Executive Summary
Alabama's Comprehensive Information Security Program

For years and years, Alabama's approach to information security had been one of institutionalized decentralization. Each functional unit did the best they could at protecting the information resources entrusted to their care. This approach worked well in a point-to-point SNA network environment with most of our information assets housed on the State's big mainframe computers in datacenters protected by heavy doors with keycard entry, automatic fire suppression systems, and battery backup systems with generators to keep them charged. In addition, the data was protected by RACF and was considered as safe as it could be.

Suddenly the environment changed to a TCP/IP based network. To nobody's surprise, it was discovered that an IP based network with servers scattered all over the state and a very large pipe to the Internet required a totally different approach to security.

Various attempts to get our corporate arms around security met with mixed support and limited success. In mid 2005, a new State Chief Information Officer embraced the idea of having a Security Officer and a structured approach to information security. For the past two years, the Information Services Division has taken the lead role in securing the information assets of the State of Alabama.

These efforts have included the retention of two security business partners to assists us in our security efforts, the creation of the Office of Information Security, the sanctioning of the Information Security Council, development of a Cyber Security Management Plan, participation in national security focused organizations, and a myriad of security related activities associated with each of the aforementioned.

Alabama now has a much improved security posture, as well as leadership and staff who realize that security is everybody's business and that it is a process, not an event.

Alabama's Comprehensive Information Security Program

A. Concise description of the business problem and solution, including length of time in operation.

The business problem facing Alabama's Information Services Division (ISD) is how to adequately secure Alabama's information resources while providing citizen access to the State controlled information that they demand and deserve. This challenge is compounded by the ever changing nature of the environment as well as limited resources available. ISD, as the central information technology authority for the Executive Branch of government has the responsibility of providing enterprise solutions to common technology problems faced by the customer agencies and information security certainly falls within that responsibility.

The solution was initiated approximately two years ago when the decision was made by ISD's new Chief Information Officer to formalize ISD's information security efforts. The position of Information Security Officer was created with that position reporting to the ISD Assistant Director for Planning, Standards and Compliance. An Office of Information Security was created to by lead by the Information Security Officer. Contracts were signed with two information security focused business partners to assist with the development of a formalized information security management approach. Accomplishments over the past two years include:

Creation and publishing of a comprehensive set of policies, procedures, and standards (National Institute of Standards and Technology based) to be used by ISD, and our customer agencies, to address information security issues. As of today this set includes the following:

Policy 600-00: Information Security
Policy 600-01: Commitment to Information Security
Policy 600-02: Information Security for Service Providers
Policy 600-03: Security Council
    Procedure 600-03P1: Security Council
    Procedure 600-03P2: Security Document Workflow
Policy 600-04: Cyber Security Incidence Response
    Standard 600-04S1: Incident Response Controls
    Procedure 600-04P1: Cyber Security Incident Reporting
Policy 610-01: Security Awareness & Training
    Standard 610-01S1: Security Awareness
Policy 620-01: Network & Systems Access
    Standard 620-01S1: Access Management

- Policy 620-03: Authentication
  - Standard 620-03S1: Authentication - Passwords
  - Standard 620-03S2: Authentication - Biometrics
- Policy 630-01: Acceptable Use
  - Standard 630-01S1: Acceptable Use - Prohibited Activities
- Policy 630-02: Internet Access
- Policy 630-03: Email Usage
  - Standard 630-03S1: E-Mail Usage
- Policy 630-04: Instant Messaging
- Policy 630-05: Internet Content Management
  - Standard 630-05S1: Internet Content Management - Blocked Categories
- Policy 630-06: Software Licensing & Use
- Policy 640-01: External Connections
  - Standard 640-01S1: Interconnecting IT Systems
  - Standard 640-01S2: Secure Web Application Deployment
- Policy 640-02: Remote Access
  - Standard 640-02S1: Remote Access Controls
  - Standard 640-02S2: Virtual Private Networks
  - Standard 640-02S3: Dial-in Access
  - Standard 640-02S4: Remote Maintenance
- Policy 640-03: Wireless Security
  - Standard 640-03S1: Wireless Networks
  - Standard 640-03S2: Wireless Clients
  - Standard 640-03S3: Bluetooth Security
- Policy 640-04: Voice Over Internet Protocol
  - Standard 640-04S1: VoIP Security
- Policy 650-01: Physical Security
  - Standard 650-01S1: Physical Security
  - Standard 650-01S2: Access Management
- Policy 660-01: Application Security
- Policy 660-02: System Security
- Policy 670-01: Risk Management
  - Standard 670-01S1: Risk Assessment
  - Standard 670-01S2: Risk Mitigation
  - Standard 670-01S3: Vulnerability Scanning
- Policy 670-02: Monitoring and Reporting
  - Standard 670-02S1: Monitoring and Reporting
- Policy 670-03: Vulnerability Management
  - Standard 670-03S1: Vulnerability Management
- Policy 670-04: Virus Protection
  - Standard 670-04S1: Virus Protection
- Policy 670-05 Intrusion Detection/Prevention
  - Standard 670-05S1: Intrusion Detection/Prevention Systems
- Policy 670-06: Log Management
  - Standard 670-06S1: Log Management

Policy 670-07: Backup and Recovery
    Standard 670-07S1: Backup and Recovery
Policy 680-01: Information Protection
    Standard 680-01S1: Information Protection
    Standard 680-01S2: Protecting PII
    Standard 680-01S3: Removable Storage Devices
Policy 680-02: Public Information Dissemination
Policy 680-03: Encryption
    Standard 680-03S1: Encryption

All of these documents are available as PDF's to our customers, as well as the general public at http://isd.alabama.gov/policies/policies.aspx .

Creation of a Cyber Security Awareness web site which contains Cyber Security Tips for Adults, Cyber Security Tips for Children, Cyber Security Tips for Local Government, Training Opportunities, Monthly Newsletters and 3 security videos. This site is available to our customers and the general public on our portal at http://www.alabama.gov/portal/secondaryContent.jsp?page=Standard_Security .

Formation of a Security Council which meets monthly to discuss information security related matters and make decisions regarding agency related security issues. The Council is chaired by the Information Security Officer and its membership includes four ISD Assistant Directors, two large agencies IT Directors, and numerous technical staff. The Council is governed by a set of procedures which incorporates standardized forms and workflow for the dissemination of information and action items to the members.

Development of Incidence Reporting procedures to be used by ISD staff and customer agencies to report any suspected information security incident to ISD for investigation and appropriate action.

Development of Incidence Response procedures, and supporting forms, which are used by the incident response team in response to a reported suspected incident. These procedures, and forms, are not publicly due to the sensitive nature of the procedures.

Development of HIPAA Security Rule Requirements for the State of Alabama Information Technology Networks. This document delineates the responsibilities of the agencies (the Covered Entities) and ISD (a business partner) in relationship to the HIPAA Security Rule.

Development of a Conceptual Information Security Office Structure. This document is being used as the guide for staffing the Information Security Office.

All of the aforementioned, as well as others not mentioned, have been incorporated into the State of Alabama Cyber Security Management Plan. This plan is a first for Alabama and is used to guide ISD's every move when it comes to information security issues. The plan is constantly being modified to address the changing environment of information security. In addition, the Information Security Officer has become an active member of the Multi-State Information Sharing and Analysis Center (MS-ISAC). This association is extremely valuable to Alabama because of the timeliness of security related information that is disseminated to the members and the business relationships developed through partnering with all the other states on security related issues.

B. Significance to the improvement of the operation of government.

The formalization of a comprehensive information security program has improved the operation of government in several ways. First, not every information security situation has to be taken on as a project for a layperson to resolve. By having a comprehensive set of policies, procedures, and standards available for use, security can be built in up-front by using the information already available. This greatly reduces the time necessary to complete many projects with security implications. Second, if a particular issue or situation is not addressed in a published document, there is a structured approach to having it addressed by the Security Council with the result being a viable, secure solution and, when appropriate, new policies and/or standards to address the need in the future. In addition, the relationships developed with business partners, agency security staff, and the other states has greatly enhanced ISD's ability to respond appropriately to security issues and incidences.

C. Benefits realized by service recipients, taxpayers, agency or state.

The benefits resulting form ISD's efforts impact service recipients, taxpayers, our customer agencies, and the State as a whole.

Service recipients and taxpayers, who in many cases have personal information stored on a State owned resource, have the assurance that the State is taking a standards based approach to protecting their information. By modeling our policies and standards after NIST, we are taking the approach that the Federal counterparts of many of our agencies are taking in the protection of personally identifiable information. NIST has been involved in security for much longer than ISD and the taxpayers are reaping the benefits of their experience.

In addition, by having private sector business partners involved in our efforts the taxpayers are benefiting from years of experience in the implementation of best practices regarding the security of their personal information.

Our customer agencies are benefiting from our efforts because they are being provided a framework within which they can create their agency specific security policies, procedures, and standards without having to start from scratch on them. This benefits them in a couple of ways; first, they can point to us as the "bad-guys" if their management, or clients, question a particular security feature being incorporated into a business process or application. In addition, our documents can be used as-is or they can be strengthened should the agency have the need for a higher level of security in a particular area hence reducing the time necessary for them to complete policies, procedures, and standards for their agency. Also, our business partners provide us the ability to offer specialized security services (i.e. security assessments) to our customer agencies that would not be available under a less comprehensive program.

The State benefits from our security program because the Information Security Officer, as well as two Assistant Directors, actively participates in MS-ISAC and this exposes Alabama to a myriad of security related resources and contacts in the Federal Government, other states, and the private sector. This exposure accelerates and strengthens Alabama's knowledge of security related issues and our ability to respond to them.

D. Realized return on investment, short-term/long-term payback (include summary calculations).

It is difficult to quantify in dollars the actual return on investment for our security program: however, many of the benefits derived from our program have obvious financial implications. By partnering with private sector security companies and taking a standards based approach to our policy, procedures and standards development; we have saved untold hours in the development of these documents as compared to starting from scratch. These savings trickle down to the agencies in that they can adopt our documents as their own or use them as a starting point for their development; again savings of many man hours of development time. Savings are realized by having a standing Security Council, with formalized procedures for addressing issues, as opposed to addressing each issue that comes up as a separate project. The Council often solves issues for multiple agencies by providing one new security solution or standard.

The short-term payback has been ISD's ability to quickly assume a leadership role among the agencies looking to us for security solutions. Agencies now come to us for solutions instead of going out on their own and spending more taxpayer dollars.

The long-term payback is a more secure infrastructure which further promotes the use of electronic services by the citizens of Alabama which, in-turn, reduces the costs associated with the movement of paper through the various agencies. In these times of reduced budgets, reduced staff, and increasing demand for services; electronic government is becoming crucial and information security will become more and more critical.