FOR IMMEDIATE RELEASE

U.S. Navy Awards PROMIA $7 Million for Internet Security Products

Sophisticated New Techniques for Rapid Detection of Network Security Events

San Francisco, CA -- September 24, 2001 -- PROMIA Incorporated, a developer of next-generation Internet Security products, announced today that the U.S. Navy Space and Naval Warfare Systems Command (SPAWAR) has awarded PROMIA $7,000,000 to test and deliver twenty Advanced Internet Security systems. This procurement represents Phase III of a U.S. Navy Small Business Innovation Research (SBIR) Program and compliments a multi-year research and development effort by PROMIA and the U.S. Navy to design and build the systems.

The Internet security system to be delivered to the U.S. Navy is code-named the "Intelligent Agent Security Module" (IASM) and is to be deployed as a primary means of providing information analysis and protection on ships and shore-based facilities. The IASM product was designed to address known problems found in the current generation of intrusion detection devices such as the generation of high volumes of false alarms and the inability to detect new types of attacks.

IASM is a supercomputer-based system that uses a CORBATM secure component architecture designed to manage the accurate and consistent detection and validation of internally and externally generated network incidents. The system detects known attacks using various techniques to correlate single and multiple events, while novel attacks are detected using advanced analytic techniques to identify aberrant behaviors. IASM also includes a visualization component designed to encourage rapid understanding of complex events with selectable levels of response suitable to the needs of the U.S. Navy and other branches of the U.S. Department of Defense. High performance Beowulf cluster machines, supercomputing platforms developed at NASA, are included to support the analytic modules of IASM. "This", according to PROMIA's Principal Analyst, Dr. Stephen Neville, "makes it feasible to expose aberrant behaviors even within the sea of normal traffic. Traditionally hackers have had the luxury of hiding their actions within the large volumes of network messages. The combination of advanced analytic techniques with low cost, scalable supercomputers seriously hinders the attackers ability to hide." Commercial versions of the PROMIA IASM product, including a PROMIA Internet Appliance, are on schedule as required by the Navy SBIR Agreement.

Lt. Frank Ottaviano, U.S. Navy Space and Naval Warfare Systems Command (SPAWAR) Information Assurance Project Engineer is particularly interested in the possibilities offered to those with responsibility for monitoring the systems. Lt. Ottaviano expects that this will result in groundbreaking work with respect to the human interface requirements of battlefield tools. He vowed that he "will be working closely with the community of interest in this area to ensure a conclusive, easily displayed and understood, highly interactive system." Lt. Ottaviano is equally pleased with the component architecture's capability to incorporate new detection technologies as they become available.

PROMIA's President and CEO, Mr. John Mullen, said "We are very proud to be able to contribute to our country's Cyber-defense capabilities, particularly at this time in history. PROMIA's work is significant because it is based on a reusable framework for automatically assessing large amounts of sensor data, simultaneously, across multiple networks, providing pattern matching and novel attack detection." "This," he said, "surpasses traditional intrusion detection approaches which work in isolation and are limited in their ability to obtain details from this rich information store. We also believe that this component framework can be applied to other kinds of real-time data mining problems." Mr. Mullen noted the importance of PROMIA using emerging technologies such as Fuzzy Logic and Neural Networks in this product to create and apply new knowledge about Cyber attacks. Fuzzy Logic computing refers to a branch of artificial intelligence focused in accurate reasoning in a domain with high levels of uncertainty or incomplete data such as is found in the Cyber Warfare arena.

About Promia, Incorporated

Promia, Incorporated is a leading developer and supplier of distributed object and component security tools, based on open standard components with advanced analytic capabilities, to the US Government and Fortune 1000 markets. Its products are used in environments requiring high security, high reliability, high performance, and scalability.

Promia's core competencies include expertise in a wide range of computer programming languages, databases, security architectures and technologies, security assurance and evaluation, communications protocols, hardware devices, artificial intelligence techniques, data and application integration and distributed data networks. Since the early 1990's, Promia has been in the forefront of developing software infrastructure solutions based on object-oriented technology and open standards, most particularly CORBA, for organizations worldwide. Based in San Francisco, Promia also has offices in Princeton, NJ, Davis, California, and Linthicum, Maryland.

Intelligent Agent Security Manager, IASM, Promia Cyber Warfare Laboratory, and CWL are trademarks of Promia Incorporated. CORBA is a registered trademark of the Object Management Group (OMG).

PROMIA, San Francisco
160 Spear Street, Suite 320
San Francisco, CA 94105

ph 415.536.1600
fx 415.536.1616

email info@promia.com
investment@promia.com

###