Virginia Information Technologies Agency

2008 Commonwealth of Virginia Information Security Report

In keeping with our commitment to cost savings,
this report was produced in limited quantities, in-house,
utilizing an existing color printer and binding equipment.

Prepared and Published by:
Virginia Information Technologies Agency

Comments and recommendations on the
Commonwealth Information Security 2008 Annual Report
from all interested parties are welcomed and encouraged.
Suggestions may be conveyed electronically to
VITASecurityServices@VITA.Virginia.Gov

Please submit written correspondence to:

Lemuel C. Stewart Jr.
Chief Information Officer of the Commonwealth
Virginia Information Technologies Agency
Commonwealth Enterprise Solutions Center
11751 Meadowville Lane
Chester, VA 23836
cio@vita.virginia.gov

Virginia Information Technologies Agency

Table of Contents

Table of Contents

Virginia Information Technologies Agency

2008 Information Security Report

Executive Summary

This 2008 Commonwealth of Virginia Information Security Report is the first annual report to the Governor and the General Assembly and will establish a baseline for assessing the strength of the information security programs of the 88 independent and executive branch agencies, including higher education except for the four charter universities (College of William and Mary, University of Virginia, Virginia Commonwealth University and the Virginia Polytechnic Institute and State University). The detailed listing of agencies and specific security information points can be found in Appendix I.

The Commonwealth Information Security Program is comprised of the information security work done collectively at the Commonwealth level as well as all of the individual agency information security programs. The Commonwealth Information Security Program is only as sound as the sum of these collective parts and therefore the individual agency programs are of great importance.

This report is based on data points as of November 14, 2008, available to the Chief Information Security Officer (CISO) on behalf of Chief Information Officer (CIO) as a result of fulfilling the CIO responsibilities under §2.2-2009 of the Code of Virginia, *Additional duties of the CIO relating to security of government information.* This data includes whether the agency head has:

- Designated an Information Security Officer within the past two years
- Submitted a Security Audit Plan for Sensitive Systems
- Provided Corrective Action Plans for completed Security Audits
- Supplied Quarterly Updates for Corrective Action Plans
- Had personnel attend a voluntary Information Security Orientation session (Attendance is not required but indicates agencies that have taken extra action to learn how to build an effective agency information security program.)

We also utilized the reports from the Auditor of Public Accounts (APA) and consulted with APA staff concerning the preliminary results of their SJR 51 (2006) follow-up review. We analyzed the security incidents reported by executive branch agencies as required by §2.2-603.F. In addition, we utilized information from the Commonwealth Information Technology Infrastructure Partnership relative to operational security changes with network transformation as well as the status of information technology disaster recovery plans.

For this 2008 report, we conclude that most every agency is making progress in establishing information security programs adequate to safeguard the information of the Commonwealth but that more work is needed particularly in the area of security audits of sensitive systems and disaster recovery planning for those systems sensitive relative to availability. Traditionally, these areas have not been consistently planned and budgeted for when developing and implementing sensitive systems. The comprehensive assessment can

be found in the Analysis Section and the detailed information by agency is available in Appendix I.

The mission of having a strong Commonwealth Information Security Program is a journey without end as the threats and defenses change daily as the underlying information transmission and storage methods change. However, we believe that the Commonwealth of Virginia is on the right path and the accuracy of the path was recognized in September 2008 when the Commonwealth of Virginia was selected by the National Association of State Chief Information Officers as the winner of the 2008 Recognition Awards for Outstanding Achievement in the Field of Information Technology in the category of Security and Privacy for the entry *Interlocking Spheres of Collaborative Protection. http://www.nascio.org/awards/2008Awards/securityPrivacy.cfm*

Background

The 2008 Commonwealth of Virginia Information Security Report is the first annual report to the Governor and the General Assembly as required by Section C of the Code of Virginia, §2.2-2009, *Additional duties of the CIO relating to security of government information*. As such, the 2008 report will establish a baseline for assessing the strength of the information security programs that independent and executive branch agencies, including higher education, have established to protect Commonwealth information. The scope of this report is limited to the 88 independent and executive branch agencies, including higher education except for the four charter universities (College of William and Mary, University of Virginia, Virginia Commonwealth University and the Virginia Polytechnic Institute and State University).

A previous assessment of information security programs in the Commonwealth to include all branches of government was required by Senate Joint Resolution No. 51 (SJR 51), which passed during the 2006 General Assembly Session, directing the APA *"… to study the adequacy of the security of state government databases and data communications from unauthorized uses."* The resolution required the study to be completed by November 2006. The APA completed the study and issued *A Review of Information Security in the Commonwealth of Virginia, Report on Audit as of December 1, 2006,* in December 2006. In the report the APA concluded that 80% of Commonwealth agencies and institutions had either an inadequately documented information security program or no documented information security program. One of the four recommendations in the report was: *"The General Assembly may wish to consider granting the CIO authority over the other branches of government's information security programs. In addition, agencies and institutions need to develop a mutual comprehensive information security program to protect information in the Commonwealth."*

As a result of the recommendation in the SJR 51 report, Senate Bill 1029 was passed in the 2007 General Assembly session to amend the Code of Virginia, §2.2-2009, *Additional duties of the CIO relating to security of government information*, to clarify "… that policies, procedures, and standards developed for information security will apply to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education."

Senate Bill 1029 also held a new requirement that: *"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."*

Due to a lack of resources and after deliberation with APA, VITA moved forward to provide the requisite report utilizing available information. Accordingly, this report is based on data points available to the Chief Information Security Officer (CISO) on behalf of Chief Information Officer (CIO) as a result of fulfilling the CIO responsibilities under §2.2-2009, *Additional duties of the CIO relating to security of government information.*

CIO responsibilities under §2.2-2009 include such items as:

- Directing the development of policies, procedures and standards for assessing security risks
- Determining the appropriate security measures and performing security audits of government electronic information
- Developing policies, procedures, and standards that address the scope of security audits and the frequency of such security audits
- Making the annual report to the Governor and General Assembly regarding agencies' information security programs
- Receiving reports of security incidents while taking such actions as are necessary, convenient or desirable to ensure the security of the Commonwealth's electronic information and confidential data.

To fulfill his information security responsibilities under §2.2-2009, the CIO has established a Commonwealth Security and Risk Management directorate led by the Commonwealth CISO.

Approach

As stated previously, this report is not based on reviews of individual agency's information security programs, but rather is based on an analysis of available data and information as of November 14, 2008. The Information Security Policy, Standard and Audit Standard require certain data to be reported by agencies to the Commonwealth CISO and this data serves as the primary basis for the individual agency component of this report. This data includes whether an agency head has:

- Designated an Information Security Officer within the past two years
- Submitted a Security Audit Plan for Sensitive Systems

- Provided Corrective Action Plans for completed Security Audits
- Supplied Quarterly Updates for Corrective Action Plans
- Had personnel attend a voluntary Information Security Orientation session (Attendance is not required but indicates agencies that have taken extra action to learn how to build an effective agency information security program)

The detailed listing of agencies and specific security data points can be found in Appendix I. We also utilized the reports from the APA and consulted with them concerning the preliminary results of their SJR 51 follow-up review. We analyzed the security incidents reported by executive branch agencies as required by §2.2-603.F. In addition, we utilized information from the Commonwealth Information Technology Infrastructure Partnership relative to operational security changes with network transformation as well as the status of information technology disaster recovery planning that relate.

2008 Commonwealth of Virginia Information Security Program

Commonwealth – Wide Information Security Efforts

Legislative Foundation

The General Assembly has provided the legislative component of the foundation of the Commonwealth's Information Security Program by enacting two key laws aimed at the Commonwealth of Virginia's Information Security Program. This legislation requires the executive branch agency heads to report information security incidents to the CIO within 24 hours (§2.2-603.F) and requires the CIO to promulgate the information security policies and standards of the Commonwealth including the scope and frequency of security audits, issue an annual report on information security to the Governor and General Assembly and receive the security incident reports and take such action as needed to protect Commonwealth information (§2.2-2009).

Executive Branch Foundation

The Governor has provided the key executive branch component for the Commonwealth of Virginia's Information Security Program foundation by issuing Executive Order 43 (2007) - *Protecting the Security of Sensitive Individual Information in Executive Branch Operations,* which empowers the Secretary of Technology "… to coordinate and oversee all efforts within the executive branch, in every secretariat, agency, institution, board, commission, and other entity to ensure compliance with established Commonwealth Information Security Policies and Standards so that protection of sensitive individual information is appropriate and that privacy is respected to the maximum extent possible." The Secretary of Technology, in collaboration with his colleagues in the Executive Branch, has worked to advance information security policies and procedures as noted in his second annual report on those efforts to the Governor in October, 2008. Governor Kaine also issued proclamations in both 2007 and 2008 designating October as Information Security Awareness Month in concert with national efforts sponsored by the Department of Homeland Security.

Information Security Policies, Standards and Guidelines

The Information Technology Investment Board (ITIB), upon the recommendation of the CIO, has approved the Commonwealth Information Security Policy and four Information Security Standards to assist agencies in building and documenting their agency information security program. The policy is written for agency heads summarize the overall agency requirements for developing and documenting an adequate agency information security program and to highlight the agency head's responsibilities. The four standards provide greater depth on the development and documentation of an agency information security program and address the topics of general information security, information security audits, removal of Commonwealth data from surplus computer hard drives and electronic media, and the use of non-Commonwealth devices for telework. If an agency has a way of conducting business that does not comply with the requirements, there is an exception process available.

In addition to providing the Commonwealth Information Security Policy and Standards with which compliance is mandatory, the ITIB has approved optional use guidelines for seven of the nine major components of the Information Security Standard Guidelines for the remaining two components are planned to be approved in the third quarter of Fiscal Year 2009. The guidelines provide agencies with additional information on compliance with the Information Security Standard and provide business cases and templates as an assist to agencies with limited resources.

Commonwealth Information Security Council

The Commonwealth Information Security Council has been established and consists of 11 Information Security Officers who have come together to strengthen the information security posture in the Commonwealth. The members come from the independent agencies, judicial branch, and executive branch of government, including higher education. They meet monthly as a council to provide direction for the Commonwealth's Information Security Program and also have formed committees around the following four initiatives:

- Encryption
- Identity and access management
- Making information security an executive management priority
- Small agency outreach

The council's work includes such accomplishments as developing a Commonwealth of Virginia Identity and Access Management Trust Model, providing key information security messages for each week in October for inclusion in the Governor's Leadership Communiqué, giving input on data breach notification requirements and early adoption, and developing a Business Impact Analysis Tool that the Virginia Department of Emergency Management has included in the Continuity of Operations Plan Library.

Commonwealth Information Security Officers Advisory Group

The Commonwealth of Virginia's Information Security Advisory Group (ISOAG) is a very active group open to all state and local government personnel interested in improving the information security posture of the Commonwealth. The members share best practices and knowledge through regular monthly meetings and timely security alerts provided by Commonwealth Security. The group regularly interacts with national and state information

security experts and members are notified of upcoming cost-effective information security training opportunities. In fiscal year 2007, there were approximately 50 persons on the listing and six ISOAG meetings with an average attendance of 66.7 persons per meeting. In fiscal year 2008, the listing grew to about 200 persons and 12 ISAOG meetings were held with an average attendance of 88.5 persons. For the first four months of fiscal year 2009, the listing has grown to 322 persons and four meetings have been held with attendance averaging 102 persons per meeting. We expect this increase in the ISOAG listing and meeting attendance to continue and look forward to this growing trend.

Information Security Orientation

Another Commonwealth program established to assist government personnel interested in learning about building and documenting an information security program in the Commonwealth is Information Security Orientation. This session provides participants with a background on why we care about security of information, what resources are available, and a walk through the actual steps in building and documenting an agency program utilizing the Commonwealth Information Security Policy, Standards and Guidelines. Commonwealth Security began the Information Security Orientation programs in March, 2007 and has held 25 sessions with 238 people attending, including 231 from 65 Commonwealth independent and executive branch agencies, including higher education; two persons from the legislative branch and two from the judicial branch, two from two localities, and one person from a charter university (College of William & Mary). As with the ISOAG meetings, we anticipate the Information Security Orientation program will continue to flourish and expand.

Commonwealth Information Security Incident Management

The Code of Virginia, *§ 2.2-603. Authority of agency directors.* F. states: *"The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in § 2.2-2005, all known security incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other security incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within (24) twenty-four hours from when the department discovered or should have discovered their occurrence."* As stated, the security incident reporting requirement does not apply to the independent, judicial and legislative agencies.

The Commonwealth Security Incident Team classifies each incident into a category based on the purpose of the attack. The majority of the security incidents reported are categorized into three categories:

- Malware used to modify or obtain Commonwealth information
- Unauthorized physical access to Commonwealth information
- A user disclosing Commonwealth information to an unauthorized party

The security incidents that are part of the malware category used malicious code to implement or facilitate activity to modify or obtain Commonwealth information. Malicious code includes software such as viruses, spyware, key loggers, etc. Unauthorized physical access to Commonwealth information includes security incident where unauthorized parties

have physical access to Commonwealth information such as information on lost laptops. Security incidents where users disclose Commonwealth information occur when information is disclosed to unauthorized parties such as Commonwealth information directed to unauthorized parties in either paper or electronic format.

During the period of July 2007 to September 2008, 93 information security incidents were reported. Of those 93 security incidents, 30 (32%) were classified as using malicious software to modify or obtain Commonwealth information, with the majority of these attacks being Web site defacements, specifically the posting of malicious content on Web servers, and the installation of malicious software on computers. The security incidents that involved unauthorized physical access to Commonwealth information primarily were due to lost or stolen laptops and accounted for 37 (40%) of the security incidents. Accidental information disclosure, keylogging involving Commonwealth equipment, and phishing attempts targeted at Commonwealth personnel accounted for potential information disclosure in 15 (16%) of the security incidents. Eleven (12%) of the security incidents logged were classified as non-security incidents or unsuccessful attempts after a full investigation.

In addition to security incidents Commonwealth Security tracks keylogging events reported by the United States Computer Emergency Readiness Team. Each keylogging event reported to Commonwealth Security is analyzed for how it impacts the Commonwealth. When there is enough data within the event to associate it with a citizen or Commonwealth employee, the user involved is notified of the keylogging incident by the data owning agency and provided with information on what they should do to protect themselves. Between March 2007 and October 2008 there were at total of 14,944 keylogging events provided to Commonwealth Security that involved 1,252 citizens.

Commonwealth Operational Security

From an operational security perspective, the largest initiative is found in the Commonwealth Information Technology Infrastructure Partnership. The Commonwealth Enterprise Solutions Center was opened in Chesterfield County in 2007 providing a Tier III data center with a high level of physical and logical access security to replace the Commonwealth's aged data center that had been located in downtown Richmond next to the expressway and the river, with a parking deck at the core of the data center and a public café on the floor below the data center. Additionally, the Southwest Enterprise Solutions Center also was opened in Lebanon, Russell County, providing the Commonwealth with its first complete back-up data center and providing economic development and job opportunities in Southwest Virginia.

Agencies either have undergone or will undergo transformation of their personal computers, servers, networks and messaging as a result of the Commonwealth Information Technology Infrastructure Partnership. A recent paper drafted by the Commonwealth Information Technology Infrastructure Partnership states: "The [Commonwealth Information Technology Infrastructure Partnership] security team has numerous and redundant capabilities that provide the firepower needed to robustly protect Commonwealth assets. Being part of the security preventive and detective processes will provide a significant enhancement to any agency's security posture. Given the sophistication of today's cyber criminals, it is essential that Commonwealth agencies perform due diligence and exercise due care to protect and safeguard Commonwealth citizens' vital data. Besides providing a high degree of cyber protection to Commonwealth, being part of the

[Commonwealth Information Technology Infrastructure Partnership] is a positive business decision in that the [Commonwealth Information Technology Infrastructure Partnership] will provide for the state-of-the-art security tools needed to protect Commonwealth data." An analysis of existing information technology disaster recovery plans of agencies by the Commonwealth Information Technology Infrastructure Partnership indicates that many agencies do not have adequate IT disaster recovery plans due primarily to lack of resources.

Agency Information Security Efforts - See Appendix II for revisions

Particularly since the issuance of the SJR 51 report by APA, agencies have been working diligently to build and document their information security programs. Our analysis of the specific data points reviewed indicates progress has been made but more work remains.

Designation of an Information Security Officer Within the Past Two Years

A cornerstone step in building an information security program is the agency head's designation of an Information Security Officer (ISO) every two years. The agency's ISO is responsible for maintaining a liaison with the CISO and developing and managing the agency's information security program. Of the 88 Agencies, 80 (91%) agencies have designated an ISO within the past two years and 8 (9%) have not.

Attendance at Voluntary Information Security Orientation session

Attendance at Information Security Orientation is not required but indicates that agencies have taken extra action to learn how to build an effective agency information security program. A total of 65 (74%) agencies have sent 231 persons to Information Security Orientation and 23 (26%) have not had a representative attend.

Submission of a Security Audit Plan for Sensitive Systems

Agency heads must take action to have each sensitive system audited at least once every three years and submit the plan for doing so to the CISO. Placing reliance on any existing audit activity is encouraged. A security audit is an independent review to assess the effectiveness of the controls management implemented to safeguard the information processed by a system. This includes compliance with the Commonwealth Information Security Standard and any relevant federal or state laws or regulations. Of the 88 agencies, 56 (64%) have submitted a Security Audit Plan, 29 (33%) have not submitted a Security Audit Plan, and 3 (3%) have a current exception on file.

Provided Corrective Action Plans for Completed Security Audits

For security audits that have been completed, corrective action plans are required to be submitted to VITA quarterly identifying whether the agency head agrees or disagrees with the audit finding and, if in agreement, the actions planned to correct the vulnerabilities identified by the audit. If the agency head disagrees with the finding a statement of the agency's position must be provided. Of the 88 agencies, 11 (13%) submitted all corrective action plans, eight (9%) have submitted some corrective action plans, 16 (18%) have not submitted any of the corrective action plans due, and 21 (24%) have no corrective action plans due. For 29 (33%) agencies, this is not applicable as they have not yet submitted an audit plan and 3 (3%) have an exception on file.

Supplied Quarterly Updates for Corrective Action Plans

For any completed security audits for which corrective action plans have been submitted, agencies are required to submit the status of outstanding corrective actions quarterly until the corrective action has been completed. Eight (9%) agencies have submitted all updates, four (5%) agencies have submitted some updates, two (2%) agencies have not submitted any updates due, 26 (30%) agencies have no updates due, and for 48 (54%) agencies quarterly updates are not applicable since they have not submitted a security audit plan and/or a corrective action plan that was due.

The detailed listing of agencies and specific security data points can be found in Appendix I. We also utilized the reports from APA and consulted with APA staff concerning the preliminary results of their SJR 51 follow-up review, which indicate that progress in documenting agency security programs has been made but implementation of the security program is lagging somewhat. We analyzed the security incidents reported by executive branch agencies as required by §2.2-603.F. In addition, we utilized information from the Commonwealth Information Technology Infrastructure Partnership relative to operational security changes with network transformation and the status of information technology disaster recovery planning that relate.

Conclusion

Building and strengthening Commonwealth of Virginia's information security is a collaborative effort. The foundation for the Commonwealth's Information Security Program is laid by collaborative efforts of the General Assembly, Governor, ITIB, Secretary of Technology and CIO. Building on that foundation is a collaborative effort between agency heads, agency information security officers, agency technical support staff, every end user and our localities. As we increasingly strive to deliver government services digitally, the Commonwealth Information Security Program must include our citizens as well. The increasing reports of citizens using computers with keystroke logging malware installed when they utilize Commonwealth websites to obtain government services is alarming. In the future we plan to work to educate citizens on how to protect themselves while encouraging them to utilize our digitally delivered services.

Supporting these efforts is the Information Security Orientation, the efforts of our Commonwealth Information Security Council and Commonwealth Information Security Officers Advisory Group, and components of the Office of Commonwealth Preparedness's programs and those related to the Information Technology Disaster Recovery Component of the Virginia Department of Emergency Management's Continuity of Operations planning efforts. Commonwealth Security continues to promote a number of information security awareness meetings and training sessions in an effort to educate and foster collaboration among information security professionals across the Commonwealth. Attendance and participation in these meetings and training sessions continues to grow, demonstrating agency commitment to their information security programs.

For this 2008 report, we conclude that most every agency is making progress in establishing information security programs adequate to safeguard the information of the Commonwealth. However, more work is needed -- particularly in the area of security audits of sensitive systems and disaster recovery planning for those systems sensitive

relative to availability. Traditionally, these areas have not been consistently planned and budgeted for when developing and implementing sensitive systems.

The eight agencies without a designated Information Security Officer primarily are small agencies that need additional assistance in developing and documenting their information security program. The Appropriations Act passed by the 2008 General Assembly provided the Department of Accounts with two full-time equivalent positions and related funding to assist small agencies in building and documenting their information security programs so the coming year should bring some progress in this area.

Maintaining a strong Commonwealth Information Security Program is a journey without end as the threats to our information and our defenses change constantly. However, we believe that the Commonwealth of Virginia is on the right path and the accuracy of the path was recognized in September 2008 when the Commonwealth of Virginia was selected by the National Association of State Chief Information Officers as the winner of the 2008 Recognition Awards for Outstanding Achievement in the Field of Information Technology in the category of Security and Privacy for its entry *Interlocking Spheres of Collaborative Protection*. The NASCIO award recognized the level of collaboration involved with our partners –customers, state and local leaders at all levels of government, the private sector and independent organizations. Virginia could not be successful without these ongoing relationships.

Appendix I - Detailed Information by Agency - See Appendix II for revisions

Legend

Acronyms:
ISO – Information Security Officer
IS – Information Security

ISO Designated

Yes - The agency head has designated an ISO for the agency within the past two years.
No - The agency head has NOT designated an ISO for the agency within the past two years.

Attended IS Orientation

The number indicates how many agency personnel have attended the optional Information Security Orientation sessions indicating they are taking additional, voluntary action to improve security at their agency akin to "Extra Credit!"

Security Audit Plan Received

Yes - The agency head has submitted a Security Audit Plan for systems classified as sensitive based on confidentiality, integrity or availability.
No - The agency head has NOT had a Security Audit Plan submitted for systems classified as sensitive based on confidentiality, integrity or availability.
Exception – The agency head has submitted and the CISO has approved a temporary exception on file with VITA to allow time for developing the security audit plan.

Corrective Action Plans Received & Quarterly Updates Received

Yes - The agency head has submitted an adequate Corrective Action Plan/Quarterly Update for Security Audits scheduled to have been completed.
Some - The agency head has submitted an adequate Corrective Action Plan/Quarterly Update for some but NOT all Security Audits scheduled to have been completed.
No - The agency head has NOT submitted an adequate Corrective Action Plan/Quarterly Update for Security Audits scheduled to have been completed.
Not Due - The agency head did not have Security Audits scheduled to be completed or has submitted a corrective action plan within the last quarter and no quarterly update is due.
N/A - Not applicable as the agency head has not submitted an Information Security Audit Plan or a Corrective Action Plan that was due.

Agency Information Security Datapoints

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
1	Administration	Human Resource Council	YES	0	NO	N/A	N/A
2	Administration	Dept. of General Services	YES	0	YES	NO	N/A
3	Administration	Dept. of Human Res. Mgmt	YES	0	YES	Not Due	Not Due
4	Administration	Dept. Min. Bus. Enterprise	YES	2	NO	N/A	N/A
5	Administration	Employee Dispute Resolution	YES	3	YES	Not Due	Not Due
6	Administration	Compensation Board	NO	1	YES	NO	N/A
7	Administration	State Board of Elections	NO	0	YES	NO	N/A
8	Agriculture & Forestry	Dept. of Forestry	YES	1	YES	Not Due	Not Due
9	Agriculture & Forestry	Va. Dept. of Ag. & Cons. Serv.	YES	30	YES	YES	YES
10	Commerce & Trade	Dept of Business Assistance	YES	2	NO	N/A	N/A
11	Commerce & Trade	Board of Accountancy	YES	1	YES	NO	N/A
12	Commerce & Trade	Dept. of Housing & Community Development	YES	1	YES	Some	Not Due
13	Commerce & Trade	Dept. of Mines, Minerals & Energy	YES	1	YES	Some	NO
14	Commerce & Trade	Dept. of Labor & Industry	YES	3	NO	N/A	N/A
15	Commerce & Trade	Dept. of Professional & Occupational Regulation	YES	1	YES	NO	N/A
16	Commerce & Trade	Tobacco Indemnification Commission	YES	0	NO	N/A	N/A
17	Commerce & Trade	Va. Employment Commission	YES	3	YES	NO	N/A
18	Commerce & Trade	Va. Economic Development Partnership	YES	0	NO	N/A	N/A
19	Commerce & Trade	Va. Housing Development Authority	NO	1	NO	N/A	N/A
20	Commerce & Trade	Va. National Defense Industrial Authority	NO	0	NO	N/A	N/A
21	Commerce & Trade	Va. Resources Authority	NO	0	NO	N/A	N/A
22	Commerce & Trade	Va. Racing Commission	YES	2	YES	Not Due	Not Due
23	Education	Dept. of Education	YES	1	YES	NO	N/A

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
24	Education	Frontier Culture Museum of Va.	YES	0	NO	N/A	N/A
25	Education	Gunston Hall	YES	0	NO	N/A	N/A
26	Education	Jamestown Yorktown Foundation	YES	0	YES	NO	N/A
27	Education	Library of Va.	YES	1	YES	Not Due	Not Due
28	Education	State Council of Higher Education for Va.	YES	0	NO	N/A	N/A
29	Education	Science Museum of Va.	YES	0	NO	N/A	N/A
30	Education	Va. Commission for the Arts	YES	0	NO	N/A	N/A
31	Education	Va. Museum of Fine Arts	YES	2	YES	YES	Not Due
32	Education	Christopher Newport University	YES	0	YES	Not Due	Not Due
33	Education	George Mason University	YES	1	YES	Some	YES
34	Education	James Madison University	YES	0	YES	YES	Some
35	Education	Longwood University	YES	1	YES	YES	YES
36	Education	Norfolk State University	YES	2	NO	N/A	N/A
37	Education	Old Dominion University	YES	1	YES	YES	YES
38	Education	Radford University	YES	0	YES	YES	YES
39	Education	University of Mary Washington	YES	1	YES	NO	N/A
40	Education	Va. Community College System	YES	36	YES	Some	NO
41	Education	Virginia Military Institute	YES	0	YES	NO	N/A
42	Education	Virginia State University	YES	3	YES	Not Due	Not Due
43	Finance	Dept. of Accounts	YES	4	NO	N/A	N/A
44	Finance	Dept. of Planning & Budget	YES	2	NO	N/A	N/A
45	Finance	Dept. of Taxation	YES	1	YES	Some	YES
46	Finance	Dept. of Treasury	YES	2	YES	NO	N/A
47	Health & Hum. Res.	Dept. of Health Professions	YES	0	YES	Not Due	Not Due
48	Health & Hum. Res.	Dept. of Medical Assistance Services	YES	6	YES	Some	Not Due
49	Health & Hum. Res.	Dept. of Mental Health, Mental Retardation, & Substance Abuse Services	YES	15	YES	Not Due	Not Due
50	Health & Hum. Res.	Dept. of Rehabilitative Services	YES	0	YES	NO	N/A

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
51	Health & Hum. Res.	Dept. of Social Services	YES	2	YES	NO	N/A
52	Health & Hum. Res.	Tobacco Settlement Foundation	NO	0	NO	N/A	N/A
53	Health & Hum. Res.	Va. Dept. for the Aging	YES	1	YES	Not Due	Not Due
54	Health & Hum. Res.	Va. Dept. of Health	YES	3	YES	YES	YES
55	Natural Resources	Dept. of Conservation & Recreation	YES	1	YES	Some	Not Due
56	Natural Resources	Dept. of Environmental Quality	YES	4	YES	YES	Some
57	Natural Resources	Dept of Game & Inland Fisheries	YES	1	NO	N/A	N/A
58	Natural Resources	Dept. of Historic Resources	YES	2	YES	Not Due	Not Due
59	Natural Resources	Marine Resources Commission	YES	1	YES	YES	YES
60	Natural Resources	Va. Museum of Natural History	YES	1	NO	N/A	N/A
61	Public Safety	Alcoholic Beverage Control	YES	1	YES	YES	Some
62	Public Safety	Commonwealth's Attorney's Services Council	NO	0	NO	N/A	N/A
63	Public Safety	Dept. of Criminal Justice Services	YES	2	YES	NO	N/A
64	Public Safety	Dept. of Fire Programs	YES	3	YES	Not Due	Not Due
65	Public Safety	Dept. of Forensic Science	YES	1	YES	Not Due	Not Due
66	Public Safety	Dept. of Juvenile Justice	YES	3	YES	NO	N/A
67	Public Safety	Dept. of Military Affairs	NO	1	NO	N/A	N/A
68	Public Safety	Dept. of Corrections	YES	3	YES	Some	Not Due
69	Public Safety	Dept. of Correctional Education	YES	1	NO	N/A	N/A
70	Public Safety	Dept. of Veterans Services	YES	1	NO	N/A	N/A
71	Public Safety	Va. Dept. of Emergency Management	YES	1	NO	N/A	N/A
72	Public Safety	Va. State Police	YES	3	YES	Not Due	Not Due
73	Technology	The Ctr for Innovative Tech.	YES	1	YES	NO	N/A
74	Technology	Va. Info. Technologies Agency	YES	33	YES	Not Due	Not Due
75	Transportation	Dept. of Motor Vehicles	YES	2	YES	Not Due	Not Due
76	Transportation	Dept. of Aviation	YES	2	NO	N/A	N/A

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates
77	Transportation	Dept. of Rail & Public Trans.	YES	1	YES	Not Due	Not Due
78	Transportation	Motor Vehicle Dealers Board	YES	0	NO	N/A	N/A
79	Transportation	Va. Dept. Of Transportation	YES	5	YES	YES	Some
80	Independent	Indigent Defense Council	YES	4	NO	N/A	N/A
81	Independent	State Lottery Dept.	YES	2	NO	N/A	N/A
82	Independent	State Corporation Commission	YES	3	YES	Not Due	Not Due
83	Independent	Va. College Savings Plan	YES	3	YES	Not Due	Not Due
84	Independent	Va. Office for Protection & Advocacy	YES	1	EXCEPTION	EXCEPTION	N/A
85	Independent	Va. Retirement System	YES	2	YES	Not Due	Not Due
86	Independent	Va. Workers' Compensation Commission	YES	1	EXCEPTION	EXCEPTION	N/A
87	N/A	Office of the Governor	YES	3	EXCEPTION	EXCEPTION	N/A
88	N/A	Office of the Attorney General	YES	1	YES	Not Due	Not Due
	TOTALS		Y- 80 (91%) N- 8 (9%)	231 from 65 (74%) of 88 agencies	Y-56 (64%) N – 29 (33%) Exceptions – 3 (3%)	Y-11 (13%) Some – 8 (9%) N – 16 (18%) Not Due – 21 (24%) N/A – 29 (33%) Exceptions – 3 (3%)	Y-8 (9%) Some – 4 (5%) N – 2 (2%) Not Due – 26 (30%) N/A – 48 (54%)

Appendix II – Revised Detailed Information by Agency as of November 14, 2008

Legend

Acronyms:
ISO – Information Security Officer
IS – Information Security

ISO Designated

Yes - The agency head has designated an ISO for the agency within the past two years.
No - The agency head has NOT designated an ISO for the agency within the past two years.

Attended IS Orientation

The number indicates how many agency personnel have attended the optional Information Security Orientation sessions indicating they are taking additional, voluntary action to improve security at their agency akin to "Extra Credit!"

Security Audit Plan Received

Yes - The agency head has submitted a Security Audit Plan for systems classified as sensitive based on confidentiality, integrity or availability.
No - The agency head has NOT had a Security Audit Plan submitted for systems classified as sensitive based on confidentiality, integrity or availability.
Exception – The agency head has submitted and the CISO has approved a temporary exception on file with VITA to allow time for developing the security audit plan.

Corrective Action Plans Received & Quarterly Updates Received

Yes - The agency head has submitted an adequate Corrective Action Plan/Quarterly Update for Security Audits scheduled to have been completed.
Some - The agency head has submitted an adequate Corrective Action Plan/Quarterly Update for some but NOT all Security Audits scheduled to have been completed.
No - The agency head has NOT submitted an adequate Corrective Action Plan/Quarterly Update for Security Audits scheduled to have been completed.
Not Due - The agency head did not have Security Audits scheduled to be completed or has submitted a corrective action plan within the last quarter and no quarterly update is due.
N/A - Not applicable as the agency head has not submitted an Information Security Audit Plan or a Corrective Action Plan that was due.

Revised Agency Information Security Datapoints as of November 14, 2008

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Score (Points)
1	Administration	Human ~~Resource~~ Rights Council	YES	0	NO	N/A	N/A	
2	Administration	Dept. of General Services	YES	0	YES	NO	N/A	
3	Administration	Dept. of Human Res. Mgmt	YES	0	YES	Not Due	Not Due	
4	Administration	Dept. Min. Bus. Enterprise	YES	2	NO	N/A	N/A	
5	Administration	Employee Dispute Resolution	YES	3	YES	Not Due	Not Due	
6	Administration	Compensation Board	~~NO~~ YES	1	YES	NO	N/A	
7	Administration	State Board of Elections	NO	0	YES	NO	N/A	
8	Agriculture & Forestry	Dept. of Forestry	YES	1	YES	Not Due	Not Due	
9	Agriculture & Forestry	Va. Dept. of Ag. & Cons. Serv.	YES	30	YES	YES	YES	
10	Commerce & Trade	Dept of Business Assistance	YES	2	~~NO~~ YES	~~N/A~~ Not Due	~~N/A~~ Not Due	
11	Commerce & Trade	Board of Accountancy	YES	1	YES	NO	N/A	
12	Commerce & Trade	Dept. of Housing & Community Development	YES	1	YES	Some	Not Due	
13	Commerce & Trade	Dept. of Mines, Minerals & Energy	YES	1	YES	Some	NO	
14	Commerce & Trade	Dept. of Labor & Industry	YES	3	NO	N/A	N/A	
15	Commerce & Trade	Dept. of Professional & Occupational Regulation	YES	1	YES	NO	N/A	
16	Commerce & Trade	Tobacco Indemnification Commission	YES	0	NO	N/A	N/A	

Revised Agency Information Security Datapoints as of November 14, 2008

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Score (Points)
17	Commerce & Trade	Va. Employment Commission	YES	3	YES	NO	N/A	
18	Commerce & Trade	Va. Economic Development Partnership	YES	0	NO	N/A	N/A	
19	Commerce & Trade	Va. Housing Development Authority	NO	1	NO	N/A	N/A	
20	Commerce & Trade	Va. National Defense Industrial Authority	NO	0	NO	N/A	N/A	
21	Commerce & Trade	Va. Resources Authority	NO	0	NO	N/A	N/A	
22	Commerce & Trade	Va. Racing Commission	YES	2	YES	Not Due	Not Due	
23	Education	Dept. of Education	YES	1	YES	NO	N/A	
24	Education	Frontier Culture Museum of Va.	YES	0	NO	N/A	N/A	
25	Education	Gunston Hall	YES	0	NO	N/A	N/A	
26	Education	Jamestown Yorktown Foundation	YES	0	YES	NO	N/A	
27	Education	Library of Va.	YES	1	YES	Not Due	Not Due	
28	Education	State Council of Higher Education for Va.	YES	0	NO	N/A	N/A	
29	Education	Science Museum of Va.	YES	0	NO	N/A	N/A	
30	Education	Va. Commission for the Arts	YES	0	NO	N/A	N/A	
31	Education	Va. Museum of Fine Arts	YES	2	YES	YES	Not Due	
32	Education	Christopher Newport University	YES	0	YES	Not Due	Not Due	
33	Education	George Mason University	YES	1	YES	Some	YES	
34	Education	James Madison University	YES	0	YES	YES	Some	

Revised Agency Information Security Datapoints as of November 14, 2008

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Score (Points)
35	Education	Longwood University	YES	1	YES	YES	YES	
36	Education	Norfolk State University	YES	2	NO	N/A	N/A	
37	Education	Old Dominion University	YES	1	YES	YES	YES	
38	Education	Radford University	YES	0	YES	YES	YES	
39	Education	University of Mary Washington	YES	1	YES	NO	N/A	
40	Education	Va. Community College System	YES	36	YES	Some	~~NO~~ YES	
41	Education	Virginia Military Institute	YES	0	YES	NO	N/A	
42	Education	Virginia State University	YES	3	YES	Not Due	Not Due	
43	Finance	Dept. of Accounts	YES	4	NO	N/A	N/A	
44	Finance	Dept. of Planning & Budget	YES	2	~~NO~~ YES	~~N/A~~ Not Due	~~N/A~~ Not Due	
45	Finance	Dept. of Taxation	YES	1	YES	Some	YES	
46	Finance	Dept. of Treasury	YES	2	YES	~~NO~~ YES	Not Due	
47	Health & Hum. Res.	Dept. of Health Professions	YES	0	YES	Not Due	Not Due	
48	Health & Hum. Res.	Dept. of Medical Assistance Services	YES	6	YES	Some	Not Due	
49	Health & Hum. Res.	Dept. of Mental Health, Mental Retardation, & Substance Abuse Services	YES	15	YES	Not Due	Not Due	
50	Health & Hum. Res.	Dept. of Rehabilitative Services	YES	0	YES	NO	N/A	
51	Health & Hum. Res.	Dept. of Social Services	YES	2	YES	NO	N/A	
52	Health & Hum. Res.	Tobacco Settlement Foundation	NO	0	NO	N/A	N/A	
53	Health & Hum. Res.	Va. Dept. for the Aging	YES	1	YES	Not Due	Not Due	

Revised Agency Information Security Datapoints as of November 14, 2008

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Score (Points)
54	Health & Hum. Res.	Va. Dept. of Health	YES	3	YES	YES	YES	
55	Natural Resources	Dept. of Conservation & Recreation	YES	1	YES	Some	Not Due	
56	Natural Resources	Dept. of Environmental Quality	YES	4	YES	YES	Some	
57	Natural Resources	Dept of Game & Inland Fisheries	YES	1	NO	N/A	N/A	
58	Natural Resources	Dept. of Historic Resources	YES	2	YES	Not Due	Not Due	
59	Natural Resources	Marine Resources Commission	YES	1	YES	YES	~~YES~~ Not Due	
60	Natural Resources	Va. Museum of Natural History	YES	1	NO	N/A	N/A	
61	Public Safety	Alcoholic Beverage Control	YES	1	YES	YES	Some	
62	Public Safety	Commonwealth's Attorney's Services Council	NO	0	NO	N/A	N/A	
63	Public Safety	Dept. of Criminal Justice Services	YES	2	YES	NO	N/A	
64	Public Safety	Dept. of Fire Programs	YES	3	YES	Not Due	Not Due	
65	Public Safety	Dept. of Forensic Science	YES	1	YES	Not Due	Not Due	
66	Public Safety	Dept. of Juvenile Justice	YES	3	YES	NO	N/A	
67	Public Safety	Dept. of Military Affairs	NO	1	NO	N/A	N/A	
68	Public Safety	Dept. of Corrections	YES	3	YES	Some	Not Due	
69	Public Safety	Dept. of Correctional Education	YES	1	NO	N/A	N/A	
70	Public Safety	Dept. of Veterans Services	YES	1	NO	N/A	N/A	

Revised Agency Information Security Datapoints as of November 14, 2008

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Score (Points)
71	Public Safety	Va. Dept. of Emergency Management	YES	1	NO	N/A	N/A	
72	Public Safety	Va. State Police	YES	3	YES	Not Due	Not Due	
73	Technology	The Ctr for Innovative Tech.	YES	1	YES	NO	N/A	
74	Technology	Va. Info. Technologies Agency	YES	33	YES	Not Due	Not Due	
75	Transportation	Dept. of Motor Vehicles	YES	2	YES	Not Due	Not Due	
76	Transportation	Dept. of Aviation	YES	2	NO	N/A	N/A	
77	Transportation	Dept. of Rail & Public Trans.	YES	1	YES	Not Due	Not Due	
78	Transportation	Motor Vehicle Dealers Board	YES	0	NO	N/A	N/A	
79	Transportation	Va. Dept. Of Transportation	YES	5	YES	YES	Some	
80	Independent	Indigent Defense Council	YES	4	~~NO~~ YES	~~N/A~~ Not Due	~~N/A~~ Not Due	
81	Independent	State Lottery Dept.	YES	2	NO	N/A	N/A	
82	Independent	State Corporation Commission	YES	3	YES	Not Due	Not Due	
83	Independent	Va. College Savings Plan	YES	3	YES	Not Due	Not Due	
84	Independent	Va. Office for Protection & Advocacy	YES	1	EXCEPTION	EXCEPTION	Not Due	
85	Independent	Va. Retirement System	YES	2	YES	Not Due	Not Due	
86	Independent	Va. Workers' Compensation Commission	YES	1	EXCEPTION	EXCEPTION	~~N/A~~ Not Due	
87	N/A	Office of the Governor	YES	3	EXCEPTION	EXCEPTION	~~N/A~~ Not Due	

Revised Agency Information Security Datapoints as of November 14, 2008

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Score (Points)
88	N/A	Office of the Attorney General	YES	1	YES	Not Due	Not Due	
							Y-8 (9%)	
						Y-12 (14%)	Some – 4 (5%)	
						Some – 8 (9%)	N – 1 (1%)	
						N – 15 (17%)	Not Due – 34 (39%)	
					Y-59 (67%)	Not Due – 24 (27%)	N/A – 41 (47%)	
			Y- 81 (92%)		N – 26 (30%)	N/A – 26 (30%)	~~Y - 8 (9%)~~	
			N- 7 (8%)		Exceptions – 3 (3%)	Exceptions – 3 (3%)	~~N - 2 (2%)~~	
			~~Y- 80 (91%)~~	231 from 65 (74%) of 88 agencies	~~Y- 56 (64%)~~	~~Y- 11 (13%)~~	~~Not Due - 27 (31%)~~	
	TOTALS		~~N - (9%)~~		~~N - 29 (33%)~~	~~N - 16 (18%)~~	~~N/A – 47 (53%)~~	