Virginia Information Technologies Agency

Commonwealth Information Security Advisory Group (ISOAG) Meeting

February 15, 2007

Virginia Information Technologies Agency

ISOAG February 2007 Agenda

I.	Welcome	Peggy Ward, VITA
II.	Encryption Solution Ordering Status	John Kissel, VITA
III.	Executive Order 44 - Establishing Preparedness Initiatives in state Government	Constance McGeorge, OCP
IV.	VITA COOP	Cathie Brown, VITA
V.	VITA IT Disaster Recovery	Fred Duball, VITA
VI.	IT Legislation	Peggy Ward, VITA
VII.	MOAT (Security Awareness)	Rick Shaw
VIII.	Information Security Assurance Plan	Cathie Brown, VITA
IX.	Other Business	Peggy Ward, VITA

Welcome!!!

Information Risk Executive Council (IREC) – based on your feedback we purchased a Commonwealth membership that enables all Commonwealth employees with an interest to utilize IREC.

Name your ISO – Please note that the IT Security Policy states Agency Heads need to designate via e-mail to VITASecurityServices@vita.virginia.gov an ISO for the Agency and providing the person's name, title and contact information to VITA no less than biennially. The Agency Head is strongly encouraged to designate at least one backup for the ISO, as well.

IT Security Audit Plans

63 Agencies have submitted adequate plans or received an extension

54 Agencies have neither submitted a plan nor a request for an extension.

Updates sent to the Secretary of Technology weekly.

IT Partnership Audits

The following 8 agencies will have an Information Technology Security Audit performed on it's primary infrastructure by Deloitte – Touche through the IT Partnership with Northrop Grumman:

Department of Juvenile Justice
Department of Corrections
Department of Motor Vehicles
Department of Social Services
Department of Taxation
Department of Transportation
Virginia Department of Health
Virginia Information Technologies Agency

25 Agencies included in the NG SAS 70

1. Compensation Board
2. Department of Accounts
3. Department of Alcoholic Beverage Control
4. Department of Corrections
5. Department of Education
6. Department of Fire Programs
7. Department of General Services
8. Department of Health Professions
9. Department of Human Resource Management
10. Department of Juvenile Justice
11. Department of Mental Health, Mental Retardation & Substance Abuse Services
12. Department of Military Affairs
13. Department of Motor Vehicles
14. Department of Planning and Budget
15. Department of Rail and Public Transportation
16. Department of Rehabilitative Services
17. Department of Social Services
18. Department of Taxation
19. Department of Transportation
20. Department of the Treasury
21. Department of Veteran's Services
22. State Board of Elections
23. Virginia Department of Health
24. Virginia Employment Commission
25. Virginia Museum of Fine Arts

Guardian Edge - Encryption Plus

John Kissel

Agency Performance Manger

February 15, 2007

INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Implementation of Executive Order 44

Constance McGeorge
Information Security Officers Meeting
February 15, 2007

Office of Commonwealth Preparedness

Executive Order 44: Establishing Preparedness Initiatives

-Based on Governor's Priorities and 2006 Agency Preparedness Assessment

-Initiatives Coordinated through Agencies' Emergency Coordinator Officers

- Preparedness as Core Component of each Agencies Mission
- Preparedness as Part of Agencies Strategic Planning and Performance Measurement Process

Executive Order 44: Establishing Preparedness Initiatives

- Emphasis on Training and Updating Plans
- Annual Preparedness Assessment
- Governor’s Preparedness Certification Program

Executive Order 44: Uniformity, Review, and Testing of COOP

- Create and update COOPs utilizing VDEM's template (VDEM's 9/20/06 ISO Presentation)
- Utilize VDEM COOP resources available at http://www.vaemergency.com/library/coop
- Submit Updated COOPs to VDEM by April 1 of each year (through submission

Executive Order 44: Next Steps

- Agency heads designate ECOs
- OCP and VDEM provide guidance to ECOs regarding:
  - -Training Opportunities
  - -Grounds for Extensions
  - -Resolution of other COOP issues

Questions?

Virginia Information Technologies Agency

VITA COOP PLANNING

Cathie Brown, CISM, CISSP

ISOAG Meeting

February 15, 2007

expect the best

History of Planning Efforts

- SunGard contract since 1994 for MVS mainframe & 1996 for Unisys mainframe
- Special Team did Y2K Planning & Preparations
- Current SunGard contract signed in 2000 covers both MVS & Unisys mainframes, the VITA Central network & Windows & Unix servers as required
- Emergency Response Procedures developed in late 2001 (became a part of the COOP plan)
  - Names an Emergency Management Team to act at time of disaster (Executive Team)
  - Defines Authority to implement as well as Succession of Authority
  - Documents the steps in Activating an Emergency Response

Data Center Recovery

- VITA Infrastructure to include mainframes, network, routers, switches, etc.
- Agency-specific hardware if covered on the SunGard contract
- Operating systems recovered so that agencies can restore applications supporting essential business functions
- 72 Hour Recovery

Data Center Recovery (continued)

- Recovery Procedures developed for all essential functions
- Procedures include hardware, software and personnel resource requirements
- Procedures are reviewed and updated quarterly
- BIA reviewed and updated annually (June)
- Desktop exercises conducted annually (last done in November 2005)
- Exercise of data center recovery conducted at SunGard annually (last done in April 2006)

SunGard Contract Coverage

- Richmond Plaza Building Data Center
- VITA agency locations that have determined the need for SunGard backup
  - VDOT – Central Office
  - DPOR – applications at its location
  - SBE – email servers
  - DRS – one server
  - DSS – one server
- Agency-specific hardware in the RPB Data Center
  - DSS – Primepower 1500 (E10000)
  - TAX – Servers for iFile & IRMS
  - SCC - router
  - DMV - routers
  - DMAS – router
- RPB Data Center and agency specific hardware currently covered under the SunGard Contract will have disaster recovery coverage at SWESC

SunGard Contract Coverage (continued)

- VITA pays SunGard $210,304 monthly of which agency-specific costs are $51,141

- Modified quarterly if needed to assure current hardware configurations are available

Disaster Declaration at SunGard

- Decision made collaboratively by VITA and Northrop Grumman
- Disaster Declared using SunGard established procedures by VITA designees
- Declaration Fees - $75,000 for MVS; $20,000 for Unisys; $20,000 for E10000; $2,500 for Server Group
- Daily Usage Fees – $45,000 for MVS; $5,000 for Unisys; $5,000 for E10000; Server Group – no usage fee for 1st 30 days

Backup Generators

- Contract with Carter Machinery
  - Provides for 2 diesel generators within 6 hours of notification to be hooked at RPB
    - Provide power to run the VITA data center (raised floor only) and one HVAC and cooling tower for chilling the water required by the system
  - Provides for a supply of fuel for as long as the generators are needed by VITA
  - Monthly fee - $9,000
  - Activation fee - $17,679 (minimum 1 day) - $76,890 (maximum for 5 days)

Current COOP Planning Efforts

Objective: Develop a detailed written plan to complete a VITA Enterprise COOP in accordance with existing VDEM standards and guidelines.

- VITA COOP Team has been formed and meets on a bi-weekly basis.
- IT DR component of agency COOP plans will be included into the VITA IT Recovery plan.
- Plans to be based on regions as advocated by the Office of Commonwealth Preparedness & VDEM
- Executive Order 44 issued

Coop Planning Efforts

- Outreach to Customer Locations
  - IT DR Component of agency COOP plans
  - VITA needs to understand the current level of effort for agency IT DR needs at the time of integration into VITA
  - This is the level of support VITA is able to provide unless additional plans and funding have been put into place

QUESTIONS

Commonwealth Information Security Officers Meeting

Fred Duball

February 15, 2006

INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Commonwealth Enterprise Solutions Center

Meadowville Technology Park
Chesterfield County, Virginia

New Facilities / Data Centers & Disaster Recovery Solutions

- Commonwealth Enterprise Solutions Center (CESC)
  - Meadowville Technology Park, Chesterfield County, Va.
- Southwest Enterprise Solutions Center (SWESC)
  - Russell Regional Business/Technology Park, Russell County, Va.
  - Future Disaster Recovery Solutions for the Commonwealth

CESC Facility – available June 2007

- Target size of facility 192,000 S.F.
- Data center (TIER III) 50,000 S.F.
- CMOC, NOC, SOC, Technology Lab 7,000 S.F.
- Office Area 80,000 S.F.
- Common Areas 30,000 S.F.
  - Multi-purpose room (three partitioned areas / seats 260)
  - Training room (two partitioned areas / seats 40)
  - Video Teleconference / TV Production room / seats 24

CESC Benefits to Commonwealth of Virginia, Customer Agencies and VITA

- High availability via construction of Tier III Data Center; N+1 infrastructure
- High critical systems availability / visibility from new centralized management tools
  - Customer dashboard
  - Peregrine problem management
  - HP Openview workload monitoring and management
- Lower costs / high efficiencies through consolidation
- Centralized Management Operations Center
  - Consolidated operations
  - Network monitoring and management (NOC)
  - Security Management and Monitoring (SOC)

CESC Benefits cont.

- Home for new Commonwealth wide solutions
  - Consolidated state wide network
  - Consolidated messaging
  - Consolidated security system
- Home for agency critical systems
  - High availability / lower risk
  - Cost efficient Management
  - Customer visibility of workload
- More cost effective for disaster recovery
  - Planning and testing

Southwest Enterprise Solutions Center

Russell Regional Business Technology Park
Russell County, Virginia

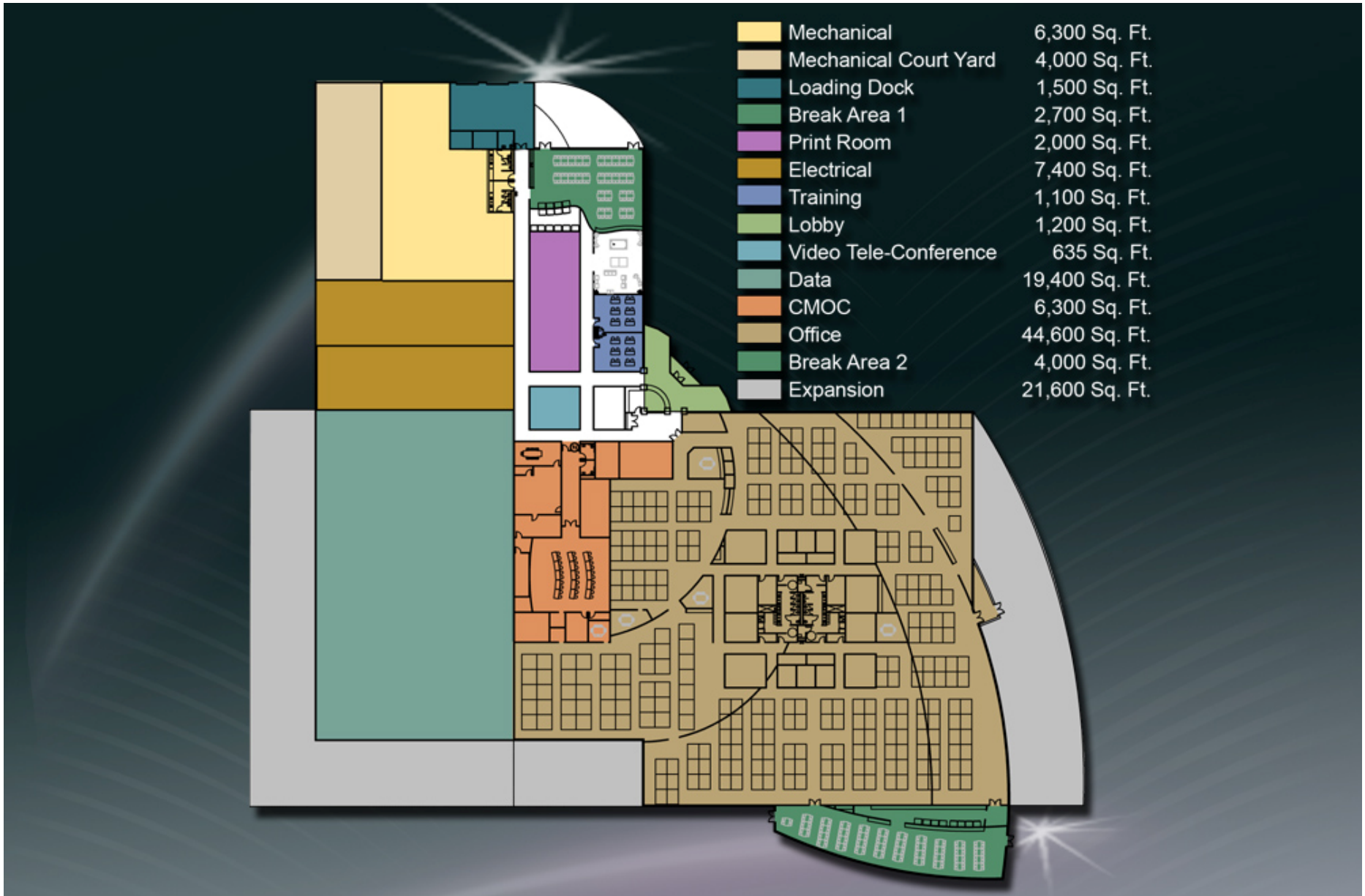
New Facilities & Disaster Recovery Solutions

New Facilities & Disaster Recovery Solutions

SWESC Facility

- Supports Economic Development of Southwest Region
  - New Facility
  - 300 + New Technology Jobs
  - Cornerstone for Technology Growth in Southwest Region

New Facilities & Disaster Recovery Solutions



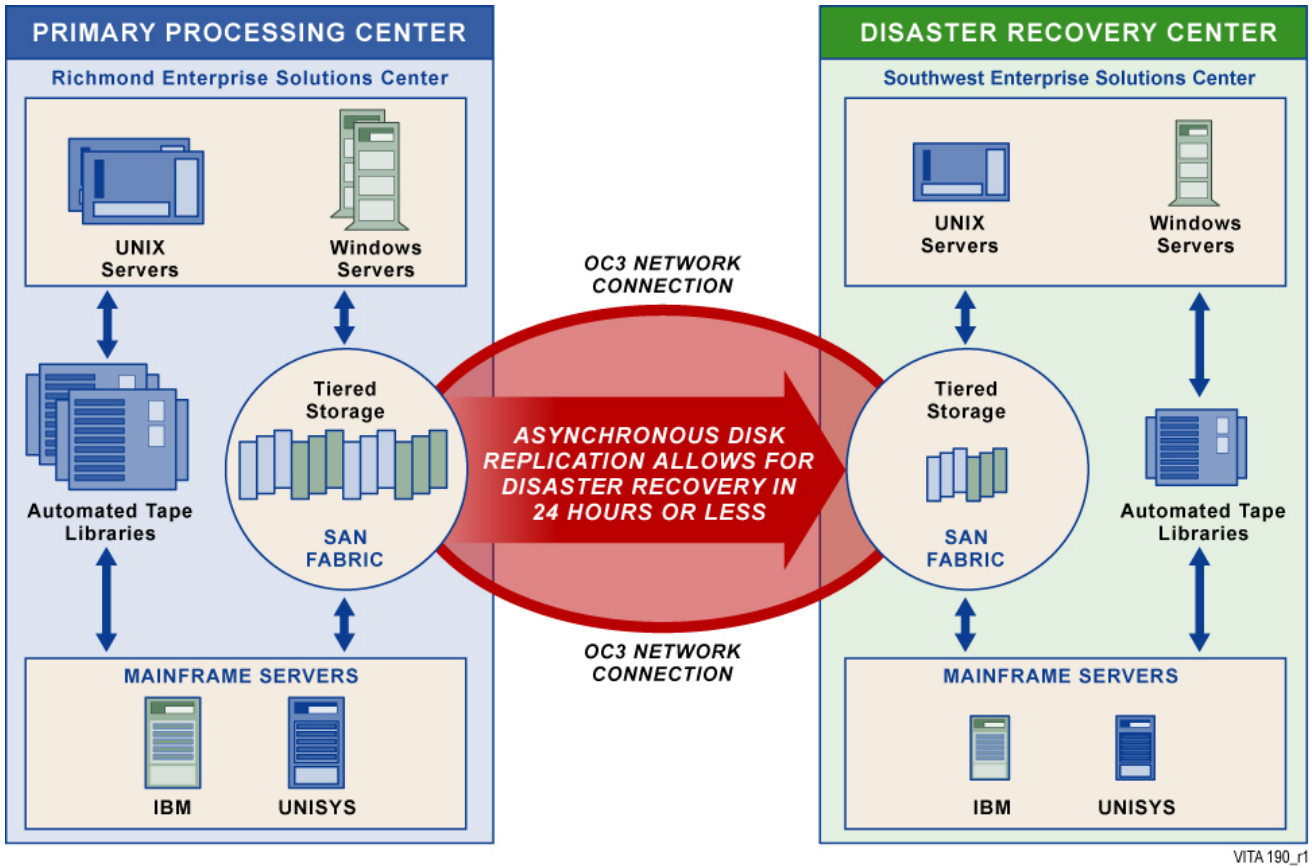
SWESC Facility – available Oct. 2007

- **Size of facility** **101,000 S.F.**
- **Data center (TIER II+)** **20,000 S.F.**
  - **Disaster Recovery Center for Commonwealth**
  - **Failover Messaging System**
- **Office area** **48,000 S.F.**
  - **Primary Help Desk / Call Center**
  - **Backup Consolidated Management Operations Center**
- **Common Areas** **10,000 S.F.**
  - **VTC**
  - **Training Room (seats 24)**
  - **Executive Conference Room**

SWESC Disaster Recovery Solutions

- **SWESC VITA Infrastructure Support**
  - **Messaging failover at SWESC for continued service**
  - **Back-up CMOC / NOC / SOC in place for continued operations**
  - **Primary help desk at SWESC for continued service**
- **For all customers currently processing at RPB & on SunGard Contract:**
  - **Disaster Recovery at SWESC**
  - **Hardware / Software / Network in place at SWESC for fast recovery**
  - **Data Replication and recovery within 24 hours (vs current 72 hrs)**
  - **Test at customer convenience (not locked into SunGard)**

SWESC Disaster Recovery Solution Overview



Key SWESC Benefits

- **Reduced Disaster Recovery time using DASD & tape storage replication**
  - SunGard (72 hour recovery) vs. SWESC (< 24 hour recovery)
- **Capability to schedule an individual agency DR test at any time, no time restrictions**
- **SWESC on the same Commonwealth network as CESC production equipment**
  - Allows capability of failover of individual servers & applications
- **For new Customers - Quick startup of a Disaster Recovery capability**
  - Existing network, equipment, facilities, staff and solutions and contract
- **Accommodates Mainframes, UNIX & Wintel servers**
  - As equipment is installed in the CESC during the transition, RPB equipment will be relocated to the SWESC and installed into configurations that are compatible with and materially backup the CESC production environment
  - CESC equipment installed to support new customer needs will be replicated in SWESC
  - Preconfigured hardware & network equipment updated to support CESC changes

Future Capabilities

- **Infrastructure will support full spectrum of Back-up and DR Solutions**
  - **Hot, Warm, Cold and Quick Ship Options Available from - Automatic Failover to on site system restore available**
  - **Backup DASD & Tape storage, replication and management services**
  - **Remote TAPE creation, vaulting and storage services**
  - **Operation from alternate locations – SWESC or other Commonwealth locations**
- **Environment in place for new customers (not on SunGard Contract) — Requires Funding for:**
  - **Business Impact Analysis (BIA)**
  - **Disaster Recovery Requirements Analysis**
  - **Solution development, implementation and testing**
  - **Performance of periodic test**

Future Service Offerings

- Review typical common DR and Back-up Requirements
- Develop standard offerings and methodology for BIA and services
- Expect refinement and definition of offerings over the next 9 months

Virginia Information Technologies Agency

2007 General Assembly Session

IT Legislation Update

Peggy Ward

HB1603 – Substitute!

Multiline telephone systems; owner or operator thereof ability to identify location from 9-1-1 call.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB1603

Multiline telephone systems. Requires owners or operators of multiline telephone systems serving residential facilities, hotels and motels, business locations, and educational institutions to ensure that a public safety answering point is able to identify the location from which a call to 9-1-1 is placed. *Patrons:* Rapp, O'Bannon and Orrock

STATUS: Passed House; in Senate Commerce and Labor

HB 1885

Voice-over-Internet protocol service; revises definition.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB1885

Voice-over-Internet protocol service. Revises the definition of Voice-over-Internet protocol service to eliminate references to the public switched telephone network and a requirement for the use of Internet protocol-compatible customer premises equipment. Providers of Voice-over-Internet protocol service are exempt from regulation by the State Corporation Commission. *Patron:* Marshall, R.G.

STATUS: Passed House; in Senate Commerce and Labor

HB 2140/SB 1244 – TABLED!

Identity theft; notification of breach of information system.
http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2140
http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1224

Database breach notification. Requires an individual or a commercial entity that conducts business in Virginia and that owns or licenses computerized data that includes personal information to conduct in good faith a reasonable and prompt investigation when it becomes aware of a breach of the security of the system. If the investigation determines that misuse of information has or is reasonably likely to occur, the individual or commercial entity shall give notice to the Virginia resident as soon as possible. Notification must be made in good faith, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. The bill also contains alternative notification provisions. The Office of the Attorney General may bring an action in law or equity to address violations of this section and other appropriate relief. The provisions of this bill, as they apply to governmental entities, become effective July 1, 2008. *House Patron: Brink Senate Patron: Howell*

STATUS: HB 2140 Tabled in House Commerce and Labor
SB 1244 Left in Senate Courts of Justice

HB 2196

Chief Information Officer; powers and duties.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2196

Powers of the CIO. Gives the CIO of the Commonwealth the power to enter into contracts with one or more other public bodies, or public agencies or institutions or localities of the several states, of the United States or its territories, or the District of Columbia for the provision of information technology services. *Patron:* Nixon

STATUS: Passed House and Senate

HB 2198

HB 2198 Electronic health records; requires those purchased by state agency to adhere to accepted standard.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2198

Electronic health records. Requires any electronic health records system or software purchased by a state agency to adhere to accepted standards for interoperability or to be certified by a recognized certification body. *Patron:* Nixon

Passed House: Passed Senate with Amendments

HB 2306/SB 1342

Public institutions of higher education; operational authority.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2306

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1342

Public institutions of higher education; operational authority. Provides operational authority for public institutions of higher education in the areas of information technology and procurement pursuant to the Restructuring Act of 2005. *House Patron:* Callahan *Senate Patron:* Houck

STATUS: HB2306 Left in Appropriations;
SB1342 Passed Senate; Referred to House Appropriations

HB 2870 – TABLED!

Cellular telephones; encouraged to program with ICE numbers

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2870

Programming cell phones with ICE numbers. Requires providers of commercial mobile telecommunications service to implement a program, in accordance with criteria developed by the Wireless E-911 Services Board, of encouraging its subscribers to program one or more ICE numbers into their mobile telephones. An ICE number is a telephone number that is programmed into a mobile telephone, and labeled ICE, which when called by a firefighter, paramedic, emergency medical technician, rescue worker, or ambulance when the subscriber is nonresponsive or impaired, will connect to the person who the subscriber desires to be contacted in case of an emergency. *Patron:* McEachin

STATUS: Tabled in Science and Technology

HB 2946

Chief Information Officer; powers and duties.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2946

Powers of the CIO; information technology recycling. Requires the CIO to contemporaneously account, to the greatest extent possible, for the recycling and disposal of information technology investments when developing policies and procedures for the procurement of such investments. *Patrons:* Plum and Nixon

STATUS: Passed House and Senate

HB 2973 – TABLED!

Unsolicited bulk electronic messages; changes scope of State's spam law

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2973

Unsolicited Bulk Electronic Messages; cell phone spam; penalty. Changes the scope of Virginia's spam law from electronic mail to electronic messages by defining electronic message as any text, image, or other communication transmitted to a computer. The bill also adds wireless communications devices to the type of devices defined as computers. The bill reduces the number of messages necessary for a person to meet the requirements of this section to 2,500 attempted recipients in any 24-hour period, 25,000 attempted recipients in any 30-day time period, or 250,000 attempted recipients in any one-year time period. Additionally a new provision would make sending unsolicited bulk electronic messages a Class 6 felony if a single recipient of an electronic message or multiple electronic messages incurs damages in excess of $250 during any one year time period. *Patron:* Bell

STATUS: Tabled in Science and Technology

HB 3148 – TABLED!

Compromised Data Disclosure Act; created

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB3148

Compromised Data Disclosure Act. Creates the Compromised Data Disclosure Act, which requires state agencies to notify residents of Virginia when their personal information maintained by a state agency has been compromised through a breach of a security system or otherwise acquired by an unauthorized person. The bill requires the Virginia Information Technology Investment Board to establish policies and procedures to implement the provisions of the bill. The bill defines personal information. *Patron:* Bulova Sickles

STATUS: Tabled in House Science and Technology

SB 845

State agencies; Chief Information Officer to develop policies, etc. relating to security data.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB845

Security of confidential state data. Requires the Chief Information Officer of the Commonwealth to develop policies, procedures, and standards relating to the security data maintained and used by state agencies. The policies, procedures, and standards must include requirements that a user be required to provide a password or other means of authentication to access a computer and to access a state-owned or operated computer network or database through the computer, and that a digital rights management system be used to control access to electronic records containing confidential information. *Patron:* Devolites Davis

STATUS: Passed Senate; in House General Laws

SB 1004 – SUBSTITUTE!

Telecommuting; use of personal computers.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1004

Telecommuting; use of personal computers. Authorizes a state agency to allow employees to use computer equipment not owned or leased by the Commonwealth to telecommute, so long as such equipment is not used to access or store data made confidential by state or federal law. The bill contains an emergency clause. *Patron:* Devolites Davis

STATUS: Passed Senate; in House Science and Technology

SB 1029 – SUBSTITUTE!

Chief Information Officer; to incorporate computer security into 4-year strategic plan.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1029

Powers of the Chief Information Officer (CIO); information security. Requires the CIO of the Commonwealth to monitor trends in information security and incorporate computer security into the four-year strategic plan for information technology. *Patron:* O'Brien

STATUS: Passed Senate; in House General Laws

SB 1111

Freedom of Information Act; closed meetings and security of public buildings.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1111

Freedom of Information Act; closed meetings; security of public buildings. Adds a closed meeting exemption for the discussion of reports or plans related to the security of any governmental facility, building or structure, or the safety of persons using such facility, building or structure.

Patron: Houck

STATUS: Passed Senate; in House General Laws

SB 1123

Auditor of Public Accounts; review security governmental databases containing personal information.

http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+SB1123

Freedom of Information Act; closed meetings; security of public buildings. Provides that the Auditor of Public Accounts shall periodically review the security of any database or information system maintained or operated by any agency or other governmental entity of the Commonwealth that contains personal information regarding any individual to ensure that appropriate measures are in place to prevent unauthorized or unlawful access to this information. On an annual basis, the Auditor shall report the results of its review to the General Assembly and make recommendations for new or revised security measures, if needed. *Patron:* Cuccinelli

STATUS: Passed Senate; in House Science and Technology

Awareity, Inc.

21st Century Tools for 21st Century Challenges

Rick Shaw – President, CEO

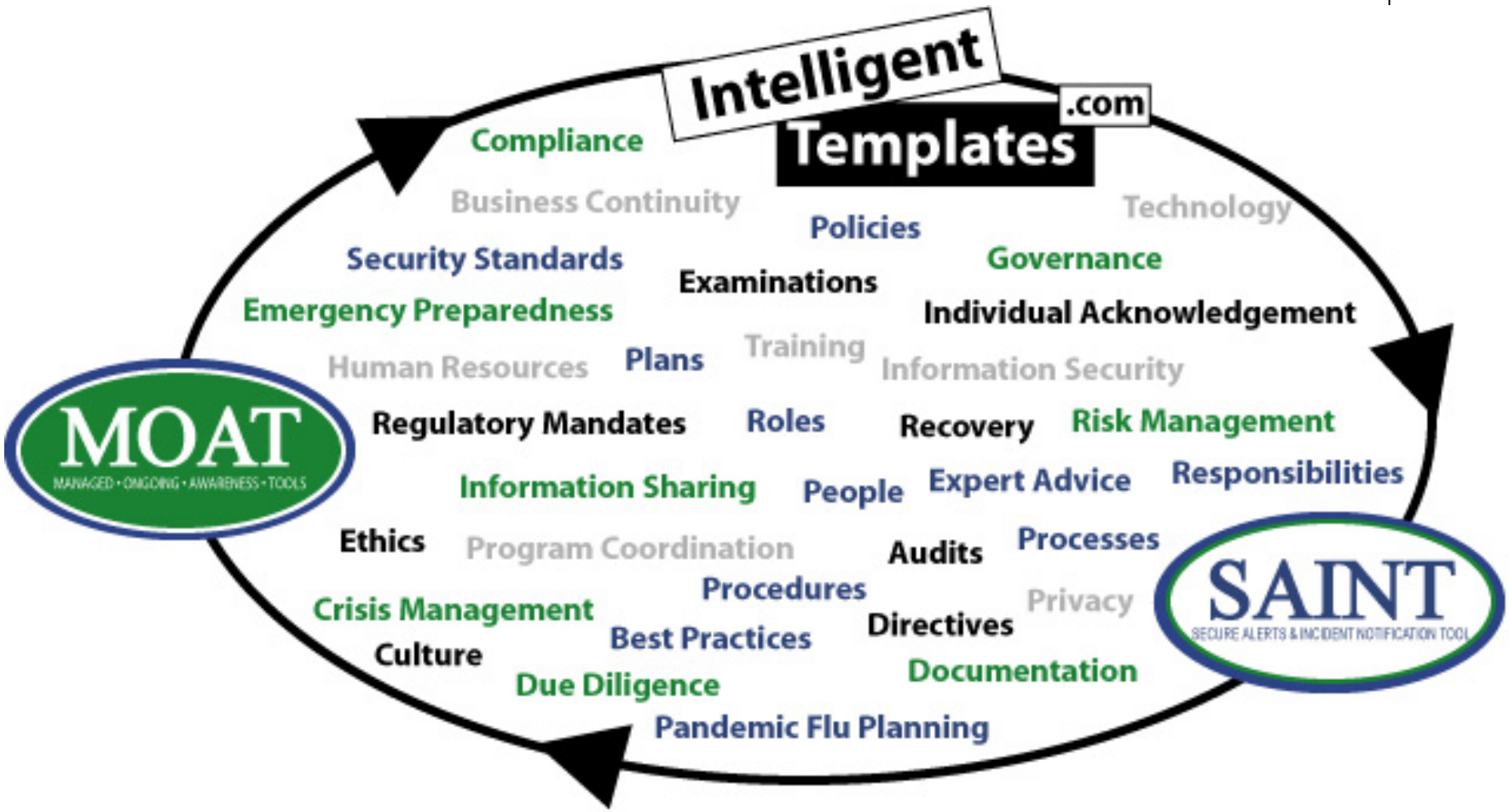
AWAREITY

What Awareity Offers?

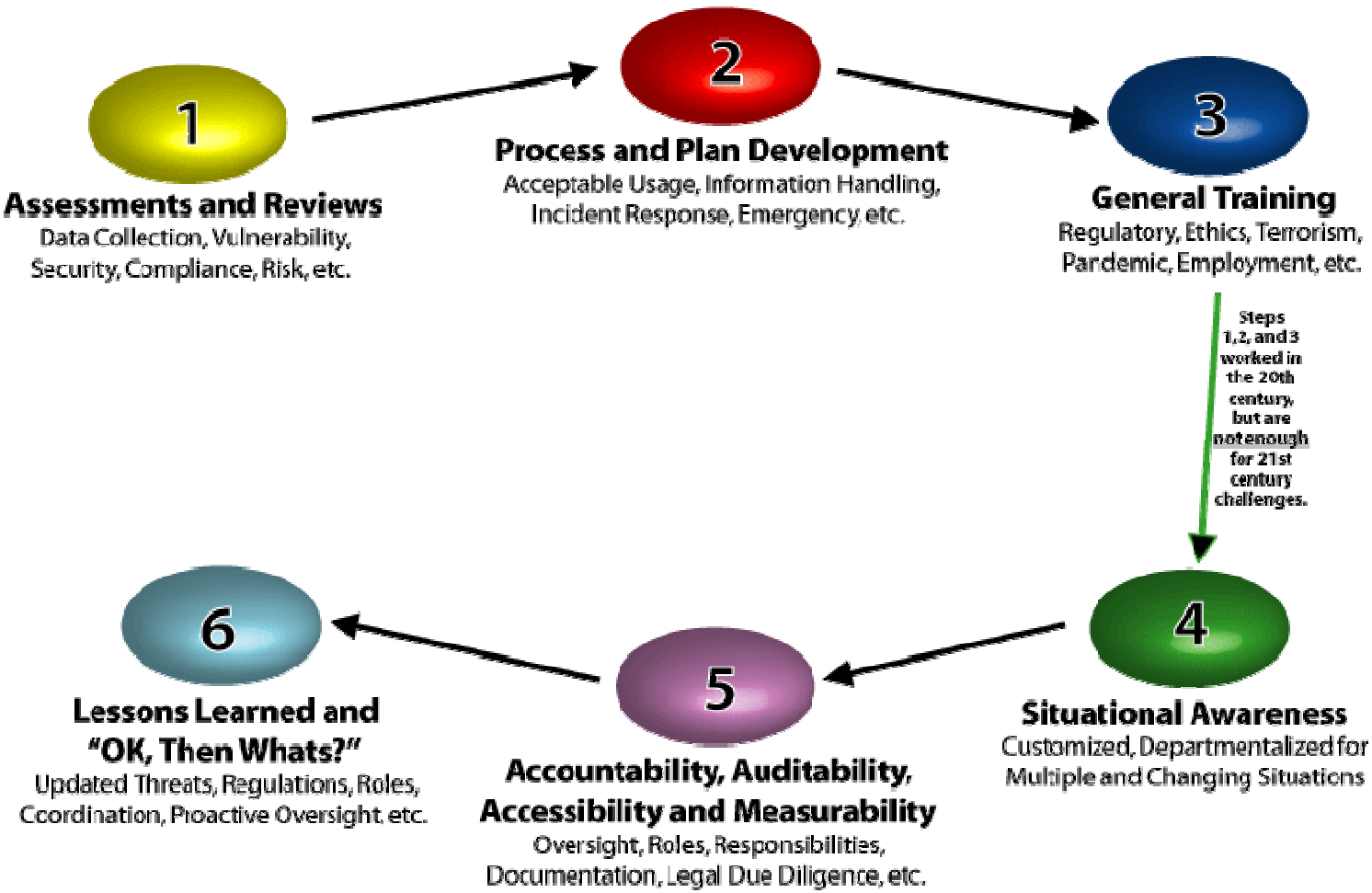
- 21st Century Tools for:
  - Automating Compliance & Governance Requirements
  - Enhancing Business Continuity & Coordination
  - Pandemic Flu & Emergency Preparedness Planning
  - Strengthening Information Security & Privacy Obligations
  - Protecting Reputation & Client Trust
  - Preventing Lawsuits & Ensuring Due Diligence
  - Connecting-the-Dots across People, Processes & Technology and across multiple organizations
  - Improving and Protecting the BOTTOM LINE
- Awareity's SaaS that most every organization needs

  (SaaS stands for Software-as-a-Service)

Awareity's SaaS Solutions

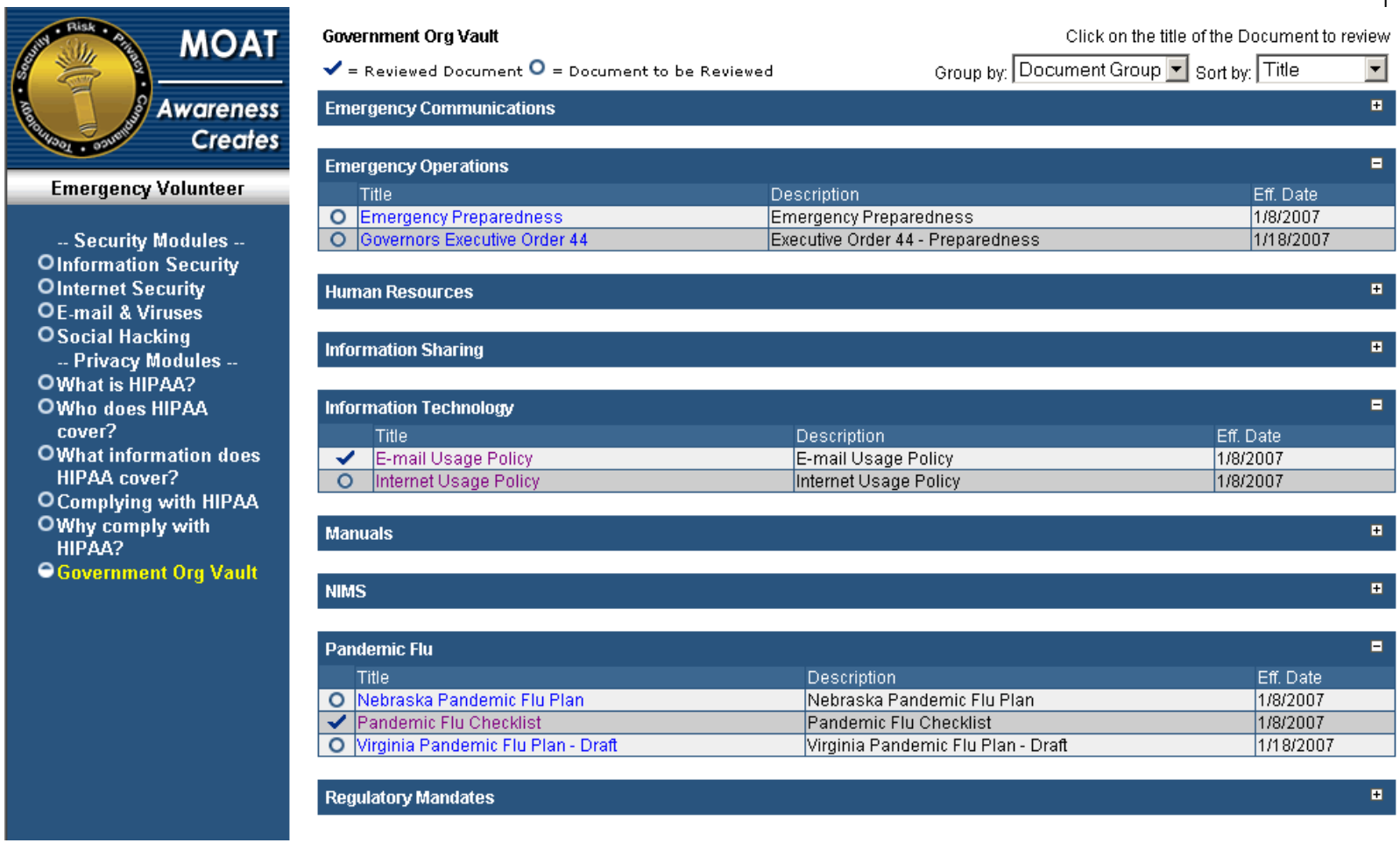


21st Century Steps to Preparedness



AWAREITY

MOAT – Managed Ongoing Awareness Tools



Executive Order 43 – Security of Sensitive Individual Information

- Effective Date was January 9, 2007
- Important Initiative and Growing Concerns
- Identity Theft is Increasingly Common Crime
- High Profile Security Breaches
- Commonwealth Information Security Policies
- Sensitive Individual Information Standards
- Ensuring Compliance and Accountability
- Ongoing Reporting by Secretary of Technology

Security Awareness is Critical

- People are the focus of sophisticated threats
  - Phishing, Spear Phishing & Pharming
  - Social Networking & Curiosity
  - Keyloggers and Spyware
- Processes are just as important as Technology
  - Information Handling (laptops, desk tops, etc.)
  - Information Sharing (vendors, users, responders, etc.)
- Connecting the Dots eliminates gaps
- Physical, Cyber, Home, Wireless, etc.
- Regulations, Executive Orders, etc.
- Situational Awareness and Anti-Virus Software

Security Awareness is Critical

Information Disposal

Information handling and information sharing have created new and significant challenges for organizations of all sizes.

Information disposal is a challenge for electronic and non-electronic information. For example, just throwing out a PC, PDA, or CD in the trash can is not a good way to dispose of devices that may contain information.

Before throwing away or selling an organizational or personal PC, PDA, or CD (or other electronic devices), just deleting all files and emptying the recycle bin on your PC is not good enough. If you are attempting to dispose of electronic information be sure you use the proper tools and specialized software that will write multiple layers of random data over the top of the sensitive information so it cannot be easily recovered when, or if, others gain access to the PC, PDA, CD, or other electronic device.

The most popular information disposal method for non-electronic information is shredding. When shredding hardcopy documents, crosscut shredders are usually considered to be more effective than strip cut shredders because strips of papers can be more easily pieced together.

Always check your organization's policy for Information Disposal guidelines to ensure that electronic information and non-electronic information are discarded properly and safely.

Awareness Validation

Question/Statement:

Accessing and protecting your sensitive and personal information is as much about how people handle, share, discard and store information as it is about the technology in place.

Select the best answer:

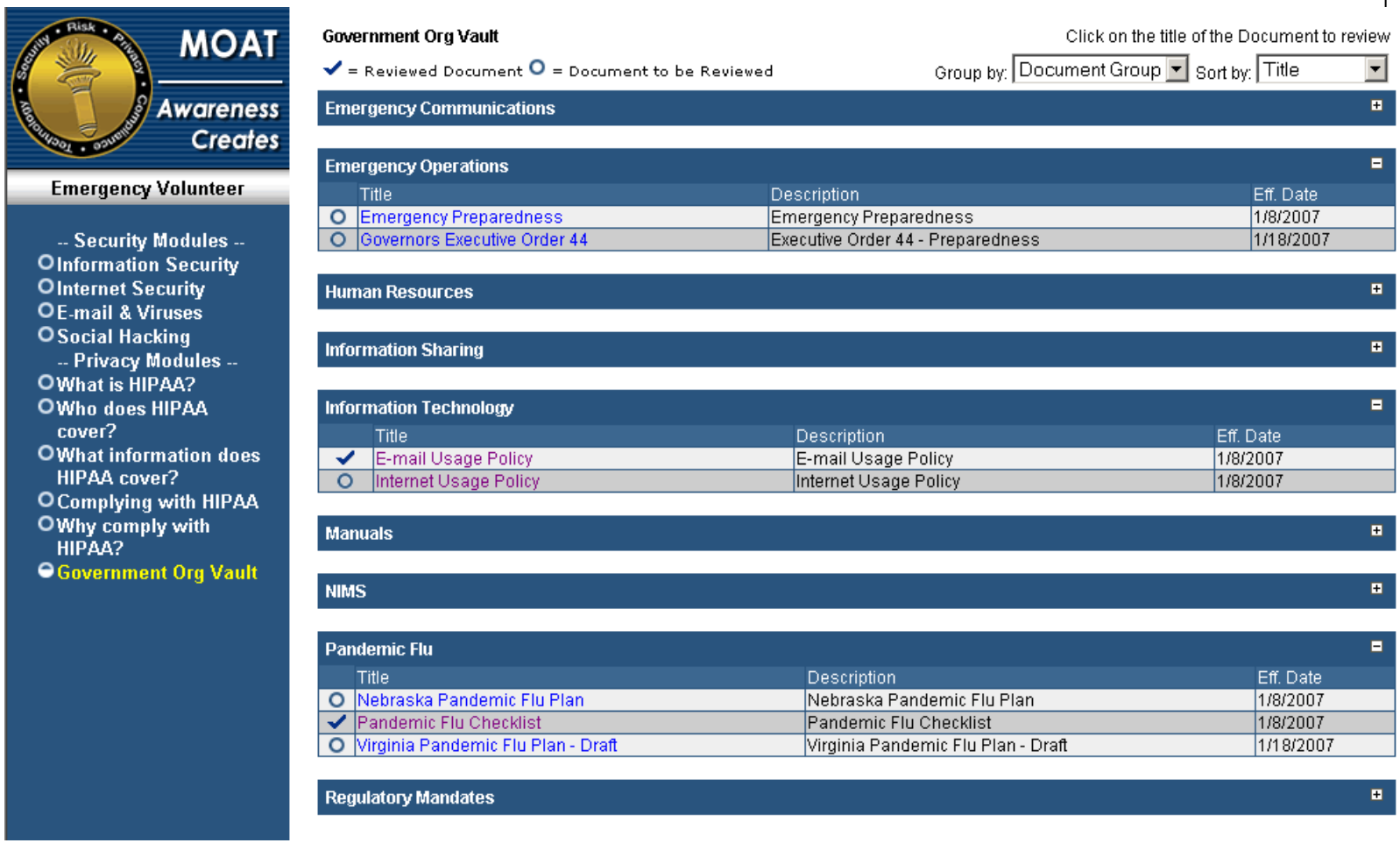
- ○ **True**
- ○ **False**

SUBMIT

Security Awareness Modules

- Security Awareness for Employees & Temps
- Security Awareness for Vendors & Contractors
- Security Awareness for Emergency Responders
- Security Modules are Updated Annually
  - New Topics, Threats, Stories and Best Practices
  - New Questions to Reiterate Key Information
- Helps Meet Regulatory Mandates
- Automatic Reminders Annually and Past Due
- Security Modules are Award Winning
- Security Modules Support Policies & Standards

MOAT – Managed Ongoing Awareness Tools



Executive Order 44 – Preparedness Initiatives

- Effective Date was January 12, 2007
- Important Government Obligations
- Agency Responsibilities
- Preparedness as an Individual Responsibility
- Planning & Assessments
- Certification Program
- Training – NIMS, NRP, Terrorism, ICS, etc.
- Reviewing, Testing, Roles, Responsibilities, etc.
- Ongoing Annual Reviews

Situational Awareness Vault

Government Org Vault

Click on the title of the Document to review

✔ = Reviewed Document ○ = Document to be Reviewed

Group by: Document Group Sort by: Title

Emergency Communications +

Emergency Operations −

	Title	Description	Eff. Date
○	Emergency Preparedness	Emergency Preparedness	1/8/2007
○	Governors Executive Order 44	Executive Order 44 - Preparedness	1/18/2007

Human Resources +

Information Sharing +

Information Technology −

	Title	Description	Eff. Date
✔	E-mail Usage Policy	E-mail Usage Policy	1/8/2007
✔	Internet Usage Policy	Internet Usage Policy	1/8/2007

Manuals +

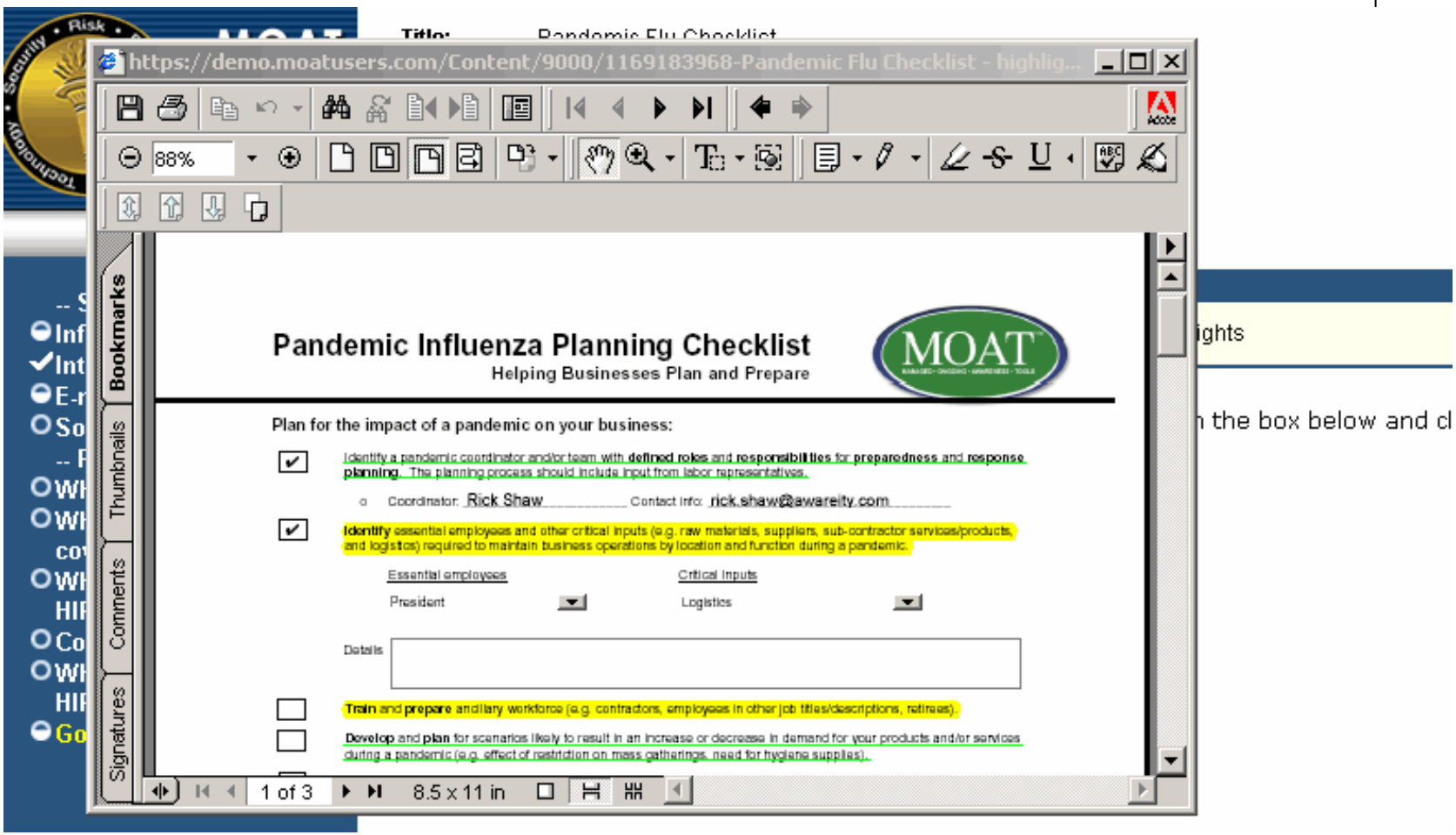
NIMS +

Pandemic Flu −

	Title	Description	Eff. Date
○	Nebraska Pandemic Flu Plan	Nebraska Pandemic Flu Plan	1/8/2007
○	Pandemic Flu Checklist	Pandemic Flu Checklist	1/8/2007
○	Virginia Pandemic Flu Plan - Draft	Virginia Pandemic Flu Plan - Draft	1/18/2007

Regulatory Mandates +

Policy Screen



Individual Acknowledgements

Title: Pandemic Flu Checklist
Description: Pandemic Flu Checklist
Printable Version

The following file is an active checklist for Pandemic Flu

Status	Document	Description
Read	PDF Adobe	Pandemic Flu Checklist with Active Fields and Highlights

If you understand and agree to comply with this policy, type **AGREE** in the box below and click the ACCEPT button.

agree

ACCEPT CANCEL

User Activity Report

User: Volunteer, Emergency **Email:** demo@awareity.com
Organization: Government Org **Department:** Volunteers
Location: **Unit:**

Date/Time	Activity Type	Additional Info
Jan 08 2007 - 11:45:48 AM	UserAdd	Student ID: 140; Student Added by Student Number: 14
Jan 16 2007 - 01:31:33 PM	UserEdit	Student ID: 140; Student Information Updated by Student Number: 14
Feb 02 2007 - 02:03:30 PM	UserEdit	Student ID: 140; Student Information Updated by Student Number: 133
Feb 02 2007 - 02:03:52 PM	login	Browser = IE
Feb 02 2007 - 02:04:31 PM	policyfile-userread	Policy ID: 74 - CIT ID: 79 - FilePath: Content/9000/1168286510-E-mail Usage Policy.pdf - MD5: 4cf8752be197a4b0b8041060e56eda69
Feb 02 2007 - 02:04:54 PM	policyagree	Policy: 74
Feb 02 2007 - 02:05:01 PM	policyfile-userread	Policy ID: 79 - CIT ID: 115 - FilePath: Content/9000/1169183968-Pandemic Flu Checklist - highlights.pdf - MD5: c357017ca880b178910b7fb1fef7cd59
Feb 02 2007 - 02:08:17 PM	policyagree	Policy: 79
Feb 02 2007 - 02:09:12 PM	lessonpass	Module.Lesson:56.1
Feb 02 2007 - 02:09:12 PM	testpass	Module.Lesson:56.1 Question: 4
Feb 02 2007 - 02:09:31 PM	testpass	Module.Lesson:56.3 Question: 5
Feb 02 2007 - 02:09:37 PM	lessonpass	Module.Lesson:56.3
Feb 02 2007 - 02:09:37 PM	testpass	Module.Lesson:56.3 Question: 6

Total Transactions: 13

Additional Vault Functionality

- Human Resource & Employment Policies
- Information Handling & Sharing Policies (laptops)
- Physical Security
- Ethics Responsibilities & Policies
- Regulatory Policies (HIPAA, OSHA, EEO, etc.)
- Continuity of Operations Plans
- Crisis Management Plans
- Evacuation Plans & Maps
- Pandemic Flu Plans & Responsibilities
- And many others…

Administrator Oversight Tools

Maintain Organizations

Maintain Users

Maintain Vault

Progress Reports

Document Reports

User Feedback Reports

User Activity Reports

TOOLS

AWAREITY

Maintain Users

User Maintenance

Organization:	Government Org	Department:	All Departments
First Name:		Email:	
Last Name:		Login ID:	
Show Inactive:	☐	Supervisor Email:	

SEARCH

User List:

User	Login ID	Department	Email	User ID	Status	Supervisor Email

ADD ADMIN

Maintain Users

Edit System User

Fields denoted by an asterisk (*) are required

Mandatory/System Information

First Name: First
Last Name: Responder *
Login ID: first.responder@gov.or *
Organization: Government Org *
Department: Emergency Director *
Group: USER *
Status: ACTIVE *
Email: demo@awareity.com *
Supervisor Email: support@awareity.com
Password: ********** *
Re-Enter Password: ********** *

☐ User must change password at next login

Curriculum Information

MOAT Curriculum: SAT-HIPAA-2007 *

Certification Information and Maintenance

Current Certification Status: Not yet Certified

UPDATE

Optional Information

AWAREITY

Progress Reports – All User Progress

Column Legend:
A = What is HIPAA?; B = Who does HIPAA cover?; C = What information does HIPAA cover?;
D = Complying with HIPAA; E = Why comply with HIPAA?; F = Information Security;
G = Internet Security; H = E-mail & Viruses; I = Social Hacking;
J = Government Org Vault;

User	Login ID	Last Login	Location	Department	Unit	Email	Phone	A	B	C	D	E	F	G	H	I	J
Admin, Awareity	awareity_admin@gov.org	1/16/2007 11:47:47 AM		None		support@awareity.com		○	○	○	○	○	○	○	○	○	○
Bates, Larry	lbates@gov.org	2/2/2007 7:06:34 AM		Executive Management		demo@awareity.com		○	○	○	○	○	◒	◒	○	○	◒
Chief, Fire	fire.chief@gov.org			Responder - Fire and Rescue		demo@awareity.com		○	○	○	○	○	○	○	○	○	○
Doctor, Doris	doris.doctor@gov.org			Responder - Emergency Medical		demo@awareity.com		○	○	○	○	○	○	○	○	○	○
Ghee, Elton	elton@gov.org	1/18/2007 11:48:07 AM		Administration		demo@awareity.com		○	○	○	○	○	◒	○	○	○	◒
Head, Department	department.head@gov.org			Executive Management		demo@awareity.com		○	○	○	○	○	○	○	○	○	○
Hoke, Melissa	mhoke@org.org	1/24/2007 11:05:29 AM		Executive Management		demo@awareity.com		○	○	○	○	○	◒	◒	○	○	○
Hruska, Mike	mhruska@gov.org			Information Technology		demo@awareity.com		○	○	○	○	○	○	○	○	○	○
Kelliher, Steve	skelliher@gov.org			Information Technology		demo@awareity.com		○	○	○	○	○	○	○	○	○	○
Lewy, Josh	jlewy@gov.org	1/23/2007 7:02:11 AM		Administration		demo@awareity.com		○	○	○	○	○	◒	○	○	○	○
Nurse, Nancy	nancy.nurse@gov.org			Responder - Emergency Medical		demo@awareity.com		○	○	○	○	○	○	○	○	○	○
Rappe, Jim	jrappe@gov.org	1/24/2007 10:02:31 AM		Administration		demo@awareity.com		○	○	○	○	○	◒	◒	○	◒	◒
Responder, First	first.responder@gov.org			Emergency Director		demo@awareity.com		○	○	○	○	○	○	○	○	○	○
Shaw, Rick	rick@gov.org	2/7/2007 10:07:04 AM		Administration		demo@awareity.com		◒	◒	◒	◒	◒	◒	◒	◒	◒	◒
Snow, Ron	ron.snow@gov.org	1/9/2007 6:58:29 AM		None		demo@awareity.com		○	○	○	○	○	◒	○	○	○	◒
Superintendent, School	school.superintendent@gov.org			School Superintendent		demo@awareity.com		○	○	○	○	○	○	○	○	○	○
Volunteer, Emergency	emergency.volunteer@gov.org	2/5/2007 8:59:23 AM		Volunteers		demo@awareity.com		○	○	○	○	○	◒	○	○	○	◒
Weaver, Katie	katie.weaver@gov.org	2/2/2007 2:10:08 PM		None		katie.weaver@awareity.com		○	○	○	○	○	◒	✓	◒	○	◒
Wood, Sheri	swood@gov.org	1/19/2007 6:04:26 AM		Executive Management		demo@awareity.com		○	○	○	○	◒	◒	○	○	◒	◒

Total Users: 19

Progress Reports – User Vault Status

Government Org

Report Date: 2/5/2007 9:02:02 AM

Document Status - (grouped by user)

Sort by: Document Name

[Print this Report]

User / Document Name		Document Agreed	Department	Location	Unit	Email
Volunteer, Emergency			None			demo@awareity.com
	123 Information Handling and Access	No				
	Business Continuity	No				
	E-mail Usage Policy	Yes				
	Emergency Preparedness	No				
	Ethics Policy	Yes				
	Governors Executive Order 44	No				
	HSPD-12 Regulations	Yes				
	Information Sensitivity and Handling	No				
	Internet Usage Policy	Yes				
	Nebraska Pandemic Flu Plan	No				
	NIMS -- IS-100 Introduction to ICS	No				
	Pandemic Flu Checklist	Yes				
	Responder Update - Seminar	No				
	Sexual Harassment Policy	Yes				
	Virginia Pandemic Flu Plan - Draft	No				

Total Users: 1

Progress Report – Document Status

Government Org

Report Date: 2/7/2007 1:50:51 PM

Document Status - (grouped by document)

Sort by: Name

[Print this Report]

Document Name / User		Document Agreed	Department	Location	Unit	Email
Pandemic Flu Checklist						
	Admin, Awareity	No	None			support@awareity.com
	Bates, Larry	No	None			demo@awareity.com
	Chief, Fire	No	None			demo@awareity.com
	Doctor, Doris	No	None			demo@awareity.com
	Ghee, Elton	No	None			demo@awareity.com
	Head, Department	No	None			demo@awareity.com
	Hoke, Melissa	No	None			demo@awareity.com
	Hruska, Mike	No	None			demo@awareity.com
	Kelliher, Steve	No	None			demo@awareity.com
	Levy, Josh	No	None			demo@awareity.com
	Nurse, Nancy	No	None			demo@awareity.com
	Rappe, Jim	No	None			demo@awareity.com
	Responder, First	No	None			demo@awareity.com
	Shaw, Rick	Yes	None			demo@awareity.com
	Snow, Ron	No	None			demo@awareity.com
	Superintendent, School	No	None			demo@awareity.com
	Volunteer, Emergency	Yes	None			demo@awareity.com
	Weaver, Katie	No	None			katie.weaver@awareity.com
	Wood, Sheri	Yes	None			demo@awareity.com

Total Document(s): 1

AWAREITY

User Activity Report

User: Volunteer, Emergency **Email:** demo@awareity.com
Organization: Government Org **Department:** Volunteers
Location: **Unit:**

Date/Time	Activity Type	Additional Info
Jan 08 2007 - 11:45:48 AM	UserAdd	Student ID: 140; Student Added by Student Number: 14
Jan 16 2007 - 01:31:33 PM	UserEdit	Student ID: 140; Student Information Updated by Student Number: 14
Feb 02 2007 - 02:03:30 PM	UserEdit	Student ID: 140; Student Information Updated by Student Number: 133
Feb 02 2007 - 02:03:52 PM	login	Browser = IE
Feb 02 2007 - 02:04:31 PM	policyfile-userread	Policy ID: 74 - CIT ID: 79 - FilePath: Content/9000/1168286510-E-mail Usage Policy.pdf - MD5: 4cf8752be197a4b0b8041060e56eda69
Feb 02 2007 - 02:04:54 PM	policyagree	Policy: 74
Feb 02 2007 - 02:05:01 PM	policyfile-userread	Policy ID: 79 - CIT ID: 115 - FilePath: Content/9000/1169183968-Pandemic Flu Checklist - highlights.pdf - MD5: c357017ca880b178910b7fb1fef7cd59
Feb 02 2007 - 02:08:17 PM	policyagree	Policy: 79
Feb 02 2007 - 02:09:12 PM	lessonpass	Module.Lesson:56.1
Feb 02 2007 - 02:09:12 PM	testpass	Module.Lesson:56.1 Question: 4
Feb 02 2007 - 02:09:31 PM	testpass	Module.Lesson:56.3 Question: 5
Feb 02 2007 - 02:09:37 PM	lessonpass	Module.Lesson:56.3
Feb 02 2007 - 02:09:37 PM	testpass	Module.Lesson:56.3 Question: 6

Total Transactions: 13

Administrator Oversight Tools

Maintain Organizations

Maintain Users

Maintain Vault

Progress Reports

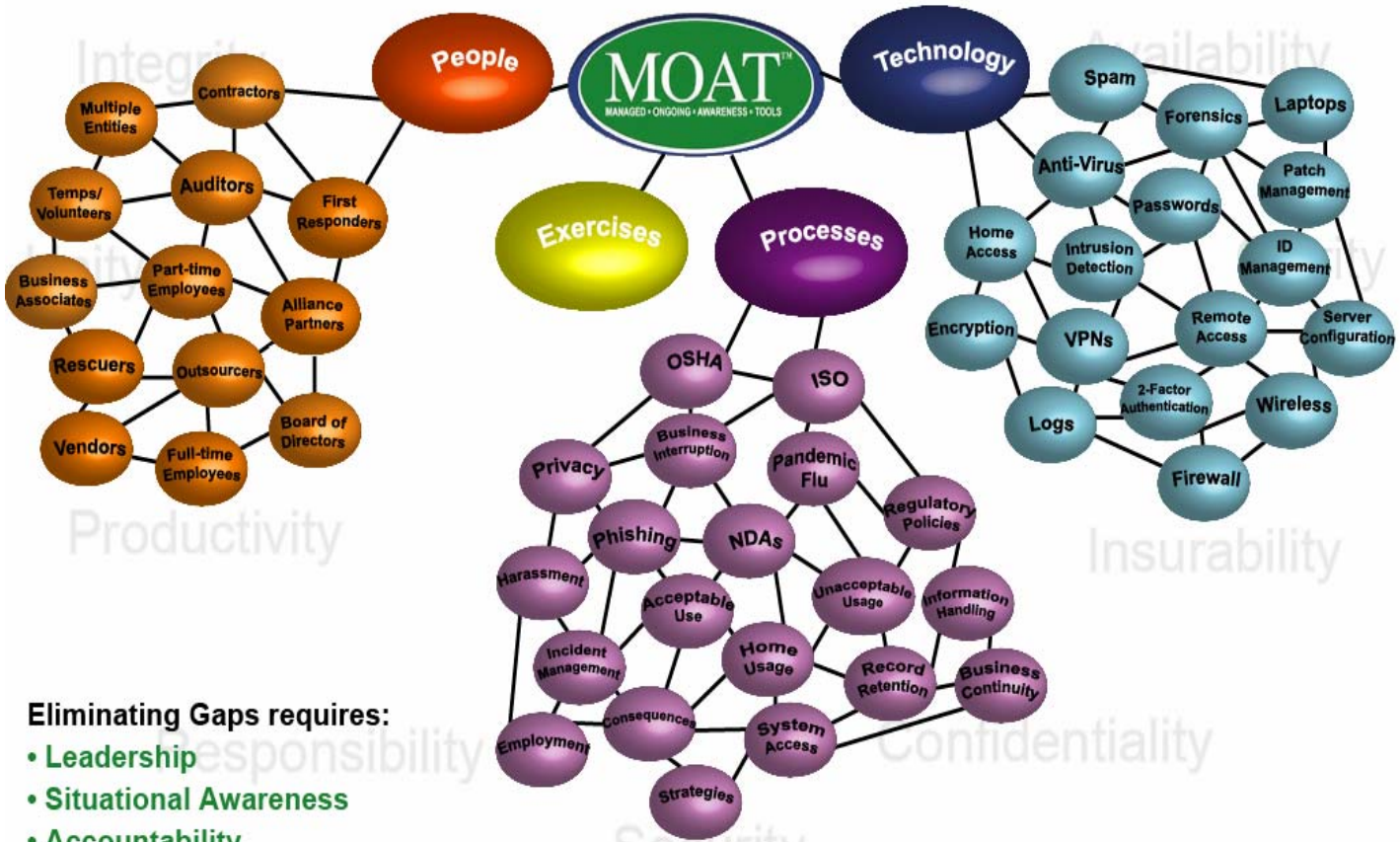
Document Reports

User Feedback Reports

User Activity Reports

TOOLS

Connecting the Dots and Eliminating Gaps



Eliminating Gaps requires:

- Leadership
- Situational Awareness
- Accountability

Connecting the Dots requires MOAT.

AWAREITY

MOAT Pricing Information

- Standard MOAT & Security Awareness Modules
  - $4/User per Year
- Enhanced MOAT & Security Awareness Modules
  - $8/User per Year (Standard + $4/User)
- Privacy Modules (HIPAA)
  - $5.50/User per Year
- Virginia Interactive is “Primary Contact” for:
  - Online Demonstrations
  - Proposals
  - Initial and Annual Billing

Questions?

To See Online Demonstration

Rick Shaw

402.730.0090

rick.shaw@awareity.com

or

Sheri Wood

804.786.1851

swood@virginiainteractive.org

Virginia Information Technologies Agency

Information Security Assurance Plan

Cathie Brown, CISM, CISSP

February 15, 2007

Assurance of Infrastructure Security

- VITA is responsible for providing a secure IT Infrastructure that supports customer agency systems and data, and
- Customer agencies need to rely on the security of the IT infrastructure in protecting high risk systems and sensitive data
- APA
  - **"Since VITA has assumed responsibility for the information technology infrastructure, the Agency Commissioner must have VITA provide assurance that their infrastructure would provide the safeguards to protect information and databases under not only state policy, but HIPAA …"**

Collect Agency "High Risk" System Information

- Customer Agency Information Security Template
  - Systems that use VITA Infrastructure
  - Systems that are "high risk" relative to confidentiality or integrity
  - Systems containing data with specific security needs
  - Requested on March 31, 2007 to be returned by May 1, 2006
  - Collected information from 63 agencies

Collect Technical Infrastructure Information

- Technical Data Survey
  - Information on Servers (logical and physical)
  - Information on Infrastructure and network devices
  - Information on environmental and physical controls
  - Information includes requirements with NG 10 Infrastructure Practices, HIPAA, ISO17799, IRS1075 and COV IT Security Policy and Standard
  - March, 2007 timeframe
  - Collecting technical data from VITA/NG Engineers

Security Analyses

- VITA will perform analyses based on security controls currently implemented and security controls required
- Document gaps and recommendations
- Work with VITA/NG technical team to develop remediation plans
- VITA Security will provide a letter of assurance as is, or develop a work plan with corrective actions or possible risk acceptance pending transformation

Letters of Assurance

- Based on these reviews, VITA will issue a letter of assurance as recommended by APA
  - Summer, 2007 timeframe
  - Will state whether controls are in place and functioning or identify where they are not, what the risk is and what the risk management plan is for exposure

Security Data Warehouse

- Developing CASS (Customer Agency Security System)
  - Phase I: Information Security Template Data
  - Phase II: Technical Data, Regulations, GAP
  - Phase III: Audits, Contingency Surveys, Exceptions
  - Phase IV: Data Collection & Verification
  - Phase V: Link to ESOC for incident management
- Customer agencies will be able to update the information in the database via a web interface

Annually

- VITA will request agencies update their information
- VITA will reassess agencies' information
- Using agency IT security audits, SAS 70 Type II Audits and/or security audits by 3rd party, VITA will assess whether controls are in place and functioning
- If needed, VITA will utilize the 'right to audit' clause in the contract with NG to provide assurance
- VITA will issue a letter of assurance to the agency

Questions

Other Business

UPCOMING EVENTS!

ISOAG MEETING DATES
Thursday, March 14, 2007
1:00 - 4:00
@ Department of Health Professions

Draft Agenda
Encryption Ordering
IT Partnership Update
SJR 51 Action Plan
Information Security Council

Upcoming Events

Virginia Digital Government Summit

March 15, 2007 Richmond Marriott

http://www.govtech.net/events/index.php/VirginiaDGS2007

ADJOURN

THANK YOU FOR YOUR TIME AND THOUGHTS

!!!