IT Switch Replacement

FY2025 Request: **$500,000**
Reference No: **AMD 65187**

AP/AL: Appropriation
Category: Public Protection
Location: Statewide
Impact House District: Statewide (HD 1 - 40)
Estimated Project Dates: 07/01/2024 - 06/30/2029

Project Type: Life / Health / Safety
Recipient: NA
House District: Statewide (HD 1 - 40)
Contact: Bob Ernisse
Contact Phone: (907)428-7210

Brief Summary and Statement of Need:
Replacing end-of-life network switches will enhance network reliability and performance, maintaining the Department of Military and Veterans' Affairs (DMVA) high readiness levels. Newer switches support advanced security protocols and bolster cybersecurity defenses. The upgrade aligns with DMVA's strategy to improve operational efficiency and overall readiness while mitigating security risks.

Funding:	FY2025	FY2026	FY2027	FY2028	FY2029	FY2030	Total
1004 Gen Fund	$500,000						$500,000
Total:	$500,000	$0	$0	$0	$0	$0	$500,000

☐ State Match Required ☐ One-Time Project ☐ Phased - new ☐ Phased - underway ☐ Ongoing
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

Prior Funding History / Additional Information:

Project Description/Justification:
Replacing end-of-life network switches is crucial for enhancing network reliability and performance, which is vital for maintaining DMVA’s high operational readiness levels. Newer switches support advanced security protocols, significantly bolstering cybersecurity defenses against increasingly sophisticated cyber threats. It will be an integral part of a highly available, redundant, and resilient infrastructure. This upgrade is not just a technological improvement; it's a strategic investment aligning with long-term goals to improve operational efficiency and overall readiness.

By replacing end-of-life network switches, significant security risks are mitigated. Potential system failures and costly downtime will be avoided. This will also ensure the continuous, secure flow of information crucial for operations during disasters and emergencies. Delaying this replacement could lead to increased vulnerability to cyber attacks, reduced network performance, and potential breaches in sensitive data security, directly impacting operational capability and mission effectiveness.