Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

MCSC-PRR-4066

Topic # N172-105

Data Integrity and Confidentiality Resilient Operating System Environment for Multi-Level Security

Redwall Technologies LLC

WHO

SYSCOM: MARCOR

Sponsoring Program: PM Intelligence Systems

Transition Target: PM Intelligence Systems

TPOC:
sbir.admin@usmc.mil

Other transition opportunities: - Department of Defense:
-- tactical communications,
-- logistics & maintenance operations,
-- flightline & electronic flight bags,
-- telehealth
- Humanitarian Aid and Disaster Relief
- Law Enforcement

https://www.marines.mil/Photos/igphoto/2002278812/

Notes: Redwall Mobile has been fielded for over 5 years without being compromised or requiring a security patch greatly reducing information technology support workload and costs. This is especially valuable in austere environments.
1. Available on the Motorola Solutions NIAP-approved LEX L11 mission critical handheld.
2. Sold as part of the Tribalco Signal Fusion Platform - multi-level security solution, all CSfC components end-to-end, includes fully integrated radio, LTE, backhaul, and network (classified & unclassified).
3. Coming soon on multiple Zebra tablets and handheld computers.
4. Recently demonstrated at 2021 Naval Integration in Contested Environments (NICE) Advanced Naval Technology Exercise (ANTX).

WHAT

Operational Need and Improvement: Commercial smartphones and tablet computers bring computing and connectivity to the battlefield, flightline, cockpit, point of maintenance, depot, telehealth and other austere environments. However, these devices have inherent OS and application vulnerabilities that expose the DoD to significant risks, and impose unpredictable OS update & patch costs. Redwall's NIAP approved security solution addresses these deficiencies, while enabling a single device to securely operate on classified and unclassified networks. The ability to exchange, store, and utilize controlled and uncontrolled information on a single device reduces logistic costs and network security risks while increasing performance of both labor and systems. Redwall devices can be easily provisioned and reprovisioned to support any mission in any user role context.

Specifications Required: A Mobile device operating system that: provides protection against zero-day vulnerabilities, provides resilience for critical system resources, has low processing overhead and memory usage for resilience, the ability to switch between two different classification levels without requiring removal of the hard disk, and is National Information Assurance Partnership (NIAP) certifiable.

Technology Developed: Behavioral Analysis focuses on how a system should behave when not under attack or influence by an adversary and considers anything else a danger. This technique is effective against zero-day exploits. Even when the cause is completely unknown, the Redwall Mobile solution will still stop the threat. Critical system resources are monitored for corruption and immediately (< 2 seconds) restored to known state providing resilience and fight-through capabilities. Temporal and cryptographic isolation enable multilevel security on a single device.

Warfighter Value: - Multi-role, multi-mission, multi-level security on a single device (eliminates burner phones and BYOD)
- Inherent security that pre-empts zero day exploits to the Android OS and by applications
- Cyber-resilience with "fight-through-attack" capability to enable mission completion and countermeasures
- Rapid, policy-based device provisioning (via cloud or local network) to create custom, mission-specific device and application profiles
- Deployed on military grade, rugged hardware from Motorola Solutions and Zebra Technologies assures long term hardware support

WHEN

Contract Number: M67854-19-C-6517 **Ending on:** October 20, 2021

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Demonstrated Feasibility for Resiliency	Low	Proof-of-concept Implementation that could detect and restore a missing or corrupt critical system resource in under 2 seconds.	3	3rd QTR FY18
Completed Vulnerability Assessment (including zero-day attacks)	Med	During our testing, we found several Android exploits that do work against standard Android devices but were rendered either ineffective or irrelevant on a Redwall-protected device.	4	1st QTR FY20
Completed Full Resiliency Implementation	Med	Identified and implemented for critical system resources including critical address ranges of the in-memory operating system (kernel, interrupt handling code & tables, system call handling code & tables, scheduler, etc.), and critical files and daemons.	6	2nd QTR FY20
Prototype with All Topic Requirements Fullfilled	Med	Live demo of full device and server capabilities for potential DoD customers. Delivery of prototype devices.	7	4th QTR FY21

HOW

Projected Business Model: Market Redwall Mobile, Secure Persona, and Digital Bodyguard to end users, and sell through channel partners, including device manufacturers, wireless carriers, resellers, and systems integrators

Company Objectives: 1. Provide value-added cybersecurity software, solutions, and services that leverage Redwall's unique, patented Redwall Mobile® Security, Secure Persona®, and Digital Bodyguard® products
2. Expand rapidly into the smartphone and tablet computer cybersecurity markets by specializing in a) multi-level security, b) application certification, monitoring & control, and c) privacy monitoring and protection.
3. Expand into 5G and Internet of Things markets by providing device control, security and privilege for as-built, as maintained, and as-operated use cases.

Potential Commercial Applications: 1. Government – Redwall enabled mobile devices are capable of meeting the most stringent security requirements, while providing unrivaled device control, and role-based separation & privacy. Use cases include multi-level security, covert missions, diplomatic corps, military theatre of operations, telehealth, flightline maintenance, digital flight bags, and logistics operations.
2. First Responders – Federal, State, & local Law enforcement and emergency response organizations, including police, fire & rescue, and humanitarian and disaster relief organizations.
3. Commercial Enterprises – Security firms, Aircraft Maintenance and Airlines, Healthcare organizations and warehousing & logistics applications
4. Personal Use – Private citizens desiring greater autonomy, security, and privacy.

Contact: John Rosenstengel, President and CEO
john.rosenstengel@redwall.us 937-477-0424