

## **ATIC PLATFORM STATEMENT**

### **CYBER SECURITY**

Communications and electronically stored information is becoming increasingly important in every aspect of our culture, including our physical, political, and economic lives. Cyber security in this context is defined to include the protection of transmitted, stored or processed public information, and any and all shared transmission infrastructure. It is a basic stewardship of government.

Recent events, including terrorist attacks against our nation and various well-publicized intrusions into vital public records via the Internet, have pointedly shown the vulnerability of our current situation. Less publicized but equally serious to us are the frequent local attempts of intrusion into public and private networks, and widespread infections by so-called "viruses." These attacks are debilitating, and in the aggregate, have cost the state and its citizens many millions of dollars. They remind us that our electronic data integrity and critical information, as well as the data infrastructure is increasingly at risk.

The state is currently well behind in assessing its specific Cyber Security needs. Such needs assessments must be completed. Outcomes of these needs assessments should include the strategic plans and activities that will protect our information infrastructure and data repositories, should provide sufficient safeguards to maintain our citizens' rights to privacy, and should promote education of citizens, business and government leaders about the risks of data corruption and destruction, and the best practices required or mandated to minimize risk. The state must also include in this planning, upgrades of our substantially inadequate electronic records management and archiving policies. If improvements are not made quickly, vital original electronic documents will be lost forever, short-changing future generations of their civilizing records and history.

It is incumbent upon our elected officials to provide both the leadership and the funding necessary to reverse these fast growing cyber and data vulnerabilities. It is nearly impossible to overstate the urgency for best practices to be defined, and for policies to be formulated, disseminated, and implemented both in government and in the private sector. Current costs of intrusions and malicious attacks have been substantial. Without appropriate levels of investments in these areas, future costs to the citizens of the state could be catastrophic.