

**2008 NASCIO Recognition Awards Nomination  
Commonwealth of Virginia**

**Nomination Category:**  
Information Security

**Title of Nomination:**  
**Information Security: Interlocking Spheres of Collaborative Protection**

**Nomination Submitted By:**  
Lemuel C. Stewart, Jr.  
Chief Information Officer  
Commonwealth of Virginia  
Virginia Information Technologies Agency

**2008 Commonwealth of Virginia NASCIO Award Submission**  
**Category: Information Security**

**Project:**

**Information Security: Interlocking Spheres of Collaborative Protection**

**Executive Summary**

Information technology is increasingly the foundation and backbone for all business, including government business. Parallel needs for efficiency and economy in government operations continue to drive adoption of IT solutions for providing government business service delivery to citizens. Accordingly, the need to protect the sensitive information involved in digital government has increased exponentially as security threats adapt, evolve and attack at an ever accelerating rate. This threat environment requires government to adopt a security posture that is both nimble and impenetrable by virtue of depth.

This vital need unfortunately was not being adequately met as recently as 2006, when Virginia had an aging, inefficient IT infrastructure and numerous operational security risks. There were more than 90 autonomous IT shops in agencies, and 60 percent of the equipment in use was from eight to 10 years old. Further, the state's primary data center building was rated a security risk. These factors combined to create an operational landscape fraught with unacceptable risk for hacking and security incidents.

To achieve the rigorous security posture required to protect its citizens and grow secure digital applications, the Chief Information Officer (CIO) of the Commonwealth and the Virginia Information Technologies (VITA) were charged with implementing appropriate standards and processes to ensure information security. Today, the Commonwealth of Virginia has developed a collaborative approach to information security that employs interlocking spheres of security:

- Top-down sphere
- Peer – peer sphere
- IT security program sphere
- Infrastructure sphere
- External sphere

Close collaboration across the interlocking spheres allows Virginia government entities to leverage ideas, knowledge and resources to strengthen the information security posture of the Commonwealth. Adoption and promotion of information security needs by executive and elected leaders provides a top-down emphasis that increases awareness and compliance at all levels of government.

This approach has greatly elevated awareness of information security needs, enabled strong partnerships at all levels of government and facilitated new strategies for defense, creating a model that can be adopted by others pursuing similar goals.

## Description of the problem and solution

Information technology is increasingly the backbone for all business, including government. Needs for efficiency in government operations continue to drive adoption of IT solutions for providing government business service delivery to citizens. Accordingly, the need to protect the sensitive information involved in digital government increased exponentially as security threats adapt, evolve and attack at an accelerating rate. Government must adopt a security posture that is both nimble and impenetrable by virtue of depth.

As recently as late 2006, Virginia had an aging, inefficient IT infrastructure and numerous operational security risks. There were more than 90 autonomous agency IT shops, and 60% of the equipment was eight to 10 years old. The state's primary data center building was rated a security risk. State agencies did not have adequate information security programs. These factors combined to create an operational landscape fraught with unacceptable risk for security incidents.

The Auditor of Public Accounts (APA) reported in 2006 that of the 104 agencies and institutions reviewed, 17% had no information security program and 63% had an inadequately documented program. The fractured security landscape lacked clear enforcement authority and communication channels.

To achieve the rigorous security posture required to protect its citizens and grow secure digital applications, the Commonwealth of Virginia developed a collaborative approach to information security that employs interlocking spheres of security:

- Top-down sphere
- Peer-to-peer sphere
- IT security program sphere
- Infrastructure sphere
- External sphere

This approach elevated awareness of information security needs, enabled strong partnerships at all levels of government and facilitated new strategies for defense in the Commonwealth, creating a model that can be adopted by others.

**Top-down Sphere:** Top-down spheres of protection involve top leadership, demonstrating that information security truly is an executive priority. The legislature, Governor, CIO, VITA, Chief Information Security Officer (CISO), Cabinet members and agency heads all have roles in maintaining information security.

The Virginia General Assembly enacted vital [legislation](#), effective July 1, 2007, to enforce information security. It codified roles of the Information Technology Investment Board, ([ITIB](#)), CIO and agency directors in information security and standardized improvements. It extended Virginia's IT Security Policy and Standards to all government branches and independent agencies.

The CIO, through VITA, is required to develop policies, procedures and standards for: assessing security risks, determining security measures and performing security audits of government electronic information; and addressing the scope and frequency of security audits, and report annually any agencies with unacceptable information security programs to the Governor and General Assembly. It provides the ITIB the option of withholding IT project funds for those agencies.

The CIO led development of the Commonwealth Information Security Policies, Standards and Guidelines (PSG) for review and approval by the ITIB. Commonwealth Security provided a [Commonwealth IT Security Audit Standard](#), [Commonwealth Data Removal Standard](#) and [Commonwealth Use of Non-Commonwealth Devices to Telework Standard](#) and [Guidelines](#) for risk management, contingency management, logical access, IT personnel security, IT security audits, data protection and threat management.

Virginia agencies are required to report all security incidents to the CIO within 24 hours from when the agency discovered - or should have discovered - the occurrence. To simplify compliance, centralized [Web-based reporting of IT security incidents](#) to the CIO was developed. Such reporting gives the Commonwealth a holistic picture of the information security posture, allowing timely security incident response and trending of security incidents for assistance and future policy and standard revisions. [Guidance on what to report](#) is provided.

In 2006 the General Assembly positioned the Commonwealth of Virginia to be the first state in the union to require Internet safety guidelines for students with the passage of [House Bill 58](#). The Department of Education developed [guidelines](#).

Governor Timothy M. Kaine strongly supports information security initiatives, including Executive Order 43, [Protecting the Security of Sensitive Individual Information in Executive Branch Operations](#) in January 2007. Governor Kaine designated October 2007 as Cyber Security Month in the Commonwealth. The Virginia legislature passed [House Joint Resolution 587](#) designating September as Internet Safety Month, in 2007 and beyond.

**Peer-to-peer sphere:** Three very active knowledge sharing programs comprise Virginia's peer to peer approach: Commonwealth Information Security Council, Information Security Officers Advisory Group and Information Security Orientation Program.

The [Commonwealth Information Security Council](#) formed in April 2007 to strengthen Virginia's information security posture. The Council has four initial initiatives. Over the past year, the Council also has finalized a Business Impact Analysis template for the Department of Emergency Management's continuity planning, surveyed the community, drafted an identity and access management trust model and provided input on data breach notification requirements. It now is developing a non-disclosure agreement for statewide use in contracts and a secure communication portal for the information security community.

The Information Security Officers Advisory Group (ISOAG) is open to all state and local government personnel interested in information security. Monthly meetings are hosted by the CISO and training opportunities are provided. 271 persons have joined from the judicial, legislative and executive branches independent agencies, higher education and localities. This active group enhances understanding of the threat environment, current operations and developing trends. It is an excellent networking and practical knowledge sharing avenue, features keynote addresses experts and provides training opportunities. An e-mail alert notification is deployed to the ISO on an as-needed basis. Advisories note that agencies receiving services from the IT Infrastructure Partnership have vulnerable devices remediated.

Information Security Officer's (ISO) orientation sessions are small group overviews. All ISOs, back-up ISOs, IT Auditors and interested persons are invited. As of May 2008, 103 persons have attended, representing 57 organizations from all branches of government.

**IT security program sphere:** The Commonwealth now proactively assesses and manages risk of its information systems at several levels. From an overarching Commonwealth perspective,

agencies are required to develop and maintain a documented information security program per [Commonwealth Standard](#) including a risk management program for systems classified as sensitive relative to confidentiality, availability or integrity of the data they process.

This enterprise process includes defining security roles and responsibilities: performing a business impact analysis; classifying systems relative to sensitivity and, for sensitive systems, also defining system boundaries; performing a risk assessment; and, performing security audits to assess effectiveness of controls. The risk assessment details credible vulnerabilities and identifies mitigating controls in place, outstanding issues needing remediation and potential control vulnerabilities that would allow unauthorized access. A [Risk Management Guideline](#) and a [Risk Assessment Example](#) assist agencies. Virginia has included security expertise into the project development lifecycle at the earliest point possible. Web-based cyber security tools are updated regularly and published as a comprehensive online [Toolkit](#).

**Infrastructure sphere:** Virginia has leveraged its IT infrastructure partnership with Northrop Grumman to solve numerous security shortfalls. With the \$270 million up-front capital investment, Virginia has designed a new infrastructure with technical security controls to enforce policy and authorize use in desktop, print, help desk, e-mail, security, network, mainframe, server and facilities.

A new primary data center, the Commonwealth Enterprise Solutions Center (CESC) in Chester, VA, opened in July 2007 with Tier III availability features including power from two separate substations, three 2250 kilowatt paralleled generators and alternate water supply. A twin back-up data center in Lebanon, VA, provides 24-hour back-up capability and will guarantee full redundancy when transformation is completed. [Information on both facilities](#) is online.

All servers and mainframes were moved from the original data center in downtown Richmond to CESC in November, 2007, eliminating a known security risk. Individual desktops across the state are being rapidly replaced with models equipped with full firewall, anti-virus and anti-spyware software; once a PC has been “refreshed,” updated versions of this software and patches for observed vulnerabilities quickly can be pushed using automated tools. Executive branch agencies utilizing the primary data center are required to provide a copy of their software backup schedule. Logs of successful backups are kept; if backups are needed, VITA and Northrop Grumman will provide recovery services to partner organizations.

“Need to have” security policies for citizens’ personal information now are being implemented, including data truncation, infrequent rather than repetitive collection and storage; encryption of data stored and in motion, background checks on persons with proximity and least privilege access to information.

In January 2008, VITA staff installed a tool to proactively defend against cyber attacks. “Honeypots” online and outside the network perimeter simulate configurations ripe for cyber attacks. A “Honeynet” calculates the source and nature of the attacks. Staff developed reporting software through Honeynet to increase the state network’s security posture. From Jan. 1 - April 1, 2008, Honeynet logged Honeypot visits by 6,163 computers infected with malware that generated 2,601,865 attacks and collected 487 unique pieces of malware.

**External Sphere:** Despite best efforts by government agencies, threats to information security are not limited to their domain. Commonwealth entities have been urged to use a “Citizen’s Awareness Banner” developed by security staff for citizen-facing Web applications where personally identifiable information may be exchanged to raise malware awareness. This banner

reminds citizens that information security is a shared responsibility and directs to a *Citizen's Guide to Online Protection*. The guide is updated as the security landscape changes.

In concert with the the Multi-State Information Sharing & Analysis Center, VITA provides the monthly, [Cyber Security Tips](#) online and in document format for redelivery.

Virginia actively participates in national cyber security initiatives and shares information with all participants. This includes [InfraGard](#), a Federal Bureau of Investigation (FBI) program, and the [Multi State – Information Sharing & Analysis Center](#) (MS-ISAC), a voluntary and collaborative organization. A statewide membership to the Information Risk Executive Council (IREC) allows Virginia state and local government employees to access the group's resources at no additional cost.

### **Significance to the improvement of the operation of government**

Close collaboration across interlocking spheres allows Virginia government entities to leverage ideas, knowledge and resources to strengthen the information security posture of the Commonwealth of Virginia. Adoption and promotion of information security needs by executive and elected leaders provides a top-down emphasis that increases awareness and compliance at all levels, eliminates silos and promotes collective strengths across all branches of government.

Centralized security monitoring and promulgation of guidance through the CIO and CISO allow continuous analysis of threats and software updates, training opportunities and topical updates, such as changes in the payment card industry.

Agencies have designated Information Security Officers to provide crucial communication into the agency. ISOs now follow industry best practices as defined by recognized authorities, including: International Standards Organization (ISO), National Institute of Standards and Technology (NIST), Information Systems Audit and Control Association (ISACA), Control Objectives for Information and Related Technologies (COBIT) and U.S. Government Accountability Office (GAO).

- Security is now proactively integrated into all stages of the IT decision-making process.
- Centralized data storage and enterprise infrastructure allow security staff to employ protective controls of citizen information and push needed software updates almost instantaneously.
- The secure remote access capability of the new infrastructure, supported by a comprehensive security awareness, training and enforcement program, enables a mobile workforce.
- Dissemination of information to citizens through multiple avenues allows the Commonwealth to raise awareness of cyber security threats and partner with its end users to raise the security profile of the state.

The proactive approach to and embrace of best practices in information security centers around a vision of a highly collaborative environment in which individual agencies and employees assume front line roles in protecting citizen data and transactions.

By creating and leading communities of interest around multiple facets of IT security, Virginia is establishing a statewide center of excellence. Well-educated practitioners share tactics and stay abreast of the evolving IT security landscape, eliminating the haves/have nots dichotomy while bolstering knowledge throughout the state workforce.

## Benefit of the project

Virginia has vastly improved the security posture of the Commonwealth through collaboration, at no extra cost to the taxpayer for most initiatives. By contrast, the cost of an information security breach involving personal citizen information is immeasurable and must be prevented.

VITA and Northrop Grumman are transforming the state's IT infrastructure at no additional cost to the taxpayer, providing multiple information security benefits:

- Standardized security architecture
- Enterprise Security Operations Center – central monitoring and management
- Two custom-built, secure, reliable data center and backup data center facilities in Virginia with robust disaster recovery capability
- A single, statewide network and secure Internet gateway
- Standard, consistent use of security tools and policies across infrastructure and PCs (firewalls, administrative rights, encryption, anti-virus, etc.) in place for more than 23,000 PCs; all will be completed by July 2009
- Standard infrastructure support and planned refresh
- Central and quick administration of security patches for newly identified vulnerabilities

Online reporting tools for security incidents streamlined the reporting and response process from days -- sometimes weeks -- to minutes.

Central threat monitoring will enable an enterprise view of and response to such attacks. An incident may seem isolated to one agency; the central incident team can assess multiple assaults.

The Commonwealth's security initiatives and visibility reflects close alignment with the stated priorities of the Governor, General Assembly, CIO and NASCIO. The initiatives are also aligned with all of the goals of the state's [Strategic Plan for Information Technology](#):

- **Accessibility to government** increases as entities securely provide more services online.
- **Collaboration and partnerships** form the base of the information security posture.
- **A trusted and reliable technical environment** is ensured through defenses erected at every level of entry.
- **A reputation of performance** is created for technology through a hardened infrastructure and protection of citizen's personal information.
- **State workforce productivity** improves as secure technology is deployed to increase efficiency and solve business problems.

The collaborative approach allowed the state to share knowledge and best practices with localities and institutions of higher education – not as a distasteful, unfunded mandate, but as a helpful toolkit -- at no additional cost.

Though information security is not a finite problem that can be “solved,” implementation of a multi-dimensional, holistic security program in Virginia created a flexible, interwoven solution that can readily adapt and best protect its citizens today -- and tomorrow.