

Static Code Vulnerability and Analysis Scan for All Public Facing Apps **FY2024 Request: \$375,000**
Reference No: 64680

AP/AL: Appropriation **Project Type:** Information Technology / Systems / Communication

Category: General Government **House District:** Statewide (HD 1-40)
Location: Statewide **Contact:** Bill Smith
Impact House District: Statewide (HD 1-40) **Contact Phone:** (907)269-6596
Estimated Project Dates: 07/01/2023 - 06/30/2028

Brief Summary and Statement of Need:

Static code vulnerability and analysis scan for all public facing applications.

Funding:	<u>FY2024</u>	<u>FY2025</u>	<u>FY2026</u>	<u>FY2027</u>	<u>FY2028</u>	<u>FY2029</u>	<u>Total</u>
1004 Gen Fund	\$375,000						\$375,000
Total:	\$375,000	\$0	\$0	\$0	\$0	\$0	\$375,000

<input type="checkbox"/> State Match Required	<input type="checkbox"/> One-Time Project	<input type="checkbox"/> Phased - new	<input type="checkbox"/> Phased - underway	<input type="checkbox"/> Ongoing
0% = Minimum State Match % Required		<input type="checkbox"/> Amendment	<input type="checkbox"/> Mental Health Bill	

Operating & Maintenance Costs:

	<u>Amount</u>	<u>Staff</u>
Project Development:	0	0
Ongoing Operating:	0	0
One-Time Startup:	0	0
Totals:	0	0

Prior Funding History / Additional Information:

Project Description/Justification:

The State Security Office (SSO) has identified a statewide gap with regard to secure application programming practices. Modern application development (programming) requires the incorporation of security practices during development, enabled through automated code testing to identify insecure code and vulnerabilities in software packages. When applications are developed by the State of Alaska (SOA) they should undergo periodic security scanning to ensure security holes or vulnerabilities have not been created (intentionally or unintentionally) by SOA application developers.

The funding will be used to purchase a software tool to enable SOA to:

- Identify the vulnerabilities in State of Alaska applications and help state developer staff fix and prevent coding issues from being created in the first place.
- Provide developer education, consultations, and overall guidance in creating our AppSec program across the State of Alaska Executive branch.

Benefits:

- An integrated developer environment for developers that offers real-time feedback to make code secure.
- Development teams find and fix coding flaws faster

Static Code Vulnerability and Analysis Scan for All Public Facing Apps

FY2024 Request: \$375,000
Reference No: 64680

- Enables us to mitigate risks quickly and meet compliance requirements for security in coding practices
- Training through contextual learning, recommended fixes and easy integrations
- Comprehensive platform solution for static code analysis, software composition analysis, and dynamic “real-time” code analysis

Impact if not funded:

If this initiative is not funded, SOA developers will continue to develop code that potentially creates vulnerabilities to Alaskan’s data. Today, the SSO does not know if SOA developed code is a threat to the environment or not because existing tools do not provide vulnerability assessments against code developed within the SOA. As a result, if this initiative is not funded the SOA remains at risk for attackers to find potentially undetectable vulnerabilities allowing them to access confidential Alaskan data.

Cost Estimate

Description	Project Estimate	OPEX Estimate	Duration
Software Licensing	\$375,000	\$375,000 Annually	12 months