

State of Alaska
State Security Office
Charter

***“Providing Leadership In Securing
Our Telecommunications and Information Technologies”***

17 March 2006
Version 1.2

Mission:

The mission of the State of Alaska (SOA) Security Office is complex and has multiple functions. The primary mission is to develop and recommend a Strategic Enterprise Security Plan to protect the telecommunication and information assets, data, systems, and networks that deliver the communications and information from damage resulting from failures of confidentiality, integrity, and availability.

Focus:

The SOA Security Office will meet the security mission by applying a primary focus on policy, SLA, project and process management, applying a unified defense in depth security model and promoting security awareness and training.

The SOA Security Office will perform these tasks by utilizing a collaborative and centralized support model to monitor, report, identifying, and mitigate the threats, risks and liabilities to the telecommunication and information technology assets, services, systems, networks and data of the Executive Branch, and by working collaboratively with the Legislative and Judicial Branches of State of Alaska government.

Business Drivers/Background:

The State of Alaska for many years has relied heavily on the application of computer-based systems for the efficient and effective management of complex governmental operations. Rapid and continuing technical advances in information processing have increased the dependence of state agencies and the public on information and automated systems.

The value of data and software, in terms of restoration costs or losses, entrusted to State employees far exceeds the value of its associated hardware. For that reason, recognition must be given to the fact that information processed by computers is a significant state asset and requires protection accordingly.

The purpose of the State Security Office is to provide solution recommendations that create an environment within the State of Alaska enterprise that maintains system security, data integrity and privacy by preventing unauthorized access to data, and by preventing misuse of, damage to, or loss of the information entrusted to State employees.

Ultimate responsibility for the selection of the controls to offset threats, create policies and procedures, deploy tools and provide active support (resources) to protect the state's telecommunication and information assets is placed upon executive management. The State Security Office exists to assist, recommend, research, educate and provide solutions to management in respect to this responsibility.

Vision:

The vision for the State Security Office is one of a functioning professional group of individuals from various state entities and strategic partners committed to effecting changes in security management of the state's vast investment in telecommunications and information technology.

The State Security Office team members will be comprised of individuals who have been duly appointed by, via the delegated authority to, the State Chief Security Officer to make decisions based on the premise of weight and balancing against specific and unique needs of the enterprise.

Goal Statement:

The State of Alaska government has been entrusted by the citizens of our state with ensuring and maintaining the confidentiality, integrity, and availability of the telecommunication and information assets, data, systems, networks, and services within the state government. The State Security Office takes this responsibility seriously.

As such, the Goal of the State Security Office is to work in collaboration with state agencies in the development of the processes that will ensure the implementation of the State of Alaska Security Framework in the use of all telecommunication and information systems, services, processes, or assets for the State of Alaska Enterprise. However, in this collaborative spirit, the state agencies must also acknowledge no electronic services or functions can be adequately maintained without paying due diligence to security.

Objectives:

- Define common security requirements applicable to all state agencies.
- Assess and improve the security of state telecommunication and data resources and the information derived from data resources.
- Ensure consistency and uniformity in the state agency's telecommunication and information security programs.

- Ensure continued confidentiality, availability and reliability of state telecommunication and information assets and resources.
- To provide security education and awareness to state agency's staff.

Scope:

The State Security Office is charged with providing security policies, solutions and processes that can apply to all state government branch agencies, employees, contractors, partners or vendors that operate or manage telecommunication and information technology services, equipment or data to support state business functions.

All government agencies or branches, corporations or entities, local or federal government, and all public or private entities that need or desire access to those telecommunication and technology services, equipment or data, beyond such access that is available to the general public, must adhere to the decisions, policies, procedures and standards of the State of Alaska government. The State Security Office will ensure adherence to all applicable state and federal laws, regulations, statutes, administrative codes, orders and directives, policies, and procedures, and standards.

High Level Deliverables:

- Work collaboratively with all state entities to ensure a unified defense in depth structure and processes that protect the assets, information, networks and systems of the State of Alaska government.
- Act as Lead in the remediation of threats, risks and liabilities to the State of Alaska telecommunication and information assets.
- Ensure adherence with the security mission of the state.
- Provide Enterprise security monitoring, reporting, assessments, and mitigation techniques.
- Continued development of processes which support the refinement and revision of Strategic Enterprise Security Mission Plan.
- Continued development of the Enterprise Security Framework.
- Continued development of the Enterprise Security Policies, Procedures, Guidelines and Directives.

Role and Responsibility:

State Security Office

The State Security Office is governed by the State of Alaska Executive Management and is in support of state statute. The State Security Office, by the delegated authority from the Commissioner of Administration, is directed to ensure the confidentiality, integrity, and availability of the State of Alaska Executive Branch Government entrusted, owned, or operated telecommunications and information technology services, systems, data, and resources (assets). To include, but not limited to, all government branches, agencies, corporations, or other government entities (whether local or federal); and all public or private entities and persons that need or desire access to those said

telecommunication and technology services, systems, data, or resources beyond such access that is available to the general public.

The State Security Office will ensure the confidentiality, integrity, and availability of State assets, by creating policy, procedure, guideline, and directive recommendations to the Commissioner of Administration and/or the Enterprise Investment Board via the Director of the Enterprise Technology Services Division and by providing security training and awareness programs for all government employees. The State Security Office will actively participate in the education and enforcement of any adopted security policies, procedures, guidelines, and directives.

The Department Computer Security Designee's (DCSD) and Department Information Security Officers (ISO's)

The State Security Office will utilize the DCSD's and/or DISO as the primary department liaison for security issues within each department. Each DCSD or DISO will be responsible for directly engaging their department staff to facilitate security planning, education and awareness programs and actively participating in the enforcement and assurance of State and Department Security Policies, Procedures, and Guidelines.

Technology Management Council (TMC) and Functional Work Groups (FWGs)

The State Security Office will support the TMC and FWGs by providing security reviews and recommendations on department IT plans, product solutions recommendations, waiver requests, and ensure general compliance with the State Security Policies, Procedures, and Guidelines on solutions being deployed within the Executive Agencies. The State Security Office may also utilize the TMC, or FWGs, as a forum of vetting security procedures and guidelines that the Security Office may submit as recommended processes to the Commissioner of Administration and/or the Enterprise Investment Board for adoption.

State Incident Response Team (IRT)

The State Security Office will develop and lead an Incident Response Team. The IRT will assist the State Security Office in the event of a major incident and maybe empowered by the State Security Office to assist in the remediation of incidents and/or vulnerabilities within State Telecommunications or Information Systems or Information. The State Security Office may also utilize the IRT as a forum of vetting security policy that the Security Office may submit to the Commissioner of Administration and/or the Enterprise Investment Board for adoption.