
MANAGEMENT DIRECTIVE

245.19

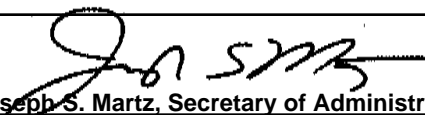
Number

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE

Subject:

Enterprise Technology Security Council

By Direction Of:


Joseph S. Martz, Secretary of Administration

Date:

May 3, 2006

This directive establishes the Commonwealth of Pennsylvania Enterprise Technology Security Council.

1. PURPOSE. The Governor's IT Governance Executive Order, 2004-8 tasked OA/OIT with the responsibility to deploy enterprise-wide technology, including establishing product standards, technical reviews of agency systems, and establishing security procedures and protocols. The purpose of the Enterprise Technology Security Council (ETSC) is to make recommendations aimed at improving the security of Commonwealth computer systems and the information that resides on them. The ETSC will assess security policies, procedures and solutions within the Commonwealth's information technology systems, services, and resources and develop recommendations for increasing their effectiveness. In addition, the ETSC will analyze principles of conduct for system administrators and provide policy and procedure recommendations. The ETSC will assess technical monitoring of administrative activities and make recommendations to ensure full cycle accountability and compliance with policies and procedures. The ETSC will support the development of information technology self-assessment tools for internal security auditing and compliance and will make recommendations for enterprise security best practices.

2. SCOPE. This directive applies to all individuals in departments, boards, commissions, and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow the policy and procedures stated in this directive.

3. DEFINITIONS.

a. Enterprise Technology Security Council. A team of Commonwealth employees created by this management directive who will assess security policies, procedures, and solutions within the Commonwealth's information technology systems, services, and resources and develop recommendations for increasing their effectiveness.

b. Chief Information Security Officer (CISO). The Commonwealth's lead resource responsible for establishing and enforcing Commonwealth security policies.

4. BACKGROUND. In the past, OA/OIT has been forced to disable Internet access to an entire agency during non-contained virus outbreaks. At the same time, the number of cyber attacks has increased over the last three years. This has resulted in millions of dollars in lost productivity and Commonwealth assets.

The Commonwealth seeks to alleviate the need to shut down an entire agency by providing more granular monitoring of devices with the purpose of containing an outbreak at its initial source, which helps prevent additional infections from spreading to other devices and other agency networks. Due to the demand for online government services, risks have increased in the following areas:

- a. loss or compromise of sensitive data.
- b. interruption of services to citizens.
- c. loss of federal funding (HIPAA, CJIS, etc.).
- d. litigation and legal liability.
- e. interruption of business operations.
- f. public safety and Homeland security.
- g. loss of productivity.

5. RESPONSIBILITIES.

The responsibilities of the Enterprise Technology Security Council shall be to:

- a. provide independent oversight of the administrators.
- b. support the vision of standards of excellence in IT security governance.
- c. address the challenge to create cost effective and comprehensive security initiatives.
- d. partner in the development of security standards, policies, and solutions for increased protection of Commonwealth resources.

6. GOALS and OBJECTIVES.

- a. The goals of the Enterprise Technology Security Council shall be to:
 - (1) support the vision of standards of excellence in IT security governance.
 - (2) address the challenge to develop cost effective and comprehensive technology security initiatives.
 - (3) partner in the development of security standards, policies and solutions for increased protection of Commonwealth technology resources.
 - (4) provide oversight of administrator activities.
 - (5) assess and monitor security policies, procedures and solutions within the Commonwealth's information technology systems, services, and resources and development of recommendations for increasing their effectiveness.
 - (6) provide direction around enterprise technology security policy and serve as a monitor of the activity carried out by the Enterprise Administrators, as well as the agency administrators.

(7) analyze principles of conduct for system administrators and provide policy and procedure recommendations.

(8) make recommendations aimed at improving the security of Commonwealth computer systems and the information that resides on them.

(9) monitor administrative activities and make recommendations to provide for full cycle accountability and compliance with policies and procedures.

(10) support the development of information technology self-assessment tools for internal security auditing and compliance and will make recommendations for enterprise security best practices.

(11) address security concerns, risks, vulnerabilities, best practices, and ultimate enterprise-wide adoption to increase the security of Commonwealth information, systems and assets.

b. Objectives:

(1) develop an effective process that creates a continuous enterprise security life cycle

(2) implement a formal business relationship between OA/OIT and all agencies, boards, and commissions under the Governor's jurisdiction that addresses the need for a comprehensive enterprise security approach.

(3) formulate an ETSC for the purpose of providing recommendations on enterprise security policies, processes, procedures, and solutions.

7. POLICY. OA/OIT is charged to formulate and implement an ETSC for the purpose of providing recommendations on enterprise security policies, processes, procedures, and solutions. The ETSC will assess security policies, procedures, and solutions within the Commonwealth's information technology systems, services, and resources and develop recommendations for increasing their effectiveness. In addition, the ETSC will analyze principles of conduct for system administrators and provide policy and procedure recommendations. The ETSC will assess technical monitoring of administrative activities and make recommendations to ensure full cycle accountability and compliance with policies and procedures. The ETSC will support the development of information technology self-assessment tools for internal security auditing and compliance and will make recommendations for enterprise security best practices. The ETSC shall abide by the policies and procedures set forth in the Bylaws of the ETSC as adopted by the ETSC.