

# NAVY Transition Assistance Program

SPAWAR Public Release 492 Distribution: Statement A-"Approved for public release; distribution is unlimited."

## N06-089 - RedPhone Security

### Cross-Domain SOA Processor and Router

#### NEED & CUSTOMER REQUIREMENT

**Need:** C2ISR data feeds and web services have proliferated on both classified and unclassified networks. Now there is a need for advancements in the processing of these feeds to enable them to securely cross autonomous security domains. Additionally, feeds must be accessible to low bandwidth, portable/handheld devices used by the warfighter in many diverse scenarios and operations.

**Value to the Warfighter:** RedPhone Security's DSR network card processors provide a gateway to the GIG that satisfy all NSA-identified target GIG attributes, packaged in an easy-to-install and easy-to-own form factor providing a secure, remotely administered network infrastructure from command center to the "edge".

**Operational Gap:** High-cost, medium-assurance network guard solutions are scattered throughout DoD and the Intelligence Community. These guards are expensive to operate and maintain, lack remote configuration and accreditation capabilities, and are deployed as multi-node, two-level systems instead of single-device, multi-level systems.

**Customer Specifications:** Per NSA GIG Architectural Vision document Version 1.0 (June 2007), DSR network cards must provide a multi-level, high assurance networking infrastructure that is easily extensible so that any party may plug in, and all parties are secure against cyber attack. Further, it must enable secure remote administration of the infrastructure and any computer systems connected to that infrastructure, within the strict limits of proper authorization.

**Technology Description:** RedPhone Security's Distributed Secure Router (DSR) technology may be deployed in a variety of form factors. All form factors provide high assurance publish and subscribe, infinite scalability, with configurable pipelines and integrated cross-domain capability with Type I cryptographic capability.

#### TECHNOLOGY DEVELOPMENT MILESTONES (SBIR/STTR)

Milestone	TRL	Risk	Measure of Success	TRL Date
Phase I	1	High	Formal verification (PVS) of Security Policy Model	8/26/2006
Phase I Option	3	High	Integration of prototype with OpenSSL	8/24/2007
Phase II, Prototype 1	3	High	Integration with unmodified browser using SSL; third party formal verification of Top Level Specification	1/14/2009
Phase II, Prototype 2	4	High	Composed prototype integration with web server, database, SSL, browser, and another prototype using Need-Cert protocol	9/4/2009

**Open contract:** N00039-08-C-0076 ending 06/01/2010

#### SPONSORSHIP of original SBIR/STTR Topic

**SYSCOM:** SPAWAR

**Transition Target:** PEO JTRS

**Original Sponsoring Program:** PEO C4I

**TPOC Phone Number:** (619) 524-7587



#### TECHNOLOGY TRANSITION OPPORTUNITIES (PHASE III)

**Other Potential Applications:**

Deployed in a variety of network card form factors, Redphone Security's DSRs may be plugged into Windows, Linux and embedded devices. They may be configured using a browser to meet a wide variety of high assurance, cross-domain, publish-subscribe and remotely administered network requirements for environments such as, Maritime Domain Awareness, CANES, or JTRS.

**Business Model:**

RedPhone has designed a versatile commercial, off-the-shelf product. Transition to the fleet will be through direct sale to the government and via leading system builders.

**Objective:**

With wide applicability within DoD and the private sector, RedPhone Security seeks relationships with Joint Tactical Radio System program managers and other government programs that require true multi-level secure networking.

**Company:** RedPhone Security

**Contact:** Mr. Mark Brown

**Email:** mark@redphonesecurity.com

**Phone:** (651) 204-3372