COMMONWEALTH of VIRGINIA

George F. Coulter
Chief Information Officer
Email: cio@vita.virginia.gov

Virginia Information Technologies Agency
11751 Meadowville Lane
Chester, Virginia 23836-6315
(804) 416-6100

TDD VOICE -TEL. NO.
711

March 1, 2010

The Honorable Robert F. McDonnell
Governor of Virginia
Patrick Henry Building, 3rd Floor
1111 East Broad Street
Richmond, Virginia 23219

General Assembly of Virginia
c/o Division of Legislative Automated Systems
910 Capitol Street, General Assembly Building, 6th floor
Richmond, Virginia 23219
Attn: Laura Wilborn

Dear Governor McDonnell, Mr. Speaker, Mr. President pro tempore and members of the General Assembly,

The *Code of Virginia* §2.2-2009.C directs the Chief Information Officer of the Commonwealth (CIO) to prepare an "Annual Report on Information Security in the Commonwealth" relative to executive branch agencies, independent agencies and institutions of higher education.

I am pleased to report to you that, for this 2009 report, we conclude that significant, continued progress has been made in establishing and operating electronic information security programs adequate to safeguard the information of the Commonwealth. However, more work is needed, particularly in the area of application security practices as they relate to the development and maintenance of sensitive applications. Current threat trends indicate that malicious activity is focused on the exploitation of applications to gain access to sensitive systems and personal data.

I welcome any assistance that the Governor and General Assembly can provide to ensure that the Annual Report on Information Security in the Commonwealth remains a valuable reference for Commonwealth IT security decisions.

Sincerely,

George F. Coulter

c: The Honorable Martin Kent, Chief of Staff
The Honorable James D. Duffey, Secretary of Technology
Cabinet Secretaries
Members, Information Technology Investment Board

Virginia Information Technologies Agency

2009 Commonwealth of Virginia Information Security Report

Prepared and Published by:

Virginia Information Technologies Agency

Comments and recommendations on the Commonwealth Information Security 2009 Annual Report from all interested parties are welcomed and encouraged. Suggestions may be conveyed electronically to CommonwealthSecurity@VITA.Virginia.Gov

Please submit written correspondence to:

George Coulter
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

2009 Information Security Report

Executive Summary

This 2009 Commonwealth of Virginia (COV) Information Security Report is the second annual report to the Governor and the General Assembly and follows a baseline created in 2008 for assessing the strength of the information security programs that have been established to protect Commonwealth information. The scope of this report is limited to the 85 independent and executive branch agencies including higher education, but excluding charter universities and Tier II universities.

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 and 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 December 31, 2009, available to the Chief Information Security Officer (CISO) working on behalf of Chief Information Officer (CIO). We also utilized reports from the Auditor of Public Accounts (APA), specifically *Commonwealth Information Security Implementation Semi-annual Update, November 2009*. 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.

For this 2009 report, we conclude that significant, continued progress has been made in establishing and operating electronic information security programs adequate to safeguard the information of the Commonwealth. However, more work is needed, particularly in the area of application security practices as they relate to the development and maintenance of sensitive applications. Current threat trends indicate that malicious activity is focused on the exploitation of applications to gain access to sensitive systems and personal data. 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 required defenses change daily as underlying information transmission and storage methods change. However, we believe that the Commonwealth of Virginia is on the right path.

Background

The 2009 Commonwealth of Virginia Information Security Report is the second 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*. These duties include items such 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 duties under §2.2-2009, the CIO has established a Commonwealth Security and Risk Management directorate led by the Commonwealth CISO.

Approach

The 2009 COV Information Security Report follows a baseline created in 2008 for assessing the strength of the information security programs that have been established to protect Commonwealth information. The scope of this report is limited to the 85 independent and executive branch agencies including higher education, but excludes the four charter universities[1] and the three Tier II universities[2].

This report is not based on reviews of individual agency's information security programs, but rather is based on an analysis of data and information available to the CISO as of December 31, 2009. The COV Information Security Policy, Standard and Audit Standard require that certain data be reported by agencies to the CISO and this data serves as the 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 current Information Security Audit Plan for sensitive systems
- Provided Corrective Action Plans for completed information security audits
- Supplied Quarterly Status Updates for corrective actions
- 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 Auditor of Public Accounts (APA), specifically *Commonwealth Information Security Implementation Semi-annual Update, November 2009*. We analyzed security incidents reported by executive branch agencies. 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.

1. Established in 2008: College of William and Mary, University of Virginia, Virginia Commonwealth University, and Virginia Polytechnic Institute and State University
2. Established in 2009: George Mason University, James Madison University and Virginia Military Institute

2009 COV Information Security Program

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 sets Commonwealth direction and establishes a framework that agency heads must follow in implementing information security programs. The four standards provide greater depth on the requirements 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 all of the major components of the Information Security Standard. These guidelines provide agencies with additional information on compliance with the Information Security Standard and provide business cases and templates to assist agencies.

Commonwealth Information Security Council

The Commonwealth Information Security Council consists of 11 Information Security Officers who have come together to strengthen the information security posture of the Commonwealth. The members come from all branches of government, including higher education and local government. They meet monthly as a council to provide direction for the Commonwealth's Information Security Program and have formed committees around the following four initiatives:

- Encryption
- Identity and access management
- Making information security an executive management priority
- Risk Management

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 Officer's 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 2008, there were approximately 200 ISOAG list members. Monthly ISOAG meetings were held with an average attendance of 88.5 persons. For the fiscal year 2009, the list

membership has grown to 389 persons and monthly meeting attendance averaged 99.7 persons. For the first four months of fiscal year 2010, the list membership has grown to 423 persons and four meetings have been held with attendance averaging 92.4 persons. We expect this increase in the ISOAG membership to continue.

Information Security Orientation

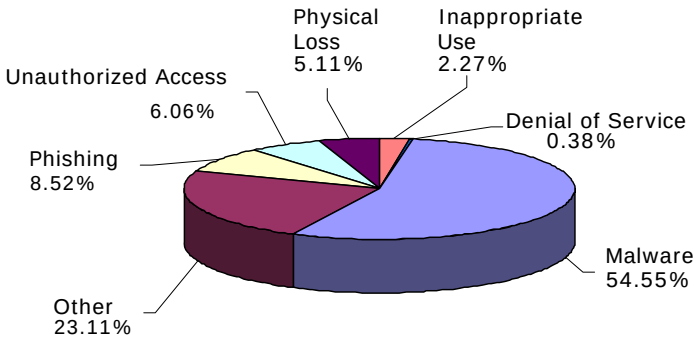
Another Commonwealth program established to assist government personnel interested in learning about building and documenting an information security program in the Commonwealth is Information Security Orientation. This session provides participants with a background on why we care about security of 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 35 sessions with 339 people attending, including 235 from 59 Commonwealth independent and executive branch agencies, including higher education within the last two years. As with the ISOAG meetings, we anticipate the Information Security Orientation program will continue to flourish and expand.

Commonwealth Information Security Incident Management

Section F. of the Code of Virginia, *§ 2.2-603 Authority of agency directors* requires that executive branch agency directors report information technology security incidents to the CIO within 24 hours of discovery. The Commonwealth Security Incident Response Team classifies each of these security incidents into a category based on the type of activity. Reported security incidents are grouped into one of the following categories:

- Malware: Execution of malicious code such as viruses, spyware and keyloggers
- Phishing: Theft, or attempted theft of user information such as account credentials
- Physical Loss: Loss or theft of any COV resource that contains COV data
- Denial of Service: Loss of availability of a COV service due to malicious activity
- Unauthorized Access: Unauthorized access to COV data (This category also includes any security incident where it may be uncertain if a malicious party accessed COV data.)
- Inappropriate Use: Misuse of COV resources
- Other: Reports where the investigation determines the event is not a security incident

2009 Security Incident Metrics



Between January 1 and October 31, 2009, 528 (*up 435*) information security incidents were reported. Of those 528 security incidents, 288 (*up 258*) were classified as using malicious software to modify or obtain Commonwealth information. The security incidents that involved unauthorized physical access to Commonwealth information primarily were due to lost or stolen laptops and

accounted for 27 (*down 10*) of the security incidents. Phishing attempts targeted at Commonwealth personnel accounted for 45 (*up 30*) of the security incidents. One-hundred-twenty-two (*up 111*) of the security incidents logged were classified as non-security incidents or unsuccessful attempts after a full investigation.

It is important to note that the Commonwealth's ability to detect and respond to these security incidents has increased in parallel with the progress of the information technology infrastructure transformation. Significant increases in key metrics are expected and are likely the result of this enhanced enterprise-wide detection capability and standardized reporting criteria.

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 January and December 2009, there were 11,046 (*down 3,898*) keylogging events provided to Commonwealth Security that involved 712 (*down 540*) citizens.

Commonwealth Operational Security

From an operational security perspective, the largest initiative is found in the Commonwealth information technology infrastructure program with Northrop Grumman. Agencies either have undergone or will undergo transformation of their personal computers, servers, networks and messaging. The program security team provides numerous and redundant capabilities to robustly protect Commonwealth assets and data as part of the transformation process.

In November 2009, VITA conducted its annual disaster recovery test at the Southwest Enterprise Solutions Center (SWESC). The purpose of testing is to ensure readiness in the event of an actual disaster. Program staff members worked with disaster recovery customers to simulate a disaster and restore the hardware and software supporting critical services at SWESC. It is a comprehensive test and reveals the strengths and weaknesses in processes, procedures, documentation, staffing and hardware. Each year, we apply the lessons learned and set the bar higher in terms of the scope and complexity of testing in subsequent years. Overall, the testing process went very well and received positive feedback from customer agencies.

Agency Information Security Efforts

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 that significant 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 85 agencies, 83 (98% - *up 7%*) agencies have designated an ISO within the past two years and 2 (2%) 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.

Of the 85 agencies, 59 (69% - *down 5%*) agencies have sent 235 persons to Information Security Orientation and 26 (31%) have not had a representative attend within the last two years.

Submission of a Current Information 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 yearly. 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 85 agencies, 76 (89% - *up 25%*) have submitted a current Information Security Audit Plan, 2 (2%) have an expired IT Security Audit Plan, 4 (5%) have never submitted an Information Security Audit Plan, and 3 (4%) agencies have a current exception on file.

Provided Corrective Action Plans for Completed Information Security Audits

For security audits that have been completed, corrective action plans are required to be submitted to the CISO 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 85 agencies, 37 (44% - *up 31%*) have submitted all corrective action plans, 4 (5%) have submitted some corrective action plans, 2 (2%) have not submitted any of the corrective action plans due, and 35 (41%) have no corrective action plans due. For 4 (5%) agencies, this is not applicable as they have not yet submitted an audit plan, and 3 (4%) agencies 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.

Of the 85 agencies, 19 (22% - *up 13%*) have submitted all updates, 3 (4%) agencies have submitted some updates, 1 (1%) agency has not submitted any updates due, 53 (62%) agencies have no updates due. For 6 (7%) agencies quarterly updates are not applicable since they have not submitted a security audit plan and/or a corrective action plan that was due, and 3 (4%) agencies have an exception on file.

[*]*The detailed listing of agencies and specific security data points can be found in Appendix I.*

Conclusion

Building and strengthening Commonwealth of Virginia's information security is a collaborative effort. The foundation for the Commonwealth's Information Security Program is the collaborative efforts of the Governor, 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 electronically, the Commonwealth Information Security Program must include our citizens as well.

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.

For this 2009 report, we conclude that significant, continued progress has been made in establishing and operating electronic information security programs adequate to safeguard the information of the Commonwealth. However, more work is needed, particularly in the area of application security practices as they relate to the development and maintenance of sensitive applications. Current threat trends indicate that malicious activity is focused on the exploitation of applications to gain access to sensitive systems and personal data.

Appendix I - Detailed Information by Agency

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 current Information Security Audit Plan for systems classified as sensitive.
No - The agency head has NOT had a Security Audit Plan submitted for systems classified as sensitive.
Exception - The agency head has submitted, and the CISO has approved a temporary exception 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.
Some - The agency head has submitted an adequate Corrective Action Plan/Quarterly Update for some but NOT all Security Audits.
No - The agency head has NOT submitted an adequate Corrective Action Plan/Quarterly Update for Security Audits.
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	Stoplight Score
1	Administration	Human Rights Council	Yes	0	Yes	Not Due	Not Due	
2	Administration	Dept. of General Services	Yes	3	Yes	Not Due	Not Due	
3	Administration	Dept. of Human Res. Mgmt	Yes	1	Yes	No	N/A	
4	Administration	Dept. Min. Bus. Enterprise	Yes	1	Yes	Not Due	Not Due	
5	Administration	Employee Dispute Resolution	Yes	2	Exception	Exception	Exception	
6	Administration	Compensation Board	Yes	1	Yes	Not Due	Not Due	
7	Administration	State Board of Elections	Yes	1	Expired	Yes	Not Due	
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	Yes	Not Due	Not Due	
11	Commerce & Trade	Board of Accountancy	Yes	0	Yes	Yes	Not Due	
12	Commerce & Trade	Dept. of Housing & Community Development	Yes	1	Yes	Yes	Yes	
13	Commerce & Trade	Dept. of Mines, Minerals & Energy	Yes	1	Yes	Yes	Yes	
14	Commerce & Trade	Dept. of Labor & Industry	Yes	1	Yes	Not Due	Not Due	
15	Commerce & Trade	Dept. of Professional & Occupational Regulation	Yes	0	Yes	Not Due	Not Due	
16	Commerce & Trade	Tobacco Indemnification Commission	Yes	1	Yes	Not Due	Not Due	
17	Commerce & Trade	Va. Employment Commission	Yes	2	Yes	Yes	Yes	
18	Commerce & Trade	Va. Economic Development Partnership	Yes	0	Yes	Not Due	Not Due	
19	Commerce & Trade	Va. National Defense Industrial Authority	Yes	0	Yes	Not Due	Not Due	
20	Commerce & Trade	Va. Resources Authority	No	0	No	N/A	N/A	
21	Commerce & Trade	Va. Racing Commission	Yes	0	Yes	Yes	Yes	
22	Education	Dept. of Education	Yes	2	Yes	Yes	Not Due	
23	Education	Frontier Culture Museum of Va.	Yes	0	Yes	Not Due	Not Due	
24	Education	Gunston Hall	Yes	0	Yes	Not Due	Not Due	
25	Education	Jamestown - Yorktown Foundation	Yes	2	Yes	Not Due	Not Due	

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Stoplight Score
26	Education	Library of Va.	Yes	0	Yes	Not Due	Not Due	
27	Education	State Council of Higher Education for Va.	Yes	0	Yes	Not Due	Not Due	
28	Education	Science Museum of Va.	Yes	1	Yes	Not Due	Not Due	
29	Education	Va. Commission for the Arts	Yes	0	Yes	Not Due	Not Due	
30	Education	Va. Museum of Fine Arts	Yes	0	Yes	Yes	Yes	
31	Education	Christopher Newport University	Yes	0	Yes	Yes	Yes	
32	Education	Longwood University	Yes	0	Yes	Yes	Yes	
33	Education	Norfolk State University	Yes	2	Yes	No	N/A	
34	Education	Old Dominion University	Yes	0	Yes	Yes	Yes	
35	Education	Radford University	Yes	0	Yes	Yes	Yes	
36	Education	Richard Bland College	Yes	0	Yes	Not Due	Not Due	
37	Education	University of Mary Washington	Yes	1	Yes	Yes	Not Due	
38	Education	Va. Community College System	Yes	43	Yes	Yes	Yes	
39	Education	Virginia State University	Yes	2	Yes	Yes	Not Due	
40	Finance	Dept. of Accounts	Yes	4	Yes	Yes	Not Due	
41	Finance	Dept. of Planning & Budget	Yes	1	Yes	Yes	Not Due	
42	Finance	Dept. of Taxation	Yes	1	Yes	Yes	Not Due	
43	Finance	Dept. of Treasury	Yes	3	Yes	Some	Some	
44	Health & Hum. Res.	Dept. of Health Professions	Yes	2	Yes	Not Due	Not Due	
45	Health & Hum. Res.	Dept. of Medical Assistance Services	Yes	4	Yes	Yes	Yes	
46	Health & Hum. Res.	Dept. of Behavioral Health and Developmental Services	Yes	22	Yes	Some	Some	
47	Health & Hum. Res.	Dept. of Rehabilitative Services	Yes	0	Yes	Yes	Not Due	
48	Health & Hum. Res.	Dept. of Social Services	Yes	1	Yes	Not due	Not Due	
49	Health & Hum. Res.	Virginia Foundation for Healthy Youth	Yes	1	Yes	Not due	Not Due	
50	Health & Hum. Res.	Va. Dept. for the Aging	Yes	0	Yes	Yes	Not Due	
51	Health & Hum. Res.	Va. Dept. of Health	Yes	5	Yes	Some	Some	
52	Natural Resources	Dept. of Conservation & Recreation	Yes	1	Yes	Yes	Yes	
53	Natural Resources	Dept. of Environmental Quality	Yes	4	Yes	Yes	Yes	

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Stoplight Score
54	Natural Resources	Dept of Game & Inland Fisheries	Yes	2	Expired	Some	No	
55	Natural Resources	Dept. of Historic Resources	Yes	2	Yes	Not Due	Not Due	
56	Natural Resources	Marine Resources Commission	Yes	3	Yes	Yes	Yes	
57	Natural Resources	Va. Museum of Natural History	Yes	2	Yes	Not Due	Not Due	
58	Public Safety	Alcoholic Beverage Control	Yes	4	Yes	Yes	Yes	
59	Public Safety	Commonwealth's Attorney's Services Council	Yes	0	Yes	Not Due	Not Due	
60	Public Safety	Dept. of Criminal Justice Services	Yes	2	Yes	Yes	Not Due	
61	Public Safety	Dept. of Fire Programs	Yes	2	Yes	Yes	Not Due	
62	Public Safety	Dept. of Forensic Science	Yes	1	Yes	Not Due	Not Due	
63	Public Safety	Dept. of Juvenile Justice	Yes	2	Yes	Not Due	Not Due	
64	Public Safety	Dept. of Military Affairs	Expired	1	No	N/A	N/A	
65	Public Safety	Dept. of Corrections	Yes	2	Yes	Yes	Yes	
66	Public Safety	Dept. of Correctional Education	Yes	1	Yes	Yes	Not Due	
67	Public Safety	Dept. of Veterans Services	Yes	0	Yes	Not Due	Not Due	
68	Public Safety	Va. Dept. of Emergency Management	Yes	1	No	N/A	N/A	
69	Public Safety	Va. State Police	Yes	2	Yes	Yes	Yes	
70	Technology	The Center for Innovative Tech.	Yes	1	Yes	Not Due	Not Due	
71	Technology	Va. Info. Technologies Agency	Yes	29	Yes	Yes	Not Due	
72	Transportation	Dept. of Motor Vehicles	Yes	1	Yes	Yes	Not Due	
73	Transportation	Dept. of Aviation	Yes	2	Yes	Not Due	Not Due	
74	Transportation	Dept. of Rail & Public Trans.	Yes	0	Yes	Not Due	Not Due	
75	Transportation	Motor Vehicle Dealers Board	Yes	0	Yes	Not Due	Not Due	
76	Transportation	Va. Dept. Of Transportation	Yes	9	Yes	Yes	Yes	
77	Independent	Indigent Defense Commission	Yes	4	Yes	Yes	Not Due	
78	Independent	State Lottery Dept.	Yes	0	Yes	Not Due	Not Due	
79	Independent	State Corporation Commission	Yes	3	Yes	Not Due	Not Due	
80	Independent	Va. College Savings Plan	Yes	3	Yes	Yes	Not Due	

	Secretariat	Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAP's Received	Quarterly Updates	Stoplight Score
81	Independent	Va. Office for Protection & Advocacy	Yes	1	Exception	Exception	Exception	
82	Independent	Va. Retirement System	Yes	1	Yes	Yes	Not Due	
83	Independent	Va. Workers' Compensation Commission	Yes	3	Exception	Exception	Exception	
84	N/A	Office of the Governor	Yes	1	No	N/A	N/A	
85	N/A	Office of the Attorney General	Yes	0	Yes	Not Due	Not Due	
	TOTALS		Y- 83 (98%) N- 1 (1%) Exp -1 (1%)	235 from 59 (69%) of 85 agencies	Y-76 (89%) N – 4 (5%) Exceptions – 3 (4%) Exp – 2 (2%)	Y- 37 (44%) Some – 4 (5%) N – 2 (2%) Not Due – 35 (41%) N/A – 4 (5%) Exceptions – 3 (4%)	Y- 19 (22%) Some – 3 (4%) N – 1 (1%) Not Due – 53 (62%) N/A – 6 (7%) Exception – 3 (4%)	Green 74 87% Yellow 5 6% Red 6 7% Total 85 100%