Department of Administrative Services
Information Security Office

Update to the Chief Information Officers Council
January 27, 2005

Current Projects:

Risk Assessment – developing questions and methodology to do agency interviews to establish current risk, identify methods for reducing risk and seeking common issues suitable for collaborative resolution.

Computer Security Incident Response Team – developing a proposal outlining responsibilities, authorities, operations, membership, implementation and other aspects of the team for review by CIO Council Security Committee.

Awareness Training – sponsoring a one-time presentation by FBI Special Agent David Schwarz on February 3rd open to all employees. Developing an on-line awareness training program with ITE and offering awareness presentations in March and April.

IT staff technical training – will pay for technical training for agency IT staff that is directly or indirectly related to security. Training must be completed by April 30th.

Vulnerability assessments – will cover the cost of a few agencies to hire assessments done of their current security posture. Offer will go first to those agencies that have expressed an interest in having an assessment done, but don't have the money to do it.

Special projects – some agencies have come to us with requests to help them address specific security issues. We are funding resolution of the problems. Any agency is welcome to request assistance for specific, critical security issues.

DAS COOP Plan – coordinating the development of the DAS Continuity of Operations Plan and will also assist with coordination of enterprise-wide continuity planning around availability of information resources.

Information Security Office Intranet site – working with ITE to establish an Intranet site to share information and provide assistance.

MS-ISAC – member of the Multi-State Information Sharing and Analysis Center, a US Homeland Security supported organization associated with US-CERT (Computer Emergency Response Team), to tie our work into national coordination efforts.

EIP Implementation Planning – involved in planning process for the implementation of the EIP recommendations. Security considerations should be a part of all discussions, so systems are inherently secure, when possible.

Implementation of the Enterprise Information Security Policy – assisting agencies in their efforts to become compliant.

Enterprise Information Security Policy
January 27, 2005

Moving toward compliance.

The CIO Council approved an Enterprise Information Security Policy and it was subsequently approved without modification by the director of the Department of Administrative Services. The policy is intended as an overarching guide for information security across the enterprise, but in a few cases lays out specific measures to be achieved. Also in a few cases, explicit timeframes are outlined.

The enterprise policy was a recommendation of the Governor's Cyber Security Task Force. The Task Force further recommended that each agency either reach full compliance within nine months of the effective date of the policy or demonstrate to the state Chief Information Security Officer significant progress toward becoming compliant. The goal was to encourage quick adoption of those measures that are achievable, while recognizing that some agencies, despite their best efforts, may not be able to comply with all requirements that quickly.

The effective date of the policy is when it is distributed to agency directors, which should be soon, giving each agency until about November 1, 2005, to become fully compliant or show that they have made measurable progress. In those areas where they are not compliant, they will be asked to submit a plan that includes the date when they expect to be.

IWD prepared a worksheet outlining each of the policy statements with space to document current status, when things are to be done and what is left to accomplish. A blank worksheet, with only minor modification, will be sent to the CIO list. It looks to be a good tool for tracking what has already been done and what still needs to be done.

When reviewing the information security policy, please consider the "big picture" and not just "tasks" that have to be accomplished. Many of the policy requirements are broad goals, which could be achieved in different ways. Many are on-going activities that are never completely finished. In those cases, it is important to develop processes to regularly review and update the measures that are in place.

The long-term goal is for security to be inherent in everything we do, not an added requirement. As you move forward with implementation of the enterprise policy, please look for ways to "build it in" not "tack it on." Also, remember that you don't have to do it all yourself. Consider innovative ways of working with others, bringing in outside resources to assist or having someone else do it for you. The ISO is anxious to work with agencies to develop efficient and effective ways of securing our valuable resources.