Topic: DOE16-030

Tri-Guard Risk Solutions LTD

ADVANCED TECHNOLOGIES FOR NUCLEAR ENERGY

Software-intensive weapon systems are becoming increasingly vulnerable to attacks that exploit software weaknesses. While many system-level accreditation and authorization have been enforced by regulatory authorities, they do not expose latent weaknesses in the composed software components and their impact on system level security controls. Tri-Guard Risk Systems has developed a software weakness management tool that evaluates and prioritizes weaknesses discovered in software code before they become vulnerabilities. This new technology will be integrated into DoD regulatory assessment and accreditation processes as well as procurement processes in the software supply chain. The approach and resulting tool sets will provide the DoD an essential cyber-security tool to identify, assess and prioritize risk, and monitor the progress of corrective efforts to address weaknesses and malicious behaviors detected in software.

Technology Category Alignment:

Cyber
Command, Control, Communications, Computers, & Intelligence (C4I)
Weapons Technologies

Contact:
Keesha M Crosby
kcrosby@tgrisksolutions.com
(703) 435-9545
http://tgrisksolutions.com/
SYSCOM: NAVAIR
Contract: N68335-19-C-0548

Corporate Brochure: https://navystp.com/vtm/open_file?type=brochure&id=N68335-19-C-0548

Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVAIR 2020-893

Topic # DOE16-030
Software Assurance Compliance verification Risk Evaluation - DEFENSE (SACRE-D)
Tri-Guard Risk Solutions LTD

WHO

SYSCOM: NAVAIR

Sponsoring Program: NAVAIR 4.1, PMA 209, PMA 281

Transition Target: NAVAIR, Navy, DoD and other government agencies who develop, procure, and utilize software applications with compliance, risk, and cyber-security requirements.

TPOC:

Other transition opportunities: DoD Prime Contractors and Commercial organizations who develop, utilize software applications and are at the forefront of the development of innovations in software cyber-security.
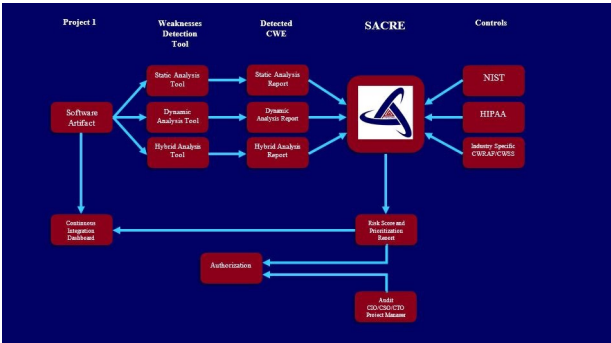
SACRE Workflow

WHAT

Operational Need and Improvement: Ensuring software integrity is key to protecting infrastructure and weapon systems from cybersecurity threats by reducing overall risk due to software weaknesses and vulnerabilities . Minimizing bugs, flaws, weaknesses, defects are key to developing secure and compliance software with minimal residual risk is essential to delivering warfighter security hardened capabilities as well as detecting vulnerabilities in weapon systems before deployment. This software weakness management tool will provide enhanced risk prioritization and mitigation of software weaknesses before they become vulnerabilities. In addition, this product will rapidly improve the assessment of software security risks and support evaluation of weaknesses to aid those without coding backgrounds insight into software as well as ensure the tenement of security is represented across the Software Security Development Life Cycle. The insight of weakness identification and the lowering of false positive will assist in minimizing zero day threats.

Specifications Required: Static output or open Source output

Technology Developed: Software Security Governance, Risk and Compliance product for developers, software managers, security engineers, ISSE, ISSO, auditors, certifiers, and Designated Approving Authorites

Warfighter Value: SACRE is Governance Risk and Compliance product that address software weakness and risk mitigation. SACRE improves and increases the accuracy in detection of software weaknesses bring software compliance and software security risk assessment commercial and open source static analysis, dynamic analysis, dynamic tracing, binary analysis, and contextual analysis. SACRE software security provides risk prioritization and mitigation of weaknesses/vulnerabilities and supports evaluation of weaknesses across each phase of the Software Development Life Cycle.

WHEN

Contract Number: N68335-19-C-0548   **Ending on:** March 19, 2021

Milestone	Risk Level	Measure of Success	Ending TRL	Date
DEMO of NAVY standards	Low	Successful mapping of static output to Navy standard	5	July 2020
Integration of Binary Software Testing Tool	High	Demo binary capability	6	December 2020
Integration into NAVAIR Cybersecurity Lab	Med	Testing of complied Software	7	TBD
Approved Products List (APL) Certification	Med	APL Certification	8	TBD
Integration of DISA STIGS and Commercial s/w Standards	Med	Successful mapping of Standards	9	TBD

HOW

Projected Business Model: ENTERPRISE, On Demand Software as a Service (SaaS); Partnering, Patent Licensing; and Software Licensing/Subscription

Company Objectives: Successful integration into the NAVAIR Cyber-security Lab. Transition technology to commercial applications and become an Industry Leader in software cyber-security testing and analysis.

Potential Commercial Applications: SACRE has direct application to any commercial software development activity requiring testing and identification of cyber-security weaknesses and vulnerabilities. SACRE can assist those commercial offerings who have need for vetting software for compliance or certification.

Contact: Keesha M Crosby, Founder
kcrosby@tgrisksolutions.com   7034359545