FOR IMMEDIATE RELEASE

U.S. Navy Increases Global Grid of Enterprise Cyber Maps

Additional Orders for Advanced Cyber Security Products

San Francisco, CA – September 11, 2012 - Promia, Inc., a developer of Enterprise Cyber Security and Asset Monitoring products, announced today the U.S. Navy has purchased advanced versions of Raven network appliances that fully satisfy the Department of Defense (DoD) requirement for Enterprise Network Mapping and Leak Detection Systems (ENMLDS).

Earlier this year Navy conducted an Analysis of Alternatives (AoA) review to determine which product would be used to satisfy the Navy portion of a US STRATCOM Enterprise Mapping and Leak Detection requirement for all DoD networks. Promia Raven was chosen above all other contestants. Based on this decision, US Navy purchased this capability from Promia, which is part of Promia's Intelligent Agent Security Manager (IASM) V2.2 and plans to begin the upgrade with twenty-three existing Promia Raven systems in global Navy Network Operation sites in 2013. To continue the planned Navy-wide ENMLDS deployment, they also ordered thirteen new Raven 2100 Rev B systems and nine more analytic ENMLDS units for new installation in the OCONUS Navy Enterprise Network (ONE-NET), supporting Navy bases in Singapore, Guam, Diego Garcia and eight other sites around the world.

The asset and network data capture scans the networks using multiple protocols, and identifies both IPv4 and IPv6 networks. It also identifies the network perimeter to any facility, defined by DoD to mean the layer of routers and managed switches inaccessible to that facility's managers. The Raven appliance also identifies the routing tables from properly configured SNMP type 1, 2 and 3 devices, as well as devices acting as Wireless Access Points (WAP). The system identifies and inventories discovered assets by IP address and resolves to the Media Access Control (MAC) level, while identifying probable Operating System (OS) and version of the discovered devices. The system also identifies the state of a specified set of ports on the discovered devices and collects both HTTP and SNMP banners from each device responding to the specified port and protocol. The ENMLDS capability in Promia Raven generates a logical mapped diagram of the router interconnections (network routes) of the facility and aggregates all discovered IPs into their assigned subnets, segments, and/or logical groupings. The system discovers live network segments including unknown/unauthorized segments, and identifies and reports unknown IP addresses without any manual intervention. In addition the system identifies devices that covertly forward network traffic, and provides a low-bandwidth network mapping engine with an adjustable packet rate/scan speed.

Included with the Raven are integrated diagnostic applications, custom fingerprints feature for asset identification and real-time leak detection alerting for access to unauthorized networks. The system generates a Web-based report of the network anomalies and allows for interactive analysis of the data, and also integrates with standard applications for accessing Web-based reports. It supports ad-hoc queries against the collected data set, and exports data into eXtensible Markup Language (XML), Java Script Object Notation (JSON) and Comma Separated Values (CSV) for text output and Portable Document Format (PDF) and Portable Network Graphics (PNG) and Tagged Image Format (TIF) for images.

Additional electronic leak detection and defense features are included such as a new "exfiltration" protection for devices that begin to act abnormally when compared to their approved behavior profiles. Other leak detection features immediately identifies and optionally blocks all SIPR to NIPR or all SIPR to non-SIPR traffic, access to identified Proxy servers, access to identified BOTNET servers or other malware infected machines. The Raven hierarchical grid of interconnected appliances provides a mechanism for immediate distribution of threat signatures, block lists, or other policy configuration information worldwide to all systems on shore and ship environments. Conversely, this hierarchical grid supports global DoD asset state collection, in both snapshot mode where all current asset states are collected, or in delta mode where only changed asset states are collected, worldwide from all sites, gathered into regional and global repositories for analysis and enterprise mapping. Promia supports Ozone Widget Framework access to all this data.

About Promia, Incorporated - *Promia, Incorporated is a leading developer and supplier of security tools, based on open standard components with advanced analytic capabilities, to the Fortune 1000 companies and government markets. Its products are used in environments requiring high security, reliability, performance, and scalability. Based in San Francisco, Promia has offices in Princeton New Jersey, and Woodland, California.*

Contact: PROMIA - San Francisco Attn: Pamela Boles Ph 415.536.1600 info@promia.com