Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

July 14, 2009

July

Virginia Information Technologies Agency

ISOAG July 2009 Agenda

I.	Welcome & Opening Remarks	Peggy Ward, VITA
II.	E-Discovery & Its Impact on Agencies	Julie Whitlock, Office of the Attorney General
III.	Collection of SSN in the Commonwealth	Lisa Wallmeyer, Joint Commission on Technology & Science
IV.	E-Mail Management Guidelines	Siri Berdahl, Library of Virginia
V.	2009 COV Security Policy & Standard	John Green, VITA
VI.	Information Risk Executive Council (IREC)	John Green, VITA
VII.	Current Hard Disk Encryption Offering	Eric Taylor, NG & Don Kendrick, VITA
VIII.	Customer Service Alerts	Don Kendrick, VITA
VIII.	2009 Commonwealth Security Data Points	Peggy Ward, VITA
IX.	Information Security Awareness Toolkit	Nakita Albritton, VITA
X.	Security Incidents – Who, what, when, & why?	Michael Watson, VITA
XI.	July 2009 Cyber Security Attacks	Michael Watson, VITA
XII.	Upcoming Events and Other Business	Peggy Ward, VITA

E-Discovery and Its Impact on Agencies

Julie Whitlock,
Assistant Attorney General
Technology and Procurement Law Section

What is discovery?

- Discovery is the process by which parties to a lawsuit exchange information, or request it from third parties
  - Requests for production of documents
  - Subpoenas
  - Depositions
  - Etc.

What is e-discovery?

- Process by which parties request “electronically stored information” = ESI
- Includes:

Emails	Metadata and embedded data
Voice mails	Spreadsheets
Word files	Text messages
Calendars	IM transcripts
Web site postings	Videos

Information on jump drives, PDAs, and Blackberries

Information stored on home or personal computers and devices, and in personal e-mail accounts

Why is e-discovery a hot topic?

- Changes to Federal Rules of Civil Procedure
  - Effective December 2006
  - Specifically address e-discovery and ESI
  - Specifically allow for sanctions, including monetary sanctions and limitation of claims or defenses available in overall suit
  - Require early conference to discuss availability, cost, and timing of producing data
- Changes to Virginia Supreme Court Rules
  - Effective January 1, 2009
  - Also now specifically reference e-discovery

Other changes

- Statewide document retention schedules have not changed, but email handling policy has
- Duty to preserve evidence has not changed

The ever-growing mountain

- Organizations may handle millions of new emails and other files every day
- If each employee has to sift through this mountain, loss of productivity would be high and likelihood of success in finding all relevant content would be low – so, where to begin?

Two Cautionary Tales ...

- *Qualcomm Inc. v. Broadcom Corp*., 2008 U.S. Dist. LEXIS 911(S.D. Cal. Jan. 7, 2008) (opinion ordering sanctions, involving underlying failure of a party to disclose 200,000 emails prior to trial)
- *United Medical Supply Co. v. United States, 77 Fed. Cl. 257* (June 27, 2007) (sanctions imposed for failure to adequately preserve ESI based on faulty email communications with contractors)

Effective Records Management = Effective Litigation Responses

- Records management ensures compliance with state and agency document retention schedules
- Provides the foundation for compliance with discovery rules
- Enables efficient review of ESI
- Reduces cost of storage, cost of searching, cost of retrieval
- Library of Virginia retention schedules address both physical records and virtual records

Virginia Code

§ 42.1-86.1. Disposition of public records. —

***

C. Each agency shall ensure that records created after July 1, 2006 and authorized to be destroyed or discarded in accordance with subsection A, <u>are destroyed or discarded in a timely manner in accordance with the provisions of this chapter</u>; provided, however, such records that contain identifying information as defined in clauses (iii) through (ix), or clause (xii) of subsection C of § 18.2-186.3, shall be destroyed within <u>six months</u> of the expiration of the records retention period.

***

(iii) social security number (iv) driver's license number
(v) bank account numbers (vi) credit or debit card numbers
(vii) PIN numbers (viii) electronic identification codes
(ix) automated or electronic signatures (xii) passwords

Duty to preserve evidence

- Common law concept accepted by courts
- Preservation of all evidence in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection (e.g. metadata)
- When litigation is reasonably likely, an entity has obligation to preserve documents and ESI relevant to anticipated claims and defense
  - Duty typically begins prior to lawsuit
  - May extend far beyond physical boundaries of the agency
  - Requires identification of what should be preserved

“Not reasonably accessible”

- Duty extends to all potentially relevant ESI, even if not “reasonably accessible”
- May not be required to produce if it is not “reasonably accessible,” but must still preserve potentially relevant ESI
- To show ESI is “not reasonably accessible,” agency must be able to show that it would be unduly burdensome or costly to produce the category requested

Early notifications

When you anticipate litigation may be in your future, either as a plaintiff or defendant, you should notify your counsel at the AG's Office

- Receive advice specific to the situation
- Discuss scope of potential litigation holds
- Identify individuals who will be involved in holds and searches
- Identify individual(s) who will be contact with AG's Office

- VITA should also be notified early on, to enable efficient responses and coordinate any necessary litigation holds
- Federal rules require parties at very beginning stages of litigation to meet and negotiate regarding the ESI that will be produced
  - Decisions will be made here that will be difficult to reverse, so come prepared!

Dear Agency

- I'm from the OAG. Your agency has been named as a party to a lawsuit in federal court.
- I will need a contact who can:
  - Be familiar with your agency's systems, terminology, and document retention and management policies.
  - Meet and discuss the case and develop an initial course of action. This will include:
    - Determining the affected organizational units within your agency
    - Identifying the locations where data may be stored
    - Designating an agency representative to be responsible for overseeing the implementation of an immediate "litigation hold" and preventing the destruction or alteration of any potentially relevant documents.

Dear Agency (con't)

- I will also need an individual from your agency to attend a conference with the opposing parties within the next 15-30 days. The following will be discussed at the conference:
  - The manner in which your agency will be preserving, maintaining, and providing ESI
  - Descriptions of the categories and locations of ESI that your agency may use to support its claim or its defenses
  - For ESI you would like to request from the other side, the substantive content of the ESI, the form in which you would like to receive the ESI, and the reasons why that particular form of production is necessary

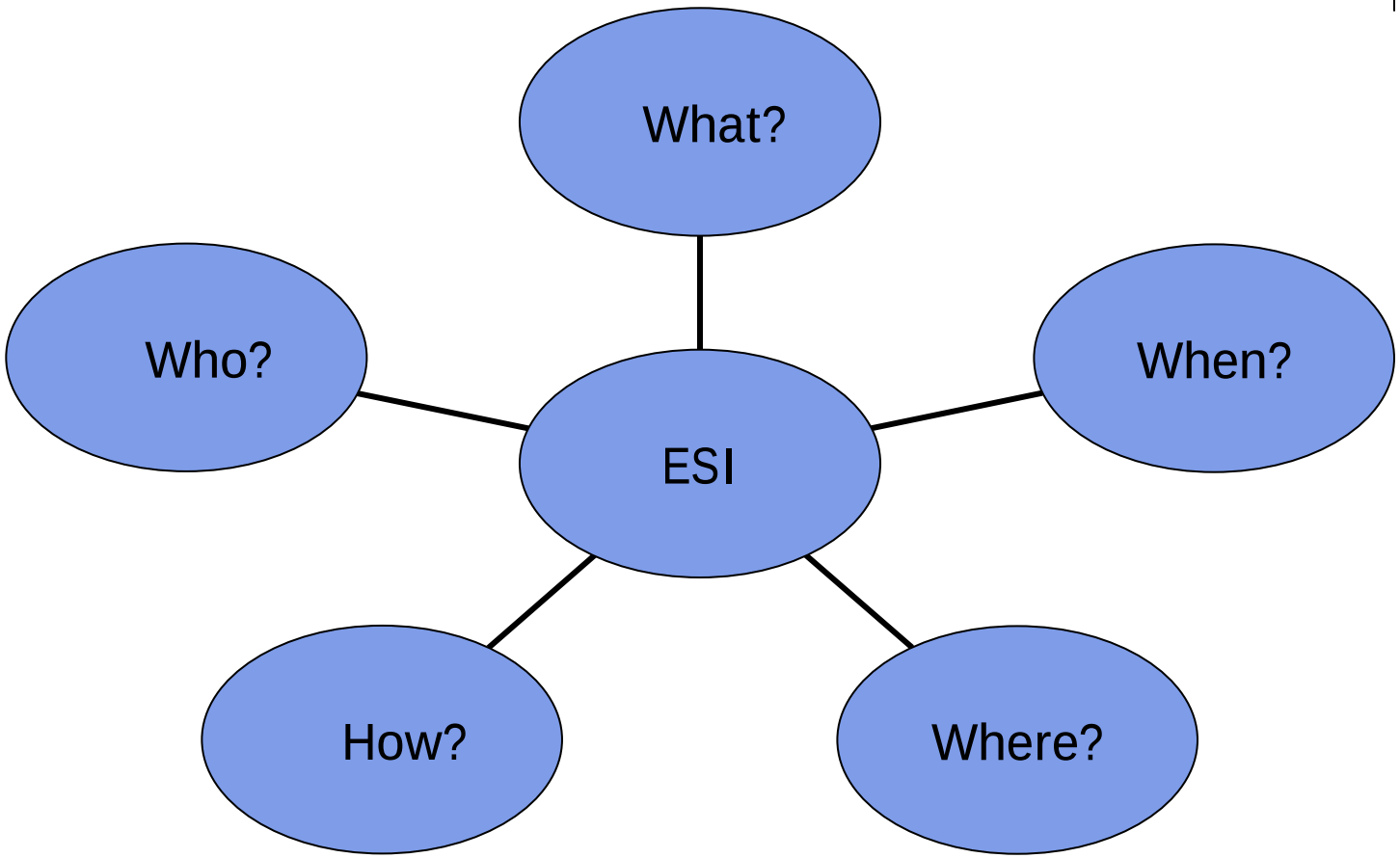
Will you be able to respond?

- Are you familiar with what you have electronically, where it is stored, in what formats, and who is responsible for it?
- Are you familiar with your automatic backup and archiving functions?
- Do you understand what would be necessary to perform a search or to retrieve archived documents?
- Do you know which positions are involved in data retention – this includes your document retention/records management officer?

You must respond quickly

- Court Rules place heavy burden on parties to be prepared to respond very quickly – if the agency cannot, the Court will decide the extent to which agency will have to produce (regardless of burden or cost)
- Once agreements or decisions are made, they will be difficult to undo
- New Rules provide Court with authority to impose non-monetary sanctions for failure to comply with Court's order

ISSUES



Issues

- **Who** will be responsible for organizing agency's response to discovery? For ensuring that litigation holds are implemented and followed? For determining where existing records can be found, and under what circumstances?
- **What** records need to be maintained? **What** records need to be searched?
- **Where** are the records that must be maintained or searched?
- **When** should holds be put in place?
- **How** will holds and searches be conducted?

Who: The relevant agency personnel

- "Rapid Response Team" may include
  - Individuals with IT responsibilities for maintaining data
  - IT individuals to assist with search
  - Records management officer
- Team will have to identify individuals with information potentially relevant to claim
- Who will be responsible for implementing the "litigation hold," ensuring it is communicated to all relevant personnel, and that it is maintained?

What: Finding the ESI

- Catalog the locations where ESI is stored, and in what form
- Consider copies, backups and archives at the agency level and the enterprise level
- Don’t forget about the individual level – ESI may be found on personal devices such as PDAs, cell phones, jump drives, etc.

Where & How: Searching

- Where is the ESI?
- How will the search be performed?
- Does a contractor need to be engaged to assist with the search?

When: Preserving the ESI

- All potentially relevant ESI, whether or not it is reasonably accessible, must be preserved
- The destruction of ESI can lead to sanctions – including limits on what defenses or claims may be presented by the party

What can my agency do now?

- Review current document retention schedules and practices
- Become familiar with what you have electronically, where it is stored, in what formats, and who is responsible for it (don’t forget personal devices)
- Become familiar with your automatic backup and archiving functions
- Begin to understand what would be necessary to perform a search or to retrieve archived documents

What else can my agency do?

- Identify positions within your agency that are involved in data retention – this includes your document retention/records management officer
- Encourage the segregation of personal or proprietary information before data is archived – to reduce the time spent segregating when responding to a request
- Review IT support contracts (including web hosting) to determine what obligations, if any, the contractor would have to retain or archive web shots and other ESI

Helpful hints for reducing potential discovery burden

- Encourage controls on “scattering” of ESI
  - Limited distribution of emails
  - Limited use of multiple forms of communication
- Consistently enforce archival programs
  - But beware of potential need to suspend where necessary
- Consider the way that documents and emails are grouped or identified – e.g. by date, by project, by concept
  - Encourage helpful subject lines
  - Consistent use of identifying information
  - Identification of attorney communications

If you are unlucky enough to have to conduct a search, consider…

- Individual privacy of user
- Prevention of data loss, whether inadvertent or intentional
- Minimizing individual disruptions while searching and responding to discovery requests
- Operational efficiencies to ensure timely preservation and processing of data
- Consistency of process

More suggestions

- E-discovery will require small cross-functional teams to foster communication, assess risks, and establish priorities
- Resist over-preserving content, which increases cost of discovery later
- Conduct regular audits and reviews

Where to turn for help

- Agency Records Officer
- The Library of Virginia
- The FOIA Council
- Your agency’s assigned counsel at the Office of Attorney General

Conclusion

Collection of SSN in the Commonwealth

Lisa Wallmeyer, Executive Director
Virginia Joint Commission on Technology & Science

JCOTS

What is JCOTS?

- JCOTS is a permanent legislative commission, established by the General Assembly in 1997 to…

  "…study all aspects of technology and science and endeavor to ***stimulate, encourage, promote, and assist*** in the development of technology and science in the Commonwealth and sound public policies related thereto…"

(§ 30-85 of the Code of Virginia)

JCOTS

Personally Identifiable Information Subcommittee

- Originally convened during 2007 Interim; continued in 2008 & 2009
- A joint subcommittee of JCOTS and the Freedom of Information Advisory Council
- Develop policy regarding the protection of personally identifiable information
  - Discussion turned to focus on over-collection of Social Security Numbers by government entities

JCOTS

What is an SSN?

123-45-6789

At its most basic, an SSN is a unique 9-digit number assigned to an individual to track certain federal benefits

HISTORY

- 1936: SSN first assigned by federal government as an account number to track social security benefits
- 1961: Congress authorizes IRS to use SSN as a tax identification number

JCOTS

What is an SSN?

- Overtime, the SSN was used for many purposes, because of its quality as a unique identifier
  - Driver's license number, student ID number, health insurance ID number, link to credit and financial institutions and transactions
- Developed into a key piece of data for identity thefts

JCOTS

The most misused SSN of all time

"The Woolworth Number"

- In 1938, the manufacturer of a wallet sold at Woolworths promoted its product by including a sample SSN card to show how it would fit in the product
- Company VP thought it would be clever to use the SSN of his secretary, Ms. Whitcher
- Sample was half the size of a real card, and printed in red
- Many purchasers adopted the sample card as their own…in 1943, 5,755 people were using the number
  - All total, 40,000 people reported their SSN as 078-05-1120
  - As late as 1977, 12 people were still reporting this as their SSN
- The SSA publicized that it was incorrect to use this number, voided it, and gave Ms. Whitcher a new SSN!

Source: The Social Security Administration www.socialsecurity.gov/history/ssn/misused.html

JCOTS

SSN & Identity Theft

- Various perspectives exist, but many agree that it is a key ingredient in identity theft
  - Not good if your social security number becomes too social!
- One potential source of SSN: government records

JCOTS

What's been done already?

- Federal Privacy Act of 1974
  - No federal, state, or local government agency may deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide his SSN
  - Exceptions:
    - Disclosure is required by federal statute
    - Disclosure was required prior to January 1, 1975 under statute or regulation adopted prior to that date to verify an individual's identity
  - Virginia has adopted similar language – Government Data Collection & Dissemination Practices Act (Va. Code § 2.2-3800 et seq.)

JCOTS

What's been done already?

- Over the past decade, Virginia has limited the use of SSN:
  - SSN can no longer be used as driver's license number (not even optional)
  - SSN can't be displayed on student ID cards or agency-issued cards
  - SSN can't be used as Health Insurance ID under state plan

JCOTS

Recent legislation

- Legislation adopted during 2009 Session of the General Assembly will prohibit a government agency from releasing more than the last four digits of a SSN in response to a FOIA request
  - Chapter 213 of the 2009 Acts of Assembly

JCOTS

What about collection of SSN?

- A lot of focus in this discussion on dissemination of social security numbers…what about looking why and when we collect it in the first place?
- Past few years have drawn attention to database breaches, misuse of information, etc.

JCOTS

Over-collection of SSN

- Focus of on-going, 2 year study of JCOTS and the FOIA Council
- Extensive survey of all state, local agencies conducted in 2008
  - Still processing results
  - Tremendous response

JCOTS

Future limitations on collection

- Beginning July 1, 2010, no agency shall collect from an individual his social security number (or any portion thereof) unless collection is:
  - Authorized or required by state or federal law; AND
  - Essential for the performance of that agency's duties

JCOTS

Questions?

Lisa Wallmeyer, Executive Director

Virginia Joint Commission on Technology & Science

jcots@dls.virginia.gov

804.786.3591

http://jcots.dls.virginia.gov

JCOTS

E-Mail Management Guidelines

LIBRARY OF VIRGINIA

Siri Berdahl,
Electronic Records
Analyst

What we'll cover

- E-mail management challenges
- LVA's mission and mandate
- E-Mail Management Guidelines

E-Mail Management Challenges

Why we need guidelines

Is E-Mail a Record?

"Public record" or "record" means recorded information that documents a transaction or activity by or with any public officer, agency or employee of an agency. **Regardless of physical form or characteristic**, the recorded information is a public record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of public business. **The medium upon which such information is recorded has no bearing on the determination of whether the recording is a public record.**

Code of Virginia, Title 42.1 Chapter 7

Virginia Public Records Act

COMMONWEALTH OF VIRGINIA

THE LIBRARY OF VIRGINIA

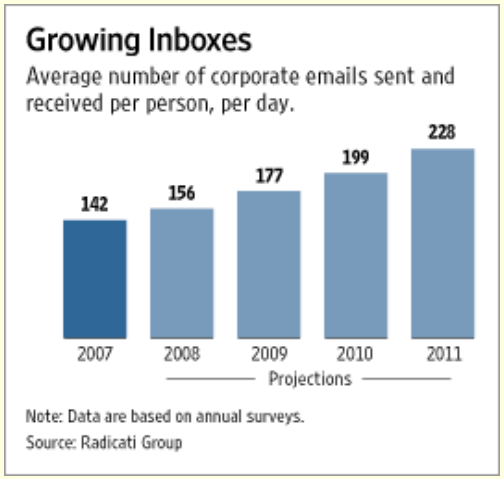
ARCHIVAL AND RECORDS MANAGEMENT SERVICES DIVISION
(Form RM-2 February 2008)

RECORDS RETENTION AND DISPOSITION SCHEDULE
GENERAL SCHEDULE NO. 19
COUNTY AND MUNICIPAL GOVERNMENTS
ADMINISTRATIVE RECORDS

EFFECTIVE SCHEDULE DATE: March 20, 2008

RECORDS SERIES AND DESCRIPTION	SERIES NUMBER	SCHEDULED RETENTION AND DISPOSITION
Correspondence/Subject Files - Board Members - Except Chairpersons This series documents incoming and outgoing letters, memoranda, faxes, notes and their attachments, in any physical format including, but not limited to, paper and e-mail.	100893	Retain 3 years, then destroy. Disposal reporting on *Certificate of Records Destruction* (RM-3 form) not required.
Correspondence/Subject Files - City/Town Manager, City/Town Council, County Administrator and Board of Supervisors This series consists of incoming and outgoing letters, memoranda, faxes, notes and their attachments, in any physical format including, but not limited to, paper and e-mail.		Refer to *General Records Retention and Disposition Schedule No. GS-4, County, City and Town Administration Records* for retention guidelines.
Correspondence/Subject Files - Department or Division Heads This series consists of incoming and outgoing letters, memoranda, faxes, notes and their attachments, in any physical format including, but not limited to, paper and e-mail.	010037	Retain 3 years then destroy.
Correspondence/Subject Files - Other Officials This series consists of incoming and outgoing letters, memoranda, faxes, notes and their attachments, in any physical format including, but not limited to, paper and e-mail.	010038	Retain 2 years then destroy.
Correspondence/Subject Files - Routine, Administrative - Not Specified Elsewhere This series consists of incoming and outgoing letters, memoranda, faxes, notes and their attachments of a routine administrative nature, in any physical format including, but not limited to, paper and e-mail.	010039	Retain as long as administratively necessary then destroy.

E-Mail Challenges



LVA’s Mandate

Why we care about e-mail management

Code of Virginia § 42.1-82
Duties and powers of Library Board

A. The State Library Board shall:
2. Issue regulations and guidelines designed to facilitate the creation, preservation, storage, filing, reformatting, management, and destruction of public records by agencies.

B. The State Library Board may establish advisory committees composed of persons with expertise in the matters under consideration to assist the Library Board in developing regulations and guidelines.

E-Mail Management Guidelines

The feature presentation

Commonwealth of Virginia

E-Mail Management Guidelines

EFFECTIVE MAY 2009

LIBRARY OF VIRGINIA
800 East Broad • Richmond, Virginia 23219
lva.virginia.gov

E-Mail Management Guidelines

Scope

These guidelines establish the basic best practices related to the creation, maintenance, use, and disposition of public records created by all state and local government employees using electronic mail applications.

E-Mail Management Guidelines

Purpose

To ensure that the Commonwealth's electronic mail records are retained economically and efficiently for as long as they have legal, fiscal, business, or historic value and that confidential information is protected while making all other electronic mail available to the citizens of Virginia.

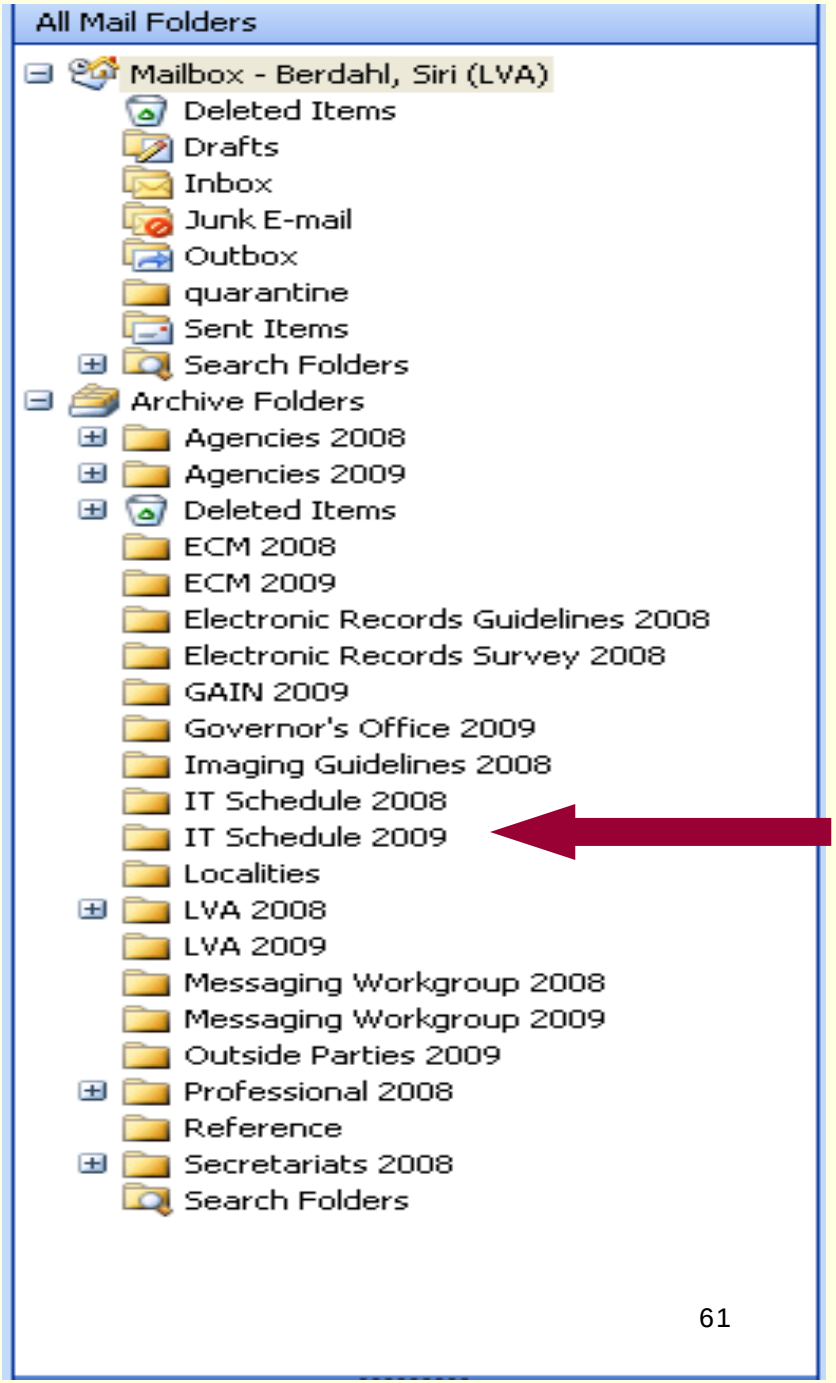
Guidelines Highlights

- Stress agency/locality responsibility
- Dissuade agencies from using “AutoArchiving” function
- Set forth procedures to enhance the legal admissibility of e-mail records
- Reiterate the importance of LVA-approved Records Retention & Disposition Schedules
- Set forth methods of appropriate e-mail storage

Acceptable E-Mail Storage

- Storing e-mails within an electronic mail system
- Creating folders that are stored outside of the mailbox but can be viewed using the e-mail client

Folders stored outside mailbox but viewed with e-mail client



Acceptable E-Mail Storage

- Storing, accessing, and managing e-mail messages and other electronic records using an Enterprise Content Management (ECM) system
- Printing e-mails along with any transmission and receipt data and maintaining them in a manual filing system

But wait! There's more!

- Users must not delete messages before the expiration of the LVA-approved retention period
- Ensure automatic deletion rules are turned off
- After an employee terminates, e-mail messages must be retained according to appropriate schedule

Learn More

For more information, read the guidelines online:

http://www.lva.virginia.gov/agencies/records/electronic/email-management-guidelines.pdf

Archives and Records Management Services

LIBRARY OF VIRGINIA

Siri Berdahl

Electronic Records Analyst

siri.berdahl@lva.virginia.gov

Phone: 804-692-3768

Fax: 804-692-3603

Virginia Information Technologies Agency

2009 COV Security Policy & Standard Update

John Green
Deputy Chief Information Security Officer

Virginia Information Technologies Agency

Policy, Standard & Guidelines Update

Progress:
Step by Step

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

Standard

Policy

= STATUS THIS MONTH

= STATUS LAST MONTH

Your Information Risk Executive Council Membership

Information Risk Executive Council

Paid COV State and local government membership!!

Key benefits:

-Save time – avoid reinventing the wheel

-Save costs – by adapting proven ideas, tools and templates from your peers to improve execution efficiency

- Minimize risk – by learning from peer experience and validating your approach

To gain access to IREC, please log into www.irec.executiveboard.com and click on the link on the right hand side that says “My organization is a member, I need a username and password”.

You will then receive a link to set up your profile and log in.

** If your domain does not end with .Virginia.Gov you will have to email: saunderj@executiveboard.com

Visit the IREC Website
www.irec.executiveboard.com

- Log onto the website and click on “Get a Username and Password”. Every member of the Commonwealth team can create a unique username and password and has unlimited, unmetered access to the resources.
- Fill out the brief form including your business email address and click “Submit”
- A link will be sent to your email address to setup your account

A Wealth of Resources are Available on the IREC website…

- **IREC Blog**
- **IREC Critical Initiative Support Plans**
- **Decision Support Centers**
- **Benchmarking, Surveys and Diagnostics**
- **Events and Webinars**
- **Peer Networking**

Teleconferences are hosted monthly and are open to the entire team.

- Register directly on the website under the “Events and Webinars” tab.
- The TCs are audio archived and can be downloaded from the website if you are unable to attend.
- The TCs save members a lot of time in understanding how to apply our profiled case studies to your business and objectives. I can schedule a call with the presenter after the TC if you have specific questions.

Upcoming Teleconferences

Effectively Supporting Disaster Recovery and Business Continuity Planning Efforts

2009-2010 Budget Outlook for Information Security

Security Implications of IT "Consumerization" and Social Media

Security Governance - A Critical Review of Common Archetypes

Managing Privileged User Access

Account Management Contact Information

- Your Account Manager is available to educate you and your team on the resources that are available through your membership. Please do not hesitate to reach out with any questions.

- The MSC's hours of operation are 8am to 6pm ET, M-F, except US Federal Holidays.

- The MSC can help you with web access, meeting registration, technical issues, and event related requests.

Jennifer Long
Phone: (919)782-3154 office / (202) 441-1656 cell
saunderj@executiveboard.com

Member Support Center
Phone: 1-866-913-8101
CEB-MemberSupport-IT@executiveboard.com

Virginia Information Technologies Agency

Current Hard Disk Encryption Offering

Eric Taylor, NG Security Architect

Don Kendrick, SMO Sr Manager

Current Hard Disk Encryption Offering

- Current deployment & IRAP (Information Risk Assessment)

- Future deployment

Virginia Information Technologies Agency

Customer Service Alerts (aka CSA)

Don Kendrick
Senior Manager Security Operations and Architecture, SMO

Virginia Information Technologies Agency

2009
Commonwealth Security Annual Report

Peggy Ward
Chief Information Security & Internal Audit 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	Pending	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	Pending	Yes	Not Due
Dept. of Housing & Community Development	Yes	1	Expired	Some	No
Dept. of Mines, Minerals & Energy	Yes	1	Pending	Yes	Yes
Dept. of Labor & Industry	Yes	3	No	N/A	N/A
Dept. of Professional & Occupational Regulation	Yes	1	Expired	No	N/A
Tobacco Indemnification Commission	Yes	0	No	N/A	N/A
Va. Employment Commission	Yes	2	Expired	Some	Yes
Va. Economic Development Partnership	Expired	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	No	N/A

Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
Dept. of Education	Yes	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	0	No	N/A	N/A
Va. Commission for the Arts	Yes	0	No	N/A	N/A
Va. Museum of Fine Arts	Yes	2	Yes	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	Yes	No	N/A
George Mason University	Yes	1	Expired	Some	Yes
James Madison University	Yes	1	Yes	Yes	Some
Longwood University	Yes	1	Expired	Yes	Yes
Norfolk State University	Yes	2	Yes	No	N/A
Old Dominion University	Yes	0	Expired	Yes	Pending
Radford University	Yes	0	Yes	Yes	Yes
University of Mary Washington	Yes	1	Yes	Not Due	Not Due
Va. Community College System	Yes	43	Expired	Pending	Pending
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	Expired	4	Yes	No	N/A
Dept. of Planning & Budget	Yes	1	Yes	No	N/A
Dept. of Taxation	Yes	0	Yes	Some	Some
Dept. of Treasury	Yes	3	Yes	Yes	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	0	Yes	Not Due	Not Due
Dept. of Medical Assistance Services	Yes	4	Yes	Yes	Yes
Department of Behavioral Health and Developmental Services ~~DMHMRSAS~~	Yes	22	Yes	No	N/A
Dept. of Rehabilitative Services	Yes	0	Expired	No	N/A
Dept. of Social Services	Yes	2	Expired	No	N/A
Virginia Foundation for Healthy Youth ~~TSF~~	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	1	Pending	Pending	Pending
Dept. of Environmental Quality	Yes	4	Expired	Some	Yes
Dept of Game & Inland Fisheries	Yes	2	Expired	Some	Some
Dept. of Historic Resources	Yes	2	Expired	No	No
Marine Resources Commission	Yes	3	Expired	Yes	No
Va. Museum of Natural History	Expired	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	Pending	Pending
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	Expired	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	Expired	Not Due	Not Due
Motor Vehicle Dealers Board	Yes	0	No	N/A	N/A
Va. Dept. Of Transportation	Yes	5	Yes	Yes	Yes

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	2	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	1	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

Virginia Information Technologies Agency

Information Security Awareness Toolkit

Nakita Albritton, CISSP, CISA, PMP
Manager, Information Security/ COOP Coordinator

Presentation Content

- Toolkit Purpose
- Current Toolkit
- Future Toolkit

Toolkit Purpose

- To assist all agencies & localities in their efforts to enhance their Information Security Awareness Programs.
- To promote consistent delivery of information security best practices.
- To provide cost efficient information security awareness components/tools.

Current Toolkit Content

- Information Security Awareness Toolkit
  - Governor's Proclamation
  - Web Banner
  - Citizen's Awareness Banner
  - VITA Security Video and Posters
  - Agency Created Material
    - (Posters, Puzzles)
  - MS-ISAC Materials for Rebranding
    - (Calendars, Bookmarks, Brochures, Posters, Newsletter)

Virginia Information Technologies Agency

Governor's Proclamation

NOW, THEREFORE, I, Timothy M. Kaine, Governor of the Commonwealth of Virginia, do hereby proclaim the month of October 2008, as **INFORMATION SECURITY AWARENESS MONTH** in the Commonwealth of Virginia and encourage all the citizens of this Commonwealth to learn about information security and put that knowledge into practice in their homes, schools, workplaces, and businesses.

CERTIFICATE of RECOGNITION

By virtue of the authority vested by the Constitution in the Governor of the Commonwealth of Virginia, there is hereby officially recognized:

INFORMATION SECURITY AWARENESS MONTH

WHEREAS, many citizens, schools, libraries, businesses and other organizations use internet or technology for a variety of tasks, including accessing government services, keeping in contact with family and friends, managing finances, conducting research, enhancing education and conducting other business; and

WHEREAS, critical infrastructure sectors are increasingly reliant on information systems to provide their services including financial services, energy, telecommunications, transportation, health care, and emergency response systems; and

WHEREAS, information technology users and the information infrastructure daily face increasing threats of and loss of privacy from malicious attack by viruses as well as malware including spyware and adware; and

WHEREAS, each year there are significant financial and personal privacy losses due to identity theft and fraud; and

WHEREAS, the Multi-State Information Sharing and Analysis Center (MS-ISAC) was established in January 2003 to provide a collaborative mechanism to help states and local governments enhance cyber security; and the Virginia Information Technologies Agency provides a comprehensive approach to help enhance the information security of the Commonwealth; and

WHEREAS, there are national organizations, such as the non-profit National Cyber Security Alliance (NCSA), policymakers, government agencies, private sector companies, and non-profit entities helping consumers, businesses, educational leaders and our youth to protect themselves online; and

WHEREAS, each one of us plays an important role in securing our cyberspace. Awareness of computer security essentials will improve the security of the Commonwealth of Virginia's information infrastructure and economy; and

WHEREAS, the U.S. Department of Homeland Security, the Multi-State Information Sharing and Analysis Center and the National Cyber Security Alliance have declared October as National Cyber Security Awareness Month;

NOW, THEREFORE, I, Timothy M. Kaine, Governor of the Commonwealth of Virginia, do hereby proclaim the month of October 2008, as **INFORMATION SECURITY AWARENESS MONTH** in the Commonwealth of Virginia and encourage all the citizens of this Commonwealth to learn about information security and put that knowledge into practice in their homes, schools, workplaces, and businesses.

Governor

Secretary of the Commonwealth

Web Banner

INFORMATION SECURITY AWARENESS MONTH
INFORMATION SECURITY
STARTS WITH "YOU"
Think Before You Click
Keep your software and operating system up-to-date.
Keep your data safe and secure.
Use hard-to-guess passwords.

Citizen Awareness Banner

Citizen Awareness Banner

Due to the ever increasing threats posed by malware running on citizen computers, it is suggested that agencies utilize the provided banner on all Internet facing citizen and partner applications where authentication is required, or where any personally identifiable information may be exchanged between the agency and your customers. The banner looks like this when the code below is used:

The security of your personal information is important to us!

Diligent efforts are made to ensure the security of Commonwealth of Virginia systems. Before you use this Web site to conduct business with the Commonwealth, please ensure your personal computer is not infected with malicious code that collects your personal information. This code is referred to as a keylogger. The way to protect against this is to maintain current Anti-Virus and security patches.

For more information on protecting your personal information online, refer to the Citizens Guide to Online Protection.

Online Protection Glossary

Keylogging Letter Template

It has been brought to our attention by the United States Computer Emergency Readiness Team (US – CERT, http://www.us-cert.gov/) through the Multi-State Information Sharing and Analysis Center (MS-ISAC, http://www.msisac.org/) that a computer utilized around ***DATE TIME*** had been compromised with a software program that allowed capture of each keystroke. This computer was utilized to perform at least one transaction that contained information related to you…

Virginia Information Technologies Agency

VITA Security Video and Posters

Virginia Information Technologies Agency

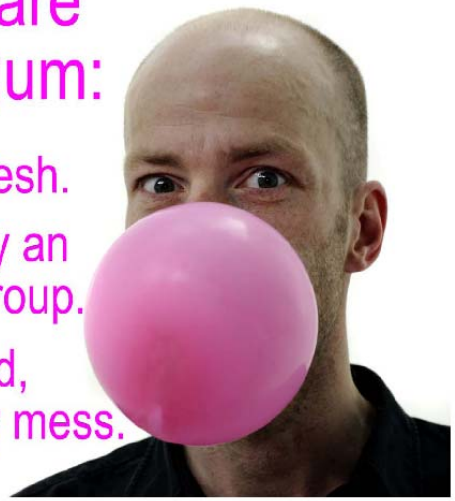
Agency Created Resource Material

Passwords are like bubble gum:

Strongest when fresh.

Should be used by an individual, not a group.

If left laying around, will create a sticky mess.



1	Across	You can turn the pages in a ____ in your hand or read one on-line.
2	Down	When creating a Password, do not use words from your favorite _<2>_, _<28 Down>_, hobby, recording artist, or _<29 Across>_.
3	Across	Before you throw something in the _____, ask yourself, "Is this something I would give to an unauthorized person or want to become publicly available?"
4	Across	Don't transmit any __ letters via email.
5	Across	___ , Peer-to-Peer, is an informal network that allows users to share other files with other users online.

_ or __<15 Across>__.

_____ - programs like viruses and spyware – Once there, they can steal information, send

ife: Keep it _____ . . . use a

eans of accessing the Internet at high speed

sites are blocked for one or more of the cross>_Risk, _<20 Down>_Risk, or <9>_Risk.

ife: Treat it like ____.

be at least ____ characters long.

can sneak onto your computer – often through then make copies of itself, quickly using up all

nternet space denoted by the function or type Current ones include ".com" for commercial tal ones, and ".org" for non-commercial

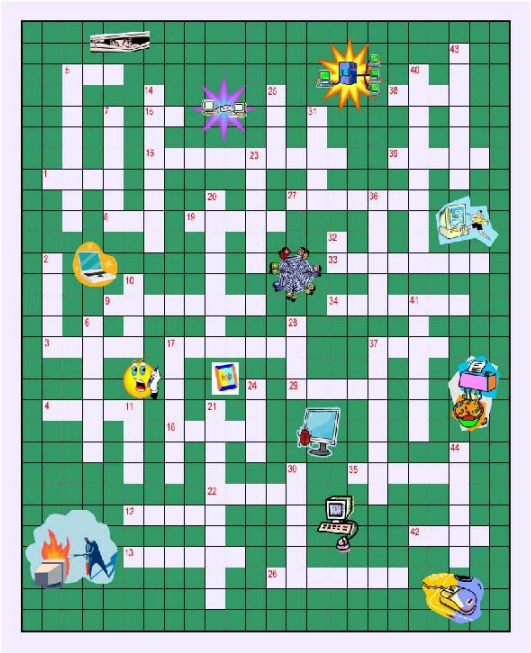
software that helps keep hackers o send out your personal rmission. It watches for outside stem and block communications n't permit.

Down>__or __<15>__.

ing of data into a secret code that can be read ode the information.

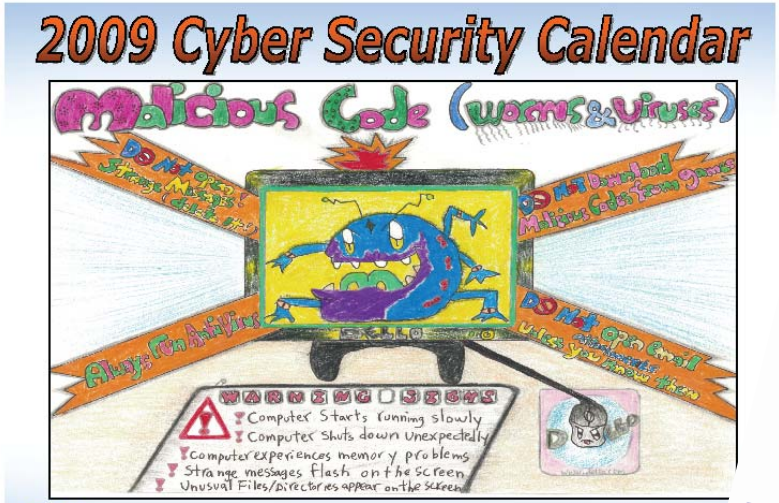
ram that may be installed on your computer nitor your use, send pop-up ads, redirect your es, or record keystrokes, which could lead to

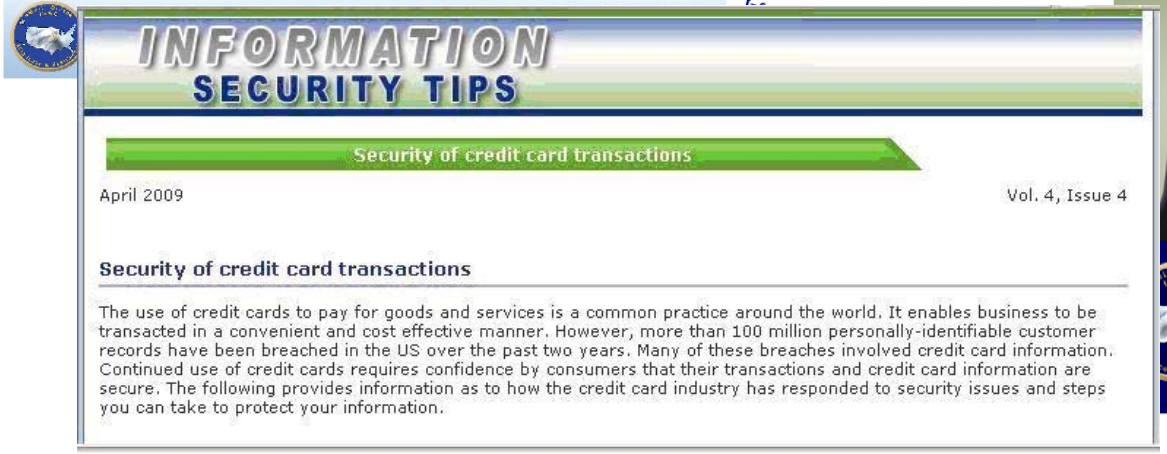
specific _____ line in your email.



Virginia Information Technologies Agency

MS-ISAC Resource Materials





INFORMATION SECURITY TIPS

Security of credit card transactions

April 2009 Vol. 4, Issue 4

Security of credit card transactions

The use of credit cards to pay for goods and services is a common practice around the world. It enables business to be transacted in a convenient and cost effective manner. However, more than 100 million personally-identifiable customer records have been breached in the US over the past two years. Many of these breaches involved credit card information. Continued use of credit cards requires confidence by consumers that their transactions and credit card information are secure. The following provides information as to how the credit card industry has responded to security issues and steps you can take to protect your information.

Future Toolkit Content

- New Design –Alignment of the Security Awareness Toolkit, Security Incident Management and the COV Resource Center
- Frequently Asked Questions
- Links to Additional .GOV Resources-For example VCU Twitter
- Additional Information Security Awareness Resources

Contact Us

For more information, please contact us at:

commonwealthsecurity@vita.virginia.gov

Virginia Information Technologies Agency

Security Incidents – Who, what, when, & why?

Michael Watson
Security Incident Management Director

We Have Previously Discussed…

- How to respond
  - Don't turn any systems off
    - If necessary pull the network plug from the system but leave it running
  - Contact Commonwealth Security
- Where to respond
  - Contact Commonwealth Security
    - Submit an incident using the Security Incident Reporting Form
    - Call the VCCC

What We Haven't Discussed…

- Security incidents & the role of the ISO in working with authorities
- Data breach the law & the standard
- Data breach notifications
- Keylogging notifications

Contacting the "Authorities"

- Who are the "authorities"?
  - Typically the Virginia State Police and/or the Federal Bureau of Investigations
- What do they need to be contacted for?
  - When the security incident involves a physical loss, the agency will need to contact the appropriate authorities
  - When the security incident involves a logical attack such as unauthorized access or other type of cyber attack, Commonwealth Security will contact the appropriate authorities & coordinate with the agency
- When in the response process should they be contacted?
  - For those security incidents that need involvement by law enforcement, they should be contacted immediately once the security incident has been confirmed
- Why does the agency need to contact the authorities for physical loss?
  - In the case of physical loss, COV Security is not in a good position to provide information about physical controls and procedures that are in place.

Data Breach – The Standard and the Law

- Who do I contact in the event of a data breach?
  - File a Commonwealth Security Incident report
  - Consult your OAG representative
- What is that I have to do?
  - The standard states that in the case of a data breach the affected parties must be notified
    - The standard is stricter than the law
- When should they be contacted?
  - As soon as possible
    - Speak with OAG first if it is necessary
  - If delay is necessary because it may impede a law enforcement investigation please get that in writing
- Why do I need to contact them if I'm pretty sure there wasn't a breach?
  - In the case that there is strong evidence a breach did not occur an exception request can be filed.

Data Breach Notifications

- Who do the notifications go to?
  - Those people whose personal information was released as part of the data breach
- What do I need to tell them?
  - A general description of what occurred and when
  - The type of personal information that was involved
  - What actions have been taken to protect the individual's personal information from further unauthorized access
  - Agency contact information
  - Actions the agency recommends that the individual take
  - A template letter is available as part of the COV Security Toolkit.
- When should they be contacted?
  - As soon as possible
  - If delay is necessary because it may impede a law enforcement investigation please get that in writing
- Why do I need to contact them?
  - The data owning agency is responsible for notifying those parties involved in a data breach

Keylogging Notifications

- Who do the notifications go to?
  - Parties who have a keylogger on their system
    - The agency also must have enough information to contact
- What do I need to tell them?
  - A general description of why you are contacting them
  - What actions are recommended to protect the individual's personal information from further unauthorized access
  - Where the information came from
  - A template letter is available as part of the COV Security Toolkit.
- When should they be contacted?
  - As soon as possible
  - Contact Commonwealth Security with how many people the agency was able to contact
- Why do I need to contact them?
  - The standard requires agencies to contact those parties known to have keylogs on them in accordance with section 9.5.2.4 of the SEC501 standard.

Virginia Information Technologies Agency

July 2009 Cyber Security Attacks

Michael Watson
Security Incident Management Director

Upcoming Events

UPCOMING EVENTS! Future 2009 ISOAG's

All currently from 1:00 – 4:00 pm at CESC though working with the Science Museum (thanks!)

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

Wednesday, August 12

Wednesday, September 9

Tuesday, October 6

Virginia Information Technologies Agency

Information Security System Association

ISSA meets on the second Wednesday of every month

- **DATE: Wednesday July 15th**
- **LOCATION: Maggiano's Little Italy, 11800 W. Broad St., #2204, Richmond/Short Pump Mall**
- **TIME: 11:30 - 1:30pm. Presentation starts at 11:45 & Lunch served at 12.**
- **Shelia Teague, Supervisory Special Agent, FBI will provide an overview on "FBI-sponsored Regional Computer Forensics Laboratory (RCFL) program."**
- **COST: ISSA members: $10 & Non-Members: $20**
- **RSVP: With Robert Thomas**

Upcoming Events – ITIB July 24

The Information Technology Investment Board (ITIB) will meet on July 24, 2009 at the Commonwealth Enterprise Solutions Center

FACTA Red Flag Requirements *NEW DATE

Implementation Date: **August** 1st, 2009

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

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/

Any Other Business ??????

ADJOURN

THANK YOU FOR ATTENDING!!