed a freeze on his credit report, a consumer reporting agency is prohibited from releasing the credit report, or any information in it, without the consumer's express authorization. The measure provides a means by which a consumer can release his report, permanently, temporarily, or to a specific third party. Certain disclosures are exempt from the freeze. Violations are a prohibited practice under the Consumer Protection Act.

Patrons: Plum, Bulova, Scott, J.M. and Shuler

STATUS: 01/29/08 House: Incorporated by Commerce and Labor (HB1311-Byron) by voice vote

HB 384

Computer trespass; alters elements of crime

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb384

Computer trespass; penalty. Alters the elements of the crime of computer trespass, no longer requiring that a person act with malicious intent in order to be guilty but requiring that the crime be committed without the consent and authorization of the computer's owner. *Patron: Ware, R.L.*

STATUS: 01/10/08 House: Assigned Courts sub: Criminal

HB 385

Computer invasion of privacy; personal information

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb385

Computer invasion of privacy; personal information; penalties. Expands the type of information, the examination of which without authority would constitute the crime of computer invasion of privacy, to include any personal information relating to any other person as well as another person's name and date of birth. ***Patron: Ware, R.L.***

STATUS: 01/10/08 House: Assigned Courts sub: Criminal

HB 390

Compromised Data Notification Act; created

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb390

Compromised Data Notification Act. Creates the Compromised Data Notification Act, which, following discovery or notification of a breach of a security system, requires a state agency that owns or licenses computerized data that includes personal information to provide notice of the breach to all residents of Virginia whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The notice shall be given in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Patrons: Bulova and Plum

STATUS: 01/10/08 House: Assigned S & T sub: #1

HB 554

Computer crimes; website redirection, penalty

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb554

Computer crimes; website redirection; penalty. Adds a Class 6 felony to the list of computer trespass crimes if a person, with malicious intent, intentionally alters the markup language or Uniform Resource Locator (URL) of a website so as to redirect a user from his intended URL or website destination to a third-party URL or website. *Patron: Griffith*

STATUS: 01/10/08 House: Referred to Committee for Courts of Justice

HB 633

Personal Information Privacy Act; prohibits dissemination of another's social security number

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb633

Personal Information Privacy Act; social security numbers. Prohibits the dissemination of another person's social security number, regardless of whether such number is obtained from a public or private record. Currently, the prohibition against dissemination only applies to social security numbers obtained from private sources. This bill is a recommendation of the Freedom of Information Advisory Council and the Joint Commission on Technology and Science. ***Patrons: May, Athey, Carrico, Cole, Cosgrove, Crockett-Stark, Gilbert, Lingamfelter, Massie, Merricks, Morgan, Poindexter, Rust and Sherwood***

STATUS: 01/17/08 House: Assigned GL sub: FOIA

HB 634

Government Data Collection and Dissemination Practices Act; disclosure of personal information

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb634

Government Data Collection and Dissemination Practices Act (GDCDPA); personal information; definition; collection of same; penalty for violation; jurisdiction of district courts. Provides that no agency shall require an individual to furnish or disclose his social security number (SSN) or driver's license number unless the furnishing or disclosure of such number is (i) expressly authorized by state or federal law and (ii) essential for the performance of that agency's duties. The bill also strengthens the remedies provisions of the GDCDPA by adding civil penalties matching those in FOIA, and grants general district courts the authority to hear GDCDPA cases. Additionally, the bill has enactment clauses giving it a delayed effective date of July 1, 2009, and requires state agencies to study their own collection and use of SSNs and report to the FOIA Council and JCOTS on such collection and use by October 1, 2008. The bill also contains a fourth enactment clause providing for the gathering of similar information about the use and collection of SSNs by cities, counties and towns with a population greater than 15,000. The bill is a recommendation of the Freedom of Information Advisory Council and JCOTS. *Patrons: May, Athey, Carrico, Cole, Cosgrove, Crockett-Stark, Hugo, Morgan, Rust and Sherwood*

STATUS: 01/08/08 House: Referred to Committee on General Laws

HB 971

Identity theft; database breach notification

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb971

Database breach notification. Requires a person or business that conducts business in Virginia and that owns or licenses computerized data that includes personal information to conduct a reasonable investigation to promptly determine the likelihood that personal information has been or will be misused when it becomes aware of an incident of unauthorized access to personal customer information. Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. The bill also contains alternative notification provisions. Any customer injured by a violation of this section may institute a civil action to recover actual damages or to enjoin any business that violates or has violated this section. ***Patron: Shannon***

STATUS: 01/29/08 House: Assigned S & T sub: #1

HB 1007

Fusion Intelligence Center; confidentiality, immunity

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1007

Virginia Fusion Intelligence Center; confidentiality; immunity. Provides that papers, evidence, information, etc., and databases or other information in the possession of the State Police are confidential and not subject to the Virginia Freedom of Information Act or the Government Data Collections and Disseminations Practices Act. The bill also provides that employees of the Department are not subject to subpoena in any civil action concerning criminal intelligence information or terrorism investigation. The bill restricts the release or dissemination of information without prior authorization from the Virginia Fusion Intelligence Center and punishes any person who knowingly disseminates information with a Class 1 misdemeanor. If such unauthorized release or dissemination results in death or serious bodily injury, such person is guilty of a Class 4 felony. *Patron: Jones, D.C.*

STATUS: 02/01/08 House: Referred to Committee on Appropriations

HB 1017

Telework Promotion and Broadband Assistance, Office of; established, report

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1017

Office of Telework Promotion and Broadband Assistance; codified; sunset. Codifies Executive Order 35 (2006) creating the Office of Telework Promotion and Broadband Assistance under the Secretary of Technology. The goals of the Office are to encourage telework as a family-friendly, business-friendly public policy that promotes workplace efficiency and reduces strain on transportation infrastructure. In conjunction with efforts to promote telework, the Office shall work with public and private entities to develop widespread access to broadband services. The provisions of this act expire on July 1, 2018. ***Patrons: Hugo, Carrico and Lingamfelter; Senator: Puckett***

Status: 01/17/08 House: Assigned GL sub: Professional/Occupational/Administrative Process

HB 1019

Telecommuting; state agencies to keep savings

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1019

Telecommuting; state agencies to keep savings. Authorizes state agencies to retain the unappropriated balance in the general appropriation act realized as a direct result of implementing a telecommuting program within the agency. *Patron: Hugo*

Status: 01/17/08 House: Assigned GL sub: Professional/Occupational/Administrative Process

HB 1052

Identity theft; notice of database breach

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1052

Database breach notification. Requires that an individual or a commercial entity that conducts business in Virginia and that owns or licenses data that includes personal information about a resident of Virginia shall, when it becomes aware of a breach of the security of the system, (i) conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and (ii) notify the Office of the Attorney General that a breach has occurred. A breach of the security of the system is defined as the unauthorized acquisition and access of unencrypted or unredacted data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Types of notification meeting the requirements of this bill are listed, but not required if, after a reasonable investigation, the person or commercial entity determines that there is no reasonable likelihood of harm to affected Virginia residents. The Attorney General may bring an action in law to address violations and ensure proper compliance with this section. Nothing in this section shall limit an individual from recovering direct economic damages resulting from a violation of this section. *Patron: Plum, Bulova and Scott, J.M.*

Status: 01/29/08 House: Assigned S & T sub: #1

HB 1087

Social security numbers; public access, exceptions

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1087

Public access to social security numbers; exceptions. Provides that the social security number of any individual contained in the public records of a local government shall be confidential and exempt from disclosure under the Freedom of Information Act. The bill provides, however, that a social security number may be released (i) in accordance with a proper judicial order; (ii) to any law-enforcement agency, officer, or authorized agent thereof acting in the performance of official law-enforcement duties; or (iii) to any data subject exercising his rights under the Government Data Collection and Dissemination Practices Act. *Patron: Sickles and Fredrick*

Status: 01/17/08 House: Assigned GL sub: FOIA

HB 1096

Protection of Social Security Numbers Act; created

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1096

Protection of Social Security Numbers Act; penalties. Creates the Protection of Social Security Numbers Act, which prohibits every agency from releasing those portions of a public record that contain the social security number of any individual. The bill contains several exemptions from this general rule and also allows disclosure of the last four digits of a social security number to certain entities for the purpose of verifying identity. The bill provides for penalties for violation and contains technical amendments. *Patron: Sickles*

Status: 01/17/08 House: Assigned GL sub: FOIA

HB 1311

Credit reports; authorizes consumer to freeze access thereto

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1311

Freezing access to credit reports. Authorizes any consumer to freeze access to his credit report. If a consumer has placed a freeze on his credit report, a consumer reporting agency is prohibited from releasing the credit report, or any information in it, without the consumer's express authorization. The measure provides a means by which a consumer can release his report, permanently, temporarily, or to a specific third party. Certain disclosures are exempt from the freeze. A fee of up to $10 may be charged for establishing or lifting a freeze, except identity theft victims are not required to pay a fee except for a temporary lifting of the freeze within 15 minutes of receipt of certain electronic requests. A person who willfully fails to comply with the requirements is liable to a consumer for actual damages of between $100 and $1,000, punitive damages, and reasonable attorney fees. A person who negligently fails to comply with the requirements is liable to a consumer for actual damages and reasonable attorney fees. *Patron: Byron*

Status: 02/01/08 House: Engrossed by House - committee substitute HB1311H1

HB 1469

Identity theft; notice of database breach

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb1469

Database breach notification. Requires an individual or entity that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery or notification of the breach to any resident of the Commonwealth whose unencrypted and unredacted personal information was, or is reasonably believed to have been accessed and acquired by an unauthorized person. A breach is defined as the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Violations by a state-charted or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator. All other violations shall be enforced by the Office of the Attorney General, which may obtain either actual damages or a civil penalty not to exceed $150,000 per breach or series of breaches of a similar nature that are discovered in a single investigation. *Patron: Byron*

Status: 01/29/08 House: Assigned S & T sub: #1

SB 336

Temporary detention orders; encryption of medical records not required

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=sb336

Temporary detention orders; encryption of medical records not required. Provides that a health care provider or designee of a local community services board or behavioral health authority shall not be required to encrypt any email containing information or medical records provided to a magistrate unless there is reason to believe that a third party will attempt to intercept the email. ***Patron: Cuccinelli***

Status: 01/31/08 Senate: Communicated to House

SB 492

Vital Records, Office of, et al.; development of alternative verification system

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=sb492

Real ID; alternative verification system. Requires the Department of Health's Office of Vital Records, along with the Department of Motor Vehicles and other appropriate state and local agencies, to develop and implement a plan to provide Virginia resident verification, as an alternative to the requirements of the federal Real ID Act of 2005. The measure specifies that Virginia shall not comply with the unfunded mandates of the Real ID Act. *Patron: Hanger*

Status: 01/16/08 Senate: Rereferred to Transportation

SB 576

Credit reports; authorizes consumer to freeze access thereto

http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=sb576

Freezing access to credit reports. Authorizes any consumer to freeze access to his credit report. If a consumer has placed a freeze on his credit report, a consumer reporting agency is prohibited from releasing the credit report, or any information in it, without the consumer's express authorization. The measure provides a means by which a consumer can release his report, permanently, temporarily, or to a specific third party. Certain disclosures are exempt from the freeze. A fee of up to $10 may be charged for establishing or lifting a freeze, except identity theft victims are not required to pay a fee except for a temporary lifting of the freeze within 15 minutes of receipt of certain electronic requests. A person who willfully fails to comply with the requirements is liable to a consumer for actual damages of between $100 and $1,000, punitive damages, and reasonable attorney fees. A person who negligently fails to comply with the requirements is liable to a consumer for actual damages and reasonable attorney fees. *Patrons: Saslaw, Howell, Lucas, McDougle, McEachin, Miller, Y.B., Puller, Quayle and Reynolds; Delegate: Byron*

Status: 01/29/08 Senate: Assigned C&L sub: Financial Institutions & Insurance

QUESTIONS?

Upcoming Events

UPCOMING EVENT!

Cyber Security Webcast - February 14 2:00 - 3:00 p.m.

The National Cyber Security Division and the Multi-State Information Sharing and Analysis Center invite you to participate in the next session of the National Webcast Initiative: ~ Emerging Trends for 2008 ~ "This webcast will provide a broad look at some of the major issues and challenges we face regarding cyber security threats. Current and emerging trends will be discussed, including botnets, online scams, identity theft, cyber crime and more. The presentation will include practical, timely advice on what can be done --in both the public and private sectors-to mitigate the risks and enhance our protection against these threats.

Don't Miss Out -- Register Now to Save Your Seat!"
http://www.msisac.org/webcast/2008-02/

UPCOMING EVENTS!

Tuesday, February 19, 12:00 - 2:00 p.m. IS Council Meeting with committee meetings from 2:00 – 3:00 CESC

To register email VITASecurityService@VITA.Virginia.gov

Thursday, February 21, 3:00 – 5:00 p.m. ISO Orientation CESC
ISO orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV IT Security Policy and Standards and is open to all Commonwealth ISO's and interested IT persons!

- To register email VITASecurityService@VITA.Virginia.gov

Tuesday, February 26, 8:30 – 11:00 a.m. - AITR Meeting CESC

UPCOMING EVENTS!

March 3-8 2008 - SANS at Virginia Tech

These classes are available to state and local government employees including state and local law enforcement at a substantial discount. The registration URL is http://www.cpe.vt.edu/isect.

The price is $700/person for the entire event. Topics include: PCI Compliance, Advanced Network Worm and Bot Analysis, Windows Command-Line Kung Fu In-Depth and Reverse-Engineering Malware. Many thanks to Randy Marchany, Va Tech IT Security Lab Director for letting us know about this opportunity!

UPCOMING EVENTS!

March 10 - 15 2008 - SANS at the Association of College and University Auditors (ACUA) in Jacksonville, Florida

AUDIT 507: Auditing Networks, Perimeters & Systems; is a six-day course and begins with a high-level introduction on methods and assessment programs. Five of the six days in the course will include hands-on exercises with the demonstrated tools on a live in-class network. Each student is required to bring their own laptop to class which will allow you to experiment with the tools discussed in class and to actually perform review functions against SANS-provided servers in class.

The class offers 36 CPE at a significantly reduced rate of $1,500 for the entire event. GIAC Certification is available for an additional charge. The class is being held at the Hyatt Regency Riverfront hotel in the heart of the downtown business, entertainment, and sports district. . For more information and to register, visit: http://www.acua.org/go/events-and-seminars/sans-institute

UPCOMING EVENTS!

NEXT ISOAG MEETING

Wednesday, March 19 1:00 – 4:00

@ CESC Unless We Receive an Offer of Another Venue!

Draft Agenda:

Web Initiatives – Judy Napier, SoTech

FRAC Cards – Mike McCallister, OCP

CAM & APM – Debbie Secor & Mike Melton, VITA

CMT Demo – Benny Ambler, VITA

2.2-2009 Report Update – Cathie Brown, VITA

Web App Hacking Demo – Tripp Sims, VITA

Legislation – Peggy Ward, VITA

Any Other Business ??????

ADJOURN

THANK YOU FOR ATTENDING!!