## Executive Summary

The Commonwealth of Pennsylvania is a trusted steward of citizen information. Trust in government is directly related to the quality of service and the sense of security that citizens feel when working with the government. To ensure the confidentiality, integrity and availability of data and services, the Commonwealth recognizes the need to have enterprise policies, standards and views of the state of security within the government.

In the past several years, the Commonwealth has implemented many solutions and technologies to improve connectivity and sharing between Commonwealth entities, with external business partners, and with citizens. These solutions have resulted in increased productivity and reduced costs; but have also led to greater Information Technology (IT) security risks related to increased connectivity.

The Office of Administration, Office for Information Technology (OA/OIT), is an executive agency responsible for leading and coordinating information technology services in the Commonwealth. In the past two years, OA/OIT has initiated several information security initiatives which together, make up the Information Security Architecture.

The Pennsylvania Information Security Architecture consists of the following initiatives and frameworks:

- **Security Governance** to evolve Information Security policies and architecture, integrated with the Commonwealth's Enterprise Architecture Governance process.
- **Security Policies** to prescribe procedures relating to technology topics such as data encryption, privacy roles and assessments and acceptable use policies.
- **Information Sharing** to establish relationships and communication vehicles through entities such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), a Pennsylvania ISAC, and the creation of a cyber security portal.
- **Identity Protection & Access Management (IPAM)** to establish a Commonwealth approach and architecture pertaining to identity management in alignment with federal and industry standards. Key components of IPAM include a Personal Identification Verification (PIV) card and identity proofing and vetting procedures.
- **Security Assessment Framework** to verify proper configuration of systems, accuracy of documentation, skills of staff members, and to determine gaps between an organizations's current and desired practices.
- **Cyber Security Exercise Program** to participate in national exercises, such as Cyber Tempest, as well as plan and hold Pennsylvania-specific exercises.
- **Enterprise Security Technologies** to ensure that agencies are using and deploying security technology and products such as antivirus, content filtering, and Network Intrusion Prevention Solutions in a consistent manner.
- **Security Awareness Program** to ensure that users are familiar with information technology security best practices, policies, procedures and standards as well as the importance of protecting confidential and sensitive information.

The development and implementation of Pennsylvania's Information Security Architecture has provided real and measurable value to the citizens of the Commonwealth. The establishment of enterprise standards and the use of enterprise license agreements have resulted in real savings of over **$27 million** to the Commonwealth for the purchase of security related solutions.

This fiscal year, the security tools have detected and/or blocked over one hundred thousand viruses, one hundred thousand spyware/adware attempts, three hundred million host intrusion events and four million inappropriate Internet usage attempts. The enterprise patch management solution allows easy identification of vulnerable systems and saves an estimated **$6 million per year** in time savings from its automation capabilities. The Commonwealth estimates it has saved **over $33 million** in avoidance of lost productivity caused by virus and worm outbreaks (based on an estimate from 2004 attacks and outbreaks).

## Description of Business Problems

The Commonwealth of Pennsylvania, with over $1 billion in IT investments annually offered by more than forty agencies, is a trusted steward of citizen information. Trust in government is directly related to the quality of service and the sense of security that citizens feel when working with the government. To ensure the confidentiality, integrity and availability of data and services, the Commonwealth recognizes the need to have enterprise policies, standards and views of the state of security within the government.

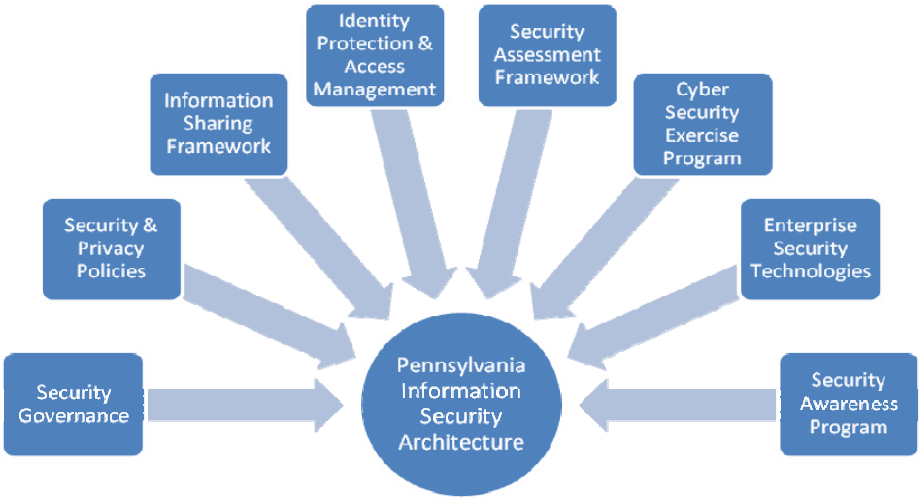
In the past several years, the Commonwealth has implemented many solutions and technologies to improve connectivity and sharing between Commonwealth entities, with external business partners, and with citizens. These solutions have resulted in increased productivity and reduced costs; but have also led to greater IT security risks related to increased connectivity. The threat of cyber attacks is a growing concern in the IT industry and within the Commonwealth. Vulnerabilities in one agency or business partner could expose the entire Commonwealth to the same risks or attacks.

The Commonwealth has recognized the need to enhance security on its networks to better protect assets from vulnerability arising from exploits of operating system security flaws, viruses, and denial of service attacks. The Commonwealth has experienced productivity interruptions and disruptions of service to both constituents and internal users in providing essential services to citizens. These disruptions have caused delays in revenue receipts, providing online services to citizens and significant expenditure of effort by agency staff to correct the problems introduced by these exploits.

Each agency has, in the past, been responsible for its own IT procurements and implementations. This model impeded the Commonwealth from creating an enterprise view into information security, led to inconsistent and disparate technology implementations, and inhibited information sharing between agencies. Agencies were making their own purchases without leveraging the enterprise pricing and without consideration to standard implementation. Risk and security assessments policies were vague and inconsistently enforced.

## Description of Solutions

The Office of Administration, Office for Information Technology (OA/OIT) is an executive agency directed by Executive Order 2004-8, *Enterprise Information Technology Governance Board*, as responsible for leading and coordinating information technology services in the Commonwealth. In the past two years, OA/OIT has initiated several information security initiatives which, together, make up the Information Security Architecture. These are depicted in the figure below and described throughout the remainder of this document.




**PA Information Security Architecture 1**

### Security Governance

Recognizing the importance of bringing collaboration, the Commonwealth has developed a mature governance model for Information Security. Integrating with the Commonwealth's Enterprise Architecture

Governance process, specific groups are responsible for developing consistent, cohesive policies, processes, and decisions regarding information security in the Commonwealth.

The **Enterprise Technology Security Council (ETSC)** is chaired by the Commonwealth's Chief Information Security Officer (CISO) and is comprised of security experts from many agencies. The purpose of ETSC is to make recommendations for improving the security of Commonwealth computer systems and the information residing on them. The group meets regularly to review security issues affecting the Commonwealth, provide security initiative recommendations and priorities, and to perform high level threat and risk analysis.

The **Enterprise Architecture Security Domain Team** is a cross-agency team that develops security policies, technologies, and standards for the Commonwealth. All Commonwealth information security policies are developed and reviewed by this team providing all agencies with the ability to participate.

Major IT initiatives and procurements are subject to approval by a **Technical Architecture Review Board**. This board is comprised of business and technology leaders whose task is to ensure agency IT and IT security initiatives are consistent, coordinated, and in compliance with existing standards.

## Security and Privacy Policies

Recognizing the ever-changing environment in which our employees work and our services are provided, the Commonwealth (through its collaborative Enterprise Architecture Governance process) continually develops and updates security-related policies. Listed below are highlights of recent security policy activities:

**End-User Acceptable Use Policy -** An updated *IT Resource Acceptable Use Policy* was published. Whereas the old policy was strictly for employees and targeted e-mail and Internet use, the updated policy adds polices relating to a broad range of IT security issues such as sensitive data encryption and the securing of portable devices and pertains to other authorized users such and consultants and volunteers. Pennsylvania is using its Electronic Learning Management System (eLMS) to distribute the policy and record employee acceptance.

**Administrator Acceptable Use Policy -** A policy covering the use of privileged accounts, *IT Administrator Acceptable Use, Auditing and Monitoring,* was published. This directive provides guidance regarding the acceptable use of Commonwealth IT resources by administrators and describes the monitoring procedures to ensure that administrators do not misuse authority.

**Information Security Policies –** Through the Enterprise Architecture Governance Structure, technology specific policies are published as Information Technology Bulletins (ITBs). In the past two years over twenty security-related policies have been published or refreshed. Key published policies include data encryption and electronic signature standards. The Security Domain Team is responsible for leading this effort.

**Information Privacy Policies -** As the Commonwealth is a trusted steward of much citizen information, policies and standards surrounding information privacy are crucial. The Commonwealth has developed in depth privacy policy which requires agencies to designate an Electronic Information Privacy Officer, perform annual system and data privacy impact assessments, categorize data and users permitted access to the data, determine which electronic information access activities are to be logged, and maintain auditable access logs compliant with applicable state and federal legislation.

## Information Sharing Framework

It is critical to establish relationships and communication vehicles before a crisis occurs. The Commonwealth, recognizing this, has developed key relationships and started key initiatives to share information with other important and relevant groups. The highlights are described below:

**MS-ISAC –** The Commonwealth is a key member of the Multi-State Information Sharing and Analysis Center (MS-ISAC). The MS-ISAC, whose mission is to provide a common mechanism for raising cyber security readiness and response in state and local governments, receives participation from all fifty states and the District of Columbia. Pennsylvania representatives sit on many MS-ISAC committees including Security Education & Awareness, Cyber Exercise Workgroup, Cyber Security Metrics & Compliance, and Operations. Additionally, the Pennsylvania CISO is a co-chairperson of the new MS-ISAC Local Government Committee.

The U.S. Department of Homeland Security has recognized the MS-ISAC as the national center for states to coordinate cyber readiness and response.

**PA-ISAC** The U.S. Department of Homeland Security is extending the information sharing model used by MS-ISAC to local governments within states. A pilot program to create intrastate ISACs was developed and Pennsylvania was one of three states selected for participation. The Pennsylvania ISAC has been established to address the Commonwealth of Pennsylvania's cyber security readiness and critical infrastructure coordination. This initiative is led by the Commonwealth CISO. Membership in PA-ISAC is open to elected and administrative officials of city, town, village, township, county and other Pennsylvania government jurisdictions. PA-ISAC provides the following benefits to members:

- Direct access to cyber security threat information from the Commonwealth
- Access to security awareness materials, including computer-based training modules
- Access to a security assessment toolkit
- Access to security policy templates
- Access to security related solutions at enterprise price points negotiated by the Commonwealth
- Regular meetings to promote peer networking and information sharing

**CISO Roundtable -** Held bimonthly, the CISO roundtable is a vehicle for direct collaboration with agency information security professionals. The CISO uses this forum to inform security professionals of relevant security topics and major projects. New initiatives are often first rolled out to this group to obtain feedback. The meetings also provide an open forum for attendees to ask questions of and discuss concerns with the CISO.

**Cyber Security Portal -** A cyber security Web site (http://cybersecurity.state.pa.us) was launched in October 2006 to provide timely, accurate and reliable information to employees, businesses and citizens. The site features online safety information applicable to employees, students, parents and children, small businesses, and local governments. It includes security newsletters, security awareness materials, a cyber security area specifically for children, links and feeds to the latest security news, event information, and an area dedicated to promoting best practices.

**Cyber Threat Advisory Level -** The Cyber Security Portal hosts the Commonwealth's Cyber Threat Advisory Level. The threat level ranges from green to red, depending on risks relating to threats, vulnerabilities and active exploits. Interested parties have the ability to sign up for e-mail alerts for cyber threat level changes, ensuring they are notified quickly when new threats are discovered.

**Alerts & Advisories Service -** The Commonwealth CISO is responsible for promulgating security threat and vulnerability information. A team is in place to monitor key sites, newsgroups and advisory services and craft alerts or advisories for distribution to interested parties. For example, Microsoft patches are evaluated and information is then distributed to agencies through the Commonwealth e-mail system and to local governments through the PA-ISAC Web portal.

## Identity Protection & Access Management (IPAM)

Identity Protection and Access Management (IPAM) is an interagency initiative launched to establish a Commonwealth enterprise approach and architecture pertaining to identity management in alignment with federal and industry standards such as Federal Information Processing Standards (FIPS 201) and Security Assertion Markup Language (SAML). IPAM is a comprehensive effort that covers many aspects of identity management including:

- **Enterprise Directory Services**. Provides for consolidation, synchronization and aggregation of shared identity information for retrieval and user authentication.
- **Access Management and Control**. Provides standards and policies for accessing Commonwealth facilities and information systems.
- **Identity Proofing and Vetting.** Outlines the processes for validating and verifying an individual's identity for the purpose of establishing credentials, such as log-in identifications and identity cards.
- **Enterprise Public Key Infrastructure (PKI**). Describes the standards for use of secure mechanisms (cryptography) to verify established identities, support digital signatures and encrypt sensitive data.

- **Commonwealth Personal Identification Verification (PIV) Card.** Provides the physical and logical layout for components of the PIV card, (e.g., magnetic strip, smart chip, photo).

During the past year, the IPAM initiative has made significant progress towards a Commonwealth-wide, identity management architecture and process. Key accomplishments include:

- Specification of the Enterprise Directory Blueprint;
- Creation of a standard Web Access and Authentication architecture;
- Creation of a FIPS 201-compliant, PIV card specification;
- Selection of a standard for user provisioning and automated password reset functions; and
- Selection of a Commonwealth-wide Shared Service Provider for digital certificates.

## Security Assessment Framework

Organized assessment and testing of security controls and processes are vital exercises for any organization. Testing verifies proper configuration of systems, accuracy of documentation and skills of staff members. Assessments determine gaps between an organization's current and desired practices.

The Commonwealth has established a policy, *Security Assessment and Testing Policy*, to specify standards surrounding security assessments, vulnerability scanning, and penetration testing on Commonwealth networks and assets. Agencies are required to perform regular assessments and vulnerability scans, share results with the Commonwealth CISO, and track the remediation of any discovered issues.

To support this policy, a comprehensive, downloadable security assessment methodology and toolkit was created to assist agencies evaluate their security procedures, determine their status relative to enterprise policy, and establish improvement targets. The toolkit consists of a variety of helpful assets including numerous targeted assessment questionnaires based on ISO 17799:2005 and a findings report template.

## Cyber Security Exercise Program

In December 2006, Pennsylvania was one of five states to participate in Cyber Tempest, a regional cyber exercise hosted by the New York State Office of Critical Infrastructure Protection, the MS-ISAC, and the U.S. Department of Homeland Security. Pennsylvania's representative was the leader of the government Sector Scenario Development Team and intricately involved during the five-month planning phase. Pennsylvania was one of only a few states selected to participate in the next major federal cyber security exercise, Cyber Storm II, in March 2008.

To continue the momentum from this exercise, the Commonwealth planned and held its own cross-agency cyber security exercise. After several months of cross agency planning and scenario creation, representatives from eleven agencies participated in a two-day cyber security table top exercise. The exercise promoted the importance of planning for cyber threats and disruptions and tested existing response frameworks and communication links between agencies. Following the exercise, a lessons-learned discussion was held and a formal action report developed.

## Enterprise Security Technologies

As part of its charter, the Bureau of Enterprise Architecture has led initiatives to create technology standards for the Commonwealth. One key goal is to ensure that agencies are using and deploying security technology in a consistent manner. Key security technology standards that have been deployed and managed include:

- **Enterprise Antivirus.** A centralized solution resulting in consistent support, consistent enforcement, and enterprise reporting.
- **Enterprise Patch Management.** A centralized solution which enables agencies to manage their own patching but allows for enterprise compliance reporting.
- **Enterprise Security Agent.** An additional layer of security; primarily defense against insider threats and zero-day worms. A federated deployment allows enterprise views of security events detected by these agents.
- **Internet Content Filtering & Access Control.** A standard implementation of a Web filtering solution and enterprise policy to enforce a minimum filter set.
- **Enterprise Active Directory Administrator Monitoring.** Consolidation of all agency accounts into a single Microsoft Active Directory infrastructure. Pennsylvania was one of the first states to complete this type of solution. The solution provides full, in-depth reporting of any user activity in the directory

and an Active Directory Administrator Monitoring solution that creates events and alerts related to administrator activity promoting trust across agencies.

- **Enterprise Network Intrusion Prevention Solution.** Deployment of an enterprise Network Intrusion Prevention Solution (NIPS) to dynamically monitor and block malicious network traffic in key locations on the Commonwealth's network.
- **Enterprise Security Information & Event Management.** The implementation of a Security Information & Event Management (SIEM) solution has enhanced the Commonwealth's ability to easily aggregate and correlate security events from multiple sources, such as enterprise firewalls and the enterprise antivirus solution. Use of a SIEM has greatly expanded the Commonwealth's ability to perform in-depth threat analysis.

## Security Awareness Programs

Security awareness training is a vital component of the Commonwealth's overall approach. It ensures that users are familiar with information technology security best practices, policies, procedures and standards as well as the importance of protecting confidential and sensitive information. Pennsylvania published Management Directive 535.9 - *Physical and Information Security Awareness Training,* which mandates security awareness training for all Commonwealth employees and contractors that access the Commonwealth's networks. The Enterprise Architecture Information Security Division developed the materials used in the program, which has been taken by over thirty thousand Commonwealth employees and contractors.

In support of security awareness, Pennsylvania participated with the MS-ISAC to promote October as Cyber Security Awareness month. The Commonwealth distributed awareness posters, newsletters and other materials to agencies and employees. A Cyber Security Awareness day was also held at the Capitol building to promote awareness to citizens and legislators.

## Public Value

The development and implementation of Pennsylvania's Information Security Architecture has provided real and measurable value to the citizens of the Commonwealth. The development and effective distribution of security policies and awareness training ensures that all users of Commonwealth IT resources are aware of their responsibilities. Increased efforts to share information with other states, the federal government and local governments greatly improve the Commonwealth's situational awareness when incidents or threats are detected.

The establishment of enterprise standards and the use of enterprise license agreements have resulted in real savings of over **$27 million** to the Commonwealth for the purchase of security-related solutions. Leveraging enterprise expertise and support contracts has also resulted in significant savings in consulting fees as solutions are commonly shared between agencies.

The Commonwealth now has a centralized monitoring and auditing capability to detect security vulnerabilities and violations at all levels of the enterprise. The security tools now provide the CISO with an enterprise view of security events which can be quickly correlated to determine the source and impact of an attack.

This fiscal year, the security tools have detected and/or blocked over one hundred thousand viruses, one hundred thousand spyware/adware attempts, three hundred million host intrusion events and four million inappropriate Internet usage attempts. The enterprise patch management solution allows easy identification of vulnerable systems and saves an estimated **$6 million per year** in time savings from its automation capabilities. The Commonwealth estimates it has saved **over $33 million** in avoidance of lost productivity caused by virus and worm outbreaks (based on an estimate from 2004 attacks and outbreaks).

Uniform security standards, policies and procedures ensure that the latest security patches and other security solutions are applied in a timely manner throughout the enterprise. Web filtering standards ensure that Commonwealth user Internet access is secure and productive. The implementation of centralized and shared services has enabled improved compliance monitoring, which, in turn, has allowed the Commonwealth to provide assistance and guidance to agencies that struggle with information security issues.
Finally, improving the confidentiality, availability and integrity of Commonwealth information has led to increased citizen confidence in the government's ability to provide electronic services and effectively guard citizen data.