Emergency 911 Compliance-Coordination Project/Network Security | **FY2007 Request: $2,689,500** | **Reference No: 41806**

AP/AL: Allocation
Project Type: Information Systems
Category: Public Protection
Location: Statewide
Contact: Eric Swanson
House District: Statewide (HD 1-40)
Contact Phone: (907)465-5655
Estimated Project Dates: 07/01/2006 - 06/30/2011
Appropriation: ETS Technology Projects

Brief Summary and Statement of Need:
This request includes E-911 project development/deployment to ensure that all State of Alaska government office telephones route dialed 911 call to the proper PSAP (Public Safety Answering Point) - displaying both the telephone number and the physical address of the phone and four (4) projects relating to the Network Security Initiative (NSI). The NSI project is a continuation that was begun in FY2005 & FY2006 to address the security vulnerabilities from a Cyber attack on the State of Alaska's network infrastructure in January 2005.

Funding:	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	Total
Gen Fund	$2,689,500						$2,689,500
Total:	$2,689,500	$0	$0	$0	$0	$0	$2,689,500

☐ State Match Required ☑ One-Time Project ☐ Phased - new ☐ Phased - underway ☐ On-Going
0% = Minimum State Match % Required ☐ Amendment ☐ Mental Health Bill

Operating & Maintenance Costs:

	Amount	Staff
Project Development:	0	0
Ongoing Operating:	0	0
One-Time Startup:	0	
Totals:	0	0

Additional Information / Prior Funding History:
Funding in the amount of $382,375 was appropriated in FY 2006, and $235,535 was appropriated in FY 2005.

Project Description/Justification:

Project Name	**Amount (in thousands)**	**Fund Source**
E-911 Compliance / Coordination		GF

Problem To Be Solved: To ensure that all SOA Government office telephones route dialed 911 calls to the local Public Safety Answering Point (PSAP) – displaying both the telephone number and the physical address of the phone.

Solution: Incorporate E911 call routing using existing (PBX) and proposed Voice over Internet Protocol (VoIP) telephone systems into the telecommunications infrastructure to ensure compliance with

federal E911 requirements.

Benefits: Deployment of E911 functionality within state government will aid communications in the event of a safety of life situation.

What We Propose to Buy: Development of a centralized E911 management system to be leveraged with existing management tools across the enterprise. Cisco's Emergency Responder (CER) solution for the telephones in use today across the State of Alaska enterprise, costs may include:

911 Solution for VoIP & PBX $1,250,000

Solution development and staff utilization of the DMVA strategic plan to refine the requirements and plan for statewide deployment using existing telecommunications providers. Definition of regional PSAPs and the development and creation of a statewide Automatic Number Identification (ANI) and Automatic Location Identifier (ALI) database, costs may include:

911 Solution development $1,500,000

Prior Funding History: No prior year funding history exists.

Timeline: The timeline for deployment within the State of Alaska telecommunications infrastructure serving SOA agencies, will coincide with the proposed deployment of Voice over Internet Protocol (VoIP) telephone system within Juneau, Anchorage and Fairbanks – representing approximately 15,000 phone sets.

The timeline for deployment across the state, using existing telecommunications infrastructures developed and made available through existing providers will take much longer and require a coordinated effort based upon municipal requirements for E911 systems. This effort will have oversight by the state E911 coordinator and the Alaska chapter of NENA (National Emergency Numbering Association).

Explanation of How Project Contributes to Your Divisional Mission: The deployment of E911 systems within the State of Alaska telecommunications network infrastructure meets federal requirements and mandates, which also will ensure a more structured response by emergency service providers to 911 calls. This is an enterprise solution affecting all of the 15,000 phones presently deployed in both the PBX and VoIP environments.

Explanation of How Project Contributes to End Result: These systems have to be in place to meet federal requirements and mandates for the E911 services. These two projects will provide the foundation to the State of Alaska network infrastructure to ensure compliance, and also to create regional PSAPs and the personnel needed to support these systems. Additional information will be forthcoming in the DMVA Strategic Plan that relates to 911 communications.

Project Name	**Amount (in thousands)**	**Fund Source**
Security – NSI Phase II		GF

Problem To Be Solved: These 4 projects are a continuation of the Network Security Initiative (NSI) that was begun in FY 2005 & FY 2006 to address the security vulnerabilities identified from a Cyber attack on the State of Alaska network infrastructure in January 2005

1) **NSI Phase II – DMZ / Extranet Service** relocation will address the deployment of existing SOA agency servers into the newly created Demilitarized Zone (DMZ) from NSI Phase I.

2) **Security Office and Operations Center** – The State of Alaska will create and support a network Security Office and Operation Center that will have the responsibility to monitor and address network security issues on the network infrastructure used by SOA agencies.

3) **Wireless Mobility Security** – The Cisco Integrated Wireless Network cost-effectively addresses the Wireless Local Area Network (WLAN) security, deployment, management, and control issues facing enterprises. This framework integrates and extends wired and wireless networks to deliver scalable, manageable, and secure WLANs with the lowest total cost of ownership.

4) **Event and System Auditing** – This project addresses the need to develop and deploy a means to log network security related events and categorize them by severity levels.

Solution:

1) In FY 2006, the creation of two Enterprise Class DMZ / Extranet environments were funded and installed. This project will allow the state to move all externally exposed services within this new environment.

2) The Security Office and Operations Center will provide a focused and effective response strategy for security issues and improved availability of state services. It will also facilitate a central point for security-related projects and act as the central statewide resource center on network security issues.

3) The deployment of secure enterprise wireless access points will provide wireless mobility as requested in numerous SOA dept IT plans. This will facilitate the movement between conference rooms and offices of portable devices (i.e. laptops, PDAs, etc.). It will also reduce the requirements for cable plants within local LANs and provide proper controls for inbound and outbound wireless traffic.

4) To deploy intelligent network auditing tools within the State of Alaska network infrastructure (WAN and LAN) to interact with Cisco Security Agent (Zero Day protection) and firewalls.

Benefits:

1) Deployment of a secure environment within the state will provide a private/public network environment within the LANs and WAN. This will significantly increase the security profile of the state by making it more difficult to obtain unauthorized access to state resources available via the network.

2) Active auditing and assessments provide a proactive function to ensure the health of SOA networks, systems, services and the IT infrastructure. Minimizes and prevents service interruptions and data loss caused from security issues.

3) Creation of secure wireless access points will help reduce the cost of current wired solutions. It will also enable security policies to be applied to the wireless environment for the state and to ensure controls on inbound and outbound traffic are enforced.

4) Use of a centralized event and system auditing management system will increase staff efficiencies by reducing investigation times of security threats and eliminate duplication of effort.

What We Propose to Buy:

1) Based upon a cost model from the off-site facility where the DMZ was created, ETS proposes deploying approximately 200 remote units (RU) that will facilitate the existing server base on the network today that has been identified belonging in the DMZ / Extranet environment.

$15 p/day x 365 days x 200 = $1,100,000

2) ETS proposes using a Managed Security Services Provider (MSSP) who has been established as a provider of these services for state and local government entities. ETS recommends a 90-day pilot by this provider (proof of concept). If this pilot is successful the provider would then create a

Security Operations Center within the State of Alaska, utilizing professional services staff. The plan is to transition this back to a state managed environment within a 2-year period.

SOC pilot for MSSP (3 month)	$ 75,000
In state SOC (w/ MSSP staff)	$ 719,000

3) ETS proposes purchasing Cisco's Wireless Access Point Solution for deployment.

Wireless access points 350	$ 175,000
Mobility security blades for 6500 switch (4 x $50k)	$ 200,000
Smartnet support	$ 30,000
AAA Server Maintenance	$ 20,000.
Wireless access clients (1000 x $35)	$ 35,000

4) ETS proposes purchasing a system with the following components:

Auditing system	$ 430,000
Hard drives for logging	$ 60,000
Maintenance	$ 10,000

Prior Funding History:

1) $382,370 was authorized prior to FY056 and $235,535 authorized in FY06

2) No prior year funding history exists.

3) No prior year funding history exists.

4) No prior year funding history exists.

Timeline:

1) The timeline to move all externally exposed services within the new DMZ / Extranet environment is dependent upon cooperation and assistance from SOA agencies. ETS intends to complete this process by the end of FY 2007.

2) The timeline for engaging the services of a Managed Security Services Provider is at the beginning of FY 2007, for the "proof of concept" (90 days) and then full engagement of this provider to create the Security Operations Center. ETS expects all associated costs for the SOC to become part of the operational budget beginning in FY 2008.

3) ETS proposes purchasing the Wireless solution in July 2006, and developing a structured deployment plan over the remainder of FY 2007.

4) ETS proposes purchasing the Event and System auditing hardware and software in July 2006, with full implementation when the Security Operations Center becomes functional in FY 2007.

Explanation of How Project Contributes to Your Divisional Mission:

These projects are associated with the Network Security Initiative. They are a continuation and migration of the State of Alaska's network infrastructure into a secure environment. ETS is the agency responsible to deliver computing and telecommunications services to the SOA agencies in the Executive Branch, with participation by the Legislature and Court System as needed. It is ETS' responsibility to ensure a secure and robust environment for those delivered services.

Explanation of

It is imperative for the State to provide a network infrastructure that is secure and protected. In this

How Project Contributes to End Result:	day and age of technology, it is our responsibility to understand the legal requirements for security as it pertains to Information Technology. Funding of these projects will enable ETS to meet our obligation to provide a secure environment.