Contact: Suzanne Magee
suzanne.magee@techguard.com
suzanne.magee@bandurasystems.com
636.489.2230

TechGuard® PoliWall® Appliances Achieve NIST's FIPS 140-2 Validation

PoliWall Certificate: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1879

Baltimore – February 15, 2013 – TechGuard Security®, a provider of trusted, scalable, and innovative technologies and services that protect critical infrastructures from cyber-attack, today announced that the PoliWall® product line achieved Federal Information Processing Standards Publications (FIPS) 140-2 Validation: Security Requirements for Cryptographic Modules. FIPS 140-2 validation is a requirement for any cryptographic product which will be used in a U.S. government agency network. The PoliWall appliance line includes the following models:

PoliWall-CCF M10 [1], M50 [2], G01 [3] and G10 [4] Series Security Appliance and software model.

"Our FIPS 140-2 certification at Level 2 with Level 3 for design assurance validates our secure coding, development and tamper resistance processes; and TechGuard's extra-mile dedication to meeting Federal agency security concerns," said Dave Maestas, CTO, TechGuard and Bandura. "This is an important component for provision of secure solutions to government buyers."

In order to expedite the FIPS 140-2 validation process, TechGuard partnered with Booz Allen Hamilton and CygnaCom Solutions. "The expert assistance of both Booz Allen and Cygnacom streamlined the process for TechGuard: Clear explanation of the FIPS requirement; documentation review; and validation testing of the PoliWall appliances and software" said Suzanne Magee, CEO and co-founder, TechGuard Security and Bandura. " FIPS 140-2 validation of the TechGuard PoliWall appliances and software demonstrates our ongoing commitment to our defense/defense industrial base customers and the security of their data."

The FIPS standard, which is utilized by the U.S. and Canadian governments, is also currently being reviewed by ISO to become an international standard. FIPS 140-2 is gaining worldwide recognition as an important benchmark for third party validations of encryption products of all kinds.

About FIPS 140-2 Cryptographic Module Validation Program

The FIPS 140-2 standard is a joint effort by the National Institute of Standards and Technology (NIST) in the United States, and the Communications Security Establishment Canada (CSEC), under the Canadian government. The Cryptographic Module Validation Program (CMVP), headed by NIST, provides module and algorithm testing for FIPS 140-2, which applies to Federal agencies using validated cryptographic modules to protect sensitive government data in

computer and telecommunication systems. FIPS 140-2 provides third-party assurance of cryptographic modules that have been validated against a set of functional requirements for a product that may be purchased by a government agency.

Level 2 (wikipedia)
Security Level 2 improves upon the physical security mechanisms of a Security Level 1 cryptographic module by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.

Level 3 (wikipedia)
In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

About PoliWall:

- PoliWall can be deployed as an appliance, in the Cloud, or as a managed solution.
- Proven PoliWall Security capabilities include: one click country-blocking, IP Reputation list processing with millions of entries—with virtually no latency--exceptions of white list/black list, QOS, ingress/egress filtering, bandwidth prioritization/DDOS protection
- PoliWall rapidly reduces the attack space with High-Speed Internet Protocol Packet Inspection Engines (HIPPIE®)
- Scalable pricing model to fit business/budget needs from 100 Mb to 10 GB throughput.
- HIPPIE and PCEL algorithms are optimized for memory and CPU utilization
- Provides rapid throughput, low CPU
- Virtual appliance easily deployed on hypervisors
- All security and management features fully support IPv6
- SNMP data and MRTG graphs provide visualization of network statistics and trend analysis for traffic to and from all countries.

Government and Defense Industrial Base customers-- Poliwall is on the GSA schedule, is Common Criteria EAL 4+ certified, FIPS 140-2 Level 2 certified, and available in100 Mb to 10 GB throughput devices.

About TechGuard®

TechGuard Security, founded in February 2000 in direct response to Presidential Decision Directive 63, provides trusted and innovative Critical Infrastructure Protection to the Department of Defense, Homeland Security, Federal agencies, and the US Critical Infrastructure. TechGuardians® research,

develop, and rapidly prototype, cutting-edge security technologies, including the patent and patent-pending PoliWall® with HIPPIE® and PCELs® technologies; and provide expert consulting services. PoliWall is marketed under Bandura, LLC a wholly-owned subsidiary of TechGuard Security . Please contact Dave.maestas@bandurasystems.com or Chris.castaldo@bandurasystems.com for more information about the PoliWall appliance or value-added reseller opportunities.

TechGuard® is a certified women-owned business enterprise. For additional information please visit http://www.techguard.com/ and follow us on twitter @poliwall.

About CygnaCom Solutions

CygnaCom Solutions operates two NVLAP accredited laboratories (NVLAP LAB CODE 0200002-0) dedicated to providing fair, objective, and cost-effective assessments of all products submitted for validation.

The Cryptographic Equipment Assessment Laboratory (CEAL) is CygnaCom Solutions' laboratory accredited to test hardware and software products for compliance with the U.S. Government's FIPS 140-1/2 and compliance with FIPS algorithms.

About Booz Allen Hamilton

Booz Allen is the premier Certification & Accreditation contractor and penetration testing/vulnerability assessment contractor to the U.S. government. We support the National Institute of Standards and Technology (NIST) and other government agencies' activities throughout the security community. We serve as primary authors to the Certification & Accreditation policy documents, and tap intellectual capital across the firm in the numerous client engagements across both the commercial and government communities as necessary. We operate several laboratories that conduct Penetration Testing and Product Validation services (e.g., Common Criteria FIPS 140-2, UCAPL, etc) . If want to learn how to get your products acquired by the U.S. Government Booz Allen Hamilton is a single stop shop for your product testing needs. Please contact the Cyber Assurance Testing (CAT) Laboratory director at catl@bah.com for more information.

###