Ohio Department of Administrative Services
John Kasich, *Governor*
Robert Blair, *Director*
Stuart R. Davis, Assistant Director/State CIO

Memorandum

To: Agency Directors, CIOs and lead IT Administrators

From: David Shaw, State Chief Information Security Officer

CC: Stuart R. Davis, Assistant Director / State Chief Information Officer

Joe Bell, Chief Audit Executive

Cynthia Klatt, Chief Auditor

Maria Jackson, Assistant Chief Auditor

Date: April 19, 2011

Re: Publication of State IT Standard: Enterprise Security Controls Framework

---

The DAS Office of Information Security and Privacy is pleased to announce the adoption and publication of the new state standard for security controls, ITS-SEC-02 Enterprise Security Controls Framework. The adoption of this standard is a significant milestone for Ohio. For the first time we will have a single standard to evaluate the security posture of individual agencies and the enterprise as a whole.

This standard sets the baseline security requirements for all agencies and establishes a security architecture or roadmap of controls that must be considered for all state systems. The standard is based on established best practices that have been vetted by both public- and private-sector security professionals. One of those best practices is the National Institute of Standards and Technology (NIST) special publication 800-53 (SP 800-53). The NIST framework is a comprehensive set of controls originally created for federal systems but is well suited for adoption by states as well. In 2009, the National Association of Chief Information Officers (NASCIO) had this to say about SP 800-53:

"Though it is designed specifically for government information security programs and applies most directly to federal agencies, a wide array of state programs that are recipients of federal funding are increasingly and more formally subject to FISMA requirements. These have directly impacted unemployment insurance, Medicare and Medicaid services, homeland security, IRS, and social security-related programs.

For these reasons, several states, including Kansas, Michigan, Minnesota, and Tennessee have chosen NIST standards, particularly 800-53, as the base framework for their security programs. Auditors in those states are using NIST checklists in the course of regular auditing."

In addition to adopting the NIST framework as our security architecture, we selected several enterprise controls. These controls are a subset of the NIST framework and apply across the entire enterprise. The selection of these controls was based on another best practice standard called the Consensus Audit Guidelines or CAG. The CAG is a listing of 20 specific controls selected to address the currently known high priority attack techniques. The CAG was developed as a collaborative effort involving both public- and private-sector security professionals to address the initial question of "where do we start?" and is widely held as an excellent starting point for a security program.

The security standard was subject to a rigorous research, development and quality control process and was recommended collaboratively by the Chief Information Security Officer Leadership (CISO-L) Subcommittee consisting of representatives from 14 state agencies. In addition to the CISO-L,

analysts with Gartner, the Multi-Agency CIO Advisory Council, and neutral third-party reviewers were consulted during the development.

As agencies embark on implementing this standard, the DAS Office of Information Security and Privacy will be available to assist you in answering questions and providing direction. The CISO-L Subcommittee will continue to work in this area to develop model policies, guidelines, opportunities for enterprise spend or adoption and to help identify centers of excellence to serve as models for other agencies.

With the adoption of this standard, the ITP-B series of statewide security policies will be rescinded and placed under review. We expect this review to be completed by the end of the fiscal year. During the review period we will replace policies as they are revised and notifications will be sent out regarding the revisions. It is our intent to keep statewide security policy to a minimum and instead use standards to govern specific control requirements. In every case we will be aligning with the NIST 800-53 control listing. As a reminder, statewide policy and standards are the minimum requirements. Agencies may, at their discretion, implement more stringent requirements to address a specific need.

As always, feel free to contact me directly if there is anything I can do to help you in protecting the state's information resources. My contact information as well as contact information for the office is listed below.

David J. Shaw, MBA, CISSP, CDMP
State CISO
Office of Information Security and Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 E. Broad Street, 40th Floor
Columbus, OH 43215

614.644.9391 Office
614.357.7660 Mobile

(Email) State.ISP@oit.ohio.gov

(Web) www.infosec.ohio.gov