**ASSURANCE CONTINUITY MAINTENANCE REPORT FOR**

**Cisco Firewall Services Module (FWSM)**

**Maintenance Report Number: CCEVS-VR-07-0027a**

**Date of Activity**:  17July 2007

**References:**  Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

"Impact Analysis Report for Common Criteria Assurance Maintenance: Update of Cisco Firewall Services Module (FMSM) 3.1 (3.17) to 3.1(4)", v0.6, 02 July 2007.

**Documentation Updated**:

Cisco Firewall Services Module developer evidence documents.

**Assurance Continuity Maintenance Report:**

On 21 June 2007, Cisco, together with Arca Common Criteria Testing Laboratory, submitted an Impact Analysis Report (IAR) to CCEVS for approval. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

**Changes to TOE:**

This maintenance activity covers a collection of bug fixes to make the FWSM function as specified. No existing functionality was removed and no new functionality was added.

The intent of this maintenance release was to correct three Denial of Service (DOS) vulnerabilities in the product when it was originally certificatied. These vulnerabilities were within the TOE but considered outside the scope of the evaluation because the Security Target does not include the threat of DOS.

**Analysis and Testing:**

All of the bug fixes were found to have no (or minimal) security relevance.

These changes were made to the FWSM after it completed the CCTL evaluation and just before it began the NSA vulnerability analysis and testing phase of its evaluation. As such, this maintenance report covers the EAL4 version of the TOE.

**Conclusion:**

**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

CCEVS reviewed the description of the changes and the analysis of their impact upon security, and found it to be satisfactory. Therefore, CCEVS agrees that the EAL4 assurance is maintained for version 3.1(4) of the product.