FOR IMMEDIATE RELEASE

Promia Intelligent Agent Security Manager (IASM) Evaluated and Validated within Common Criteria

San Francisco, CA – May 24, 2006 - Promia, Inc., developer of the Intelligent Agent Security Manager (IASM) family of Security Incident Management products, announced today that its IASM 6100 appliance has completed evaluation and validation as a product conforming to EAL 3+ within the Common Criteria Evaluation and Validation Scheme (CCEVS) in the National Information Assurance Partnership (NIAP).

The IASM 6100 is a hardened Security Incident Management appliance that meets or exceeds compliance to both the Common Criteria and DISA Security Technical Implementation Guides. Promia IASM collects and consolidate**s** security-relevant events from the logs of operating systems, applications, and network security devices and accurately analyzes collected events to detect, validate, manage, and respond to security incidents originating both inside and outside of the network systems it protects. IASM detects known attacks, through Promia and other company's sensors, as well as novel or anomalous attacks, through advanced analysis techniques that identify aberrant behaviors. IASM includes multiple visualization components designed to present ongoing attacks in a rapidly comprehendible format suitable to the needs of the U.S. Navy and other branches of the U.S. Department of Defense. High performance rack mounted cluster machines are provided in the IASM systems and have been deployed worldwide in Navy Network Operating Centers (NOC's).

The evaluation was conducted in accordance to the Common Criteria Evaluation and Validation Scheme (CCEVS). The evaluation demonstrated that IASM model 6100 meets the security requirements contained in the Security Target, which is the criteria against which the Promia Intelligent Agent Security Manager, Version 1.2 (IASM) was judged as described in the Common Criteria for Information Technology Security Evaluation, Version 2.2. Computer Sciences Corporation (accredited Common Criteria Testing Laboratory) determined that the evaluation assurance level (EAL) for the product is EAL 3 Augmented with ALC_FLR.2 and ALC_LCD.1. The evaluation methodology used by the evaluation team that conducted the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2. The product, when configured and installed according to supplied guidance, satisfies all of the security functional requirements stated in the Security Target. A validator, on behalf of the CCEVS Validation Body, monitored the evaluation carried out by Computer Sciences Corporation. The evaluation was completed in May 2006. Results of the evaluation and **NIAP** validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

Promia's Senior Software Assurance Analyst, David Chizmadia, stated "Promia is excited to have the first Security Incident Management product that has completed the evaluation and validation to meet the requirements of Common Criteria at or beyond EAL 3. This evaluation shows our company commitment to the goal of higher software assurance now being advocated and encouraged by the DoD, DHS, NIST, and OMG. We look forward to working with our customers to leverage this CC EAL 3+ evaluation in their system security certification and accreditation efforts." He went on to explain "Existing policies for system security certification and accreditation, such as NTISSP 11 and DOD Directive 8500.1, acknowledge the importance and value of CCEVS evaluations by requiring DOD organizations to favor the selection of products with a CCEVS certificate over products without one."

About Promia, Incorporated

Promia is a provider, developer, and researcher of sophisticated network and data security products to the U.S. Government, focused on data visualization and network protection of the Department of Defense's communication-centric Global Information Grid. In collaboration with government research organizations, Promia developed and deployed a series of highly sophisticated hardened appliances, utilizing multiple advanced approaches of knowledge engineering, artificial intelligence, and statistical analysis to collect, fuse, and analyze data in real-time to detect threatened data corruption, and aberrant and anomalous behavior over complex networks. Promia is based in San Francisco, with offices in Princeton NJ, Davis, CA and Linthicum, MD.

About the Common Criteria Evaluation and Validation Scheme

The Common Criteria Evaluation and Validation Scheme (CCEVS) is the U.S. program establishing an organizational and technical framework within which the trustworthiness of Information Technology (IT) Products and protection profiles can be evaluated. The CCEVS was created as part of the National Information Assurance Partnership (NIAP) between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Under the CCEVS, evaluators in independent Common Criteria Testing Laboratories verify that IA products meet the Security function and assurance requirements stated in the Security Target (ST) for the product. The evaluation processes and results are checked by CCEVS Validators to ensure compliance with both the Common Criteria and the Common Evaluation Methodology before the product is awarded its evaluation certificate. Through a multi-country agreement, the results of CCEVS evaluations are recognized and accepted in over 20 other countries.

Media Contact:
Promia San Francisco
160 Spear Street, Suite 320
San Francisco, CA 94105
Ph 415.536.1600
Fx 415.536.1616
info@promia.com

# # #