State of Alaska Network Security Infrastructure Upgrades **FY2006 Request: $3,537,500**
Reference No: AMD 40606

AP/AL: Appropriation
Project Type: Information Systems
Category: General Government
Location: Statewide
Contact: Eric Swanson
House District: Statewide (HD 1-40)
Contact Phone: (907)465-5655
Estimated Project Dates: 07/01/2005 - 06/30/2010

Brief Summary and Statement of Need:
On January 18, 2005 the State of Alaska Wide Area Network was the target of a cyber attack which resulted in the defacement of a web server owned by the Dept. of Health & Social Services. Upon further investigation, it was determined the extent and scope of the cyber attack was much larger than to a single device. In a cooperative effort with SOA agencies, approximately 110 servers appeared to have experience similar "signatures" of this attack. The significance of these attacks prompted notification to the MS-ISAC (multi state information sharing and analysis center).

Funding:	FY2006	FY2007	FY2008	FY2009	FY2010	FY2011	Total
Info Svc	$3,537,500	$12,598,000	$7,449,500	$7,400,000	$10,300,000		$41,285,000
Total:	$3,537,500	$12,598,000	$7,449,500	$7,400,000	$10,300,000	$0	$41,285,000

☐ 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:

Project Description/Justification:
On January 18, 2005 the State of Alaska Wide Area Network was the target of a cyber attack which resulted in the defacement of a web server owned by the Department of Health & Social Services. Upon further investigation, it was determined that the extent and scope of the cyber attack was much larger than to a single device. In a cooperative effort with SOA agencies, it was determined that approximately 110 servers has "similar signatures" of this attack. The significance of these attacks prompted notification to the MS-ISAC (multi state information sharing and analysis center).

This incident as reported prompted the US-CERT (United States Computer Emergency Readiness Team) to assist the State of Alaska with the investigation. A report from this group, in conjunction with an active FBI investigation, limits the amount of information that can be released at this time.

Suffice to say that the State of Alaska network infrastructure is vulnerable to continued cyber attacks that may result in the destruction or compromise of sensitive data. In response to the potential loss of connectivity to federal communications networks (i.e. NLETS, NCIC, Medicaid, etc) for ignoring this vulnerability, ETS has prepared a budget request to immediately address network infrastructure vulnerabilities in FY05, with a long range plan to be rolled into FY06. This matter should be treated as a Priority 1 item for Information Technology and funded as soon as possible.

A consortium (Northrop Grumman, GCI and Cisco Systems) effort with ETS technical staff, has prepared a detailed expenditure report outlining specific costs that will address the vulnerabilities outlined in the US-CERT initial report to the State of Alaska. The total costs for this proposal in FY2006 is $ 1,969,411 with the breakdown as follows:

SOA Network Infrastructure Upgrade Costs

Cisco Security Agent (CSA)

	Equipment Cost	Equipment Maintenance	One-Time Services	Recurring Yearly Services	Servers	Cabling	Trade-ins	Project Total	Needed in FY06
List Price	1,856,485	409,072	1,265,170	221,156	98,932	742		3,851,557	
Discounted Price	1,147,308	327,258	1,265,170	221,156	98,932	742		3,060,565	1,265,257

Cisco Security Agent – A “host-based” intrusion prevention system. This is software based application that resides on servers and personal computers. It purpose is protect against known and future cyber threats. This component also includes $40k PMO for all of these security projects and a $350k server/workstation upgrade needed for CSA deployment.

Demilitarized Zone (DMZ)

	Equipment Cost	Equipment Maintenance	One-Time Services	Recurring Yearly Services	Servers	Cabling	Trade-ins	Project Total	Needed in FY06
List Price	618,730	66,282	141,528	13,340	24,639	3,000		867,519	
Discounted Price	382,375	53,026	141,528	13,340	24,639	3,000	-	617,907	235,532

DMZ – (pronounced as separate letters) Short for demilitarized zone, a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

Core (Juneau, Anchorage & Fairbanks Network Control Centers)

	Equipment Cost	Equipment Maintenance	One-Time Services	Recurring Yearly Services	Servers	Cabling	Trade-ins	Project Total	Needed in FY06
List Price	1,800,295	147,762	143,181					2,091,238	
Discounted Price	1,112,582	118,210	143,181				-	1,373,973	261,391

Core upgrades – routers that reside in the network control centers that are “end of life” and cannot support the infrastructure upgrades for operating systems that provide security to the network.

Hub Routers (Wide Area Network)

	Equipment Cost	Equipment Maintenance	One-Time Services	Recurring Yearly Services	Servers	Cabling	Trade-ins	Project Total	Needed in FY06
List Price	1,237,605	77,311						1,314,916	
Discounted Price	764,840	61,849	-				-	826,689	61,849

Hub routers – routers that reside in approximately 44 communities that serve as “hubs” to WAN sites in that community that are “end of life” and cannot support the infrastructure upgrades for operating systems that provide security to the network.

Access Routers (Remote SOA offices on WAN)

	Equipment Cost	Equipment Maintenance	One-Time Services	Recurring Yearly Services	Servers	Cabling	Trade-ins	Project Total	Needed in FY06
List Price	2,058,275	134,277						2,192,552	
Discounted	1,272,014	107,422	-				-	1,379,436	107,422

Price									

Access routers – Routers that are attached via data circuits to “Hub” routers in 44 communities that are “end of life” and cannot support the infrastructure upgrades for operating systems that provide security to the network.

Critical Spares (for SOA WAN)									
	Equipment Cost	**Equipment Maintenance**	**One-Time Services**	**Recurring Yearly Services**	**Servers**	**Cabling**	**Trade-ins**	**Project Total**	**Needed in FY06**
List Price	524,910	47,450						572,360	
Discounted Price	324,394	37,960						362,354	37,960

Critical spares – An inventory of spare equipment for the Wide Area Network (WAN) which consists of specific router and switch types that can be deployed immediately if and when an equipment failure occurs.

Sub-Total **$ 1,969,411**

Also included in the FY2006 capital request is the remaining balance of the original FY2006 requests for System Security and Telecommunications Projects which totals $1,586,076:

ETS Equipment Replacement
This CIP is to replace SOA/WAN routers, Core network upgrades, PC refresh for ETS staff, phones, pagers, printers, satellite phones, cell phones, servers, rack software, video conferencing equipment, and upgrading PC's Productivity Suite to Office 2003.

Proposed FY06
$460,038

Network Convergence & Legacy Replacement
Continue transforming the legacy environment to a converged environment that provides connectivity across data, voice and video platforms. Includes implementing internet protocol telephony (IPT) for additional business functionality while reducing administrative and operational costs and redesigning of wide area network (WAN) in order to provide greater efficiency and support for the IPT deployment.

Proposed FY06	**Proposed FY07**	**Proposed FY08**	**Proposed FY09**	**Proposed FY10**
$460,038	$10,650,000	$7,400,000	$7,400,000	$10,300,000

WebSense Bandwidth Management
Deploy Cisco WebSense software to control, restrict, monitor, and protect the network at the State's primary entry and exit points to the Internet.

Proposed FY06	**Proposed FY07**	**Proposed FY08**
$198,000	$198,000	$49,500

Virtual Tape System Backup
Provide increased capacity for Virtual Tape System housed in the Alaska Data Center - Juneau facility; includes disaster recovery solution.

Proposed FY06	**Proposed FY07**
$450,000	$1,750,000