ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

McAfee IntruShield Intrusion Prevention System Product Family (IntruShield I-1200/I-1400 Appliances, Rev. 3.1 or earlier; I-2600/I-3000/I-4010 Appliances, Rev. 8.0 or earlier; I-2700 Appliance, Rev 2.0 or earlier; I-4000 Appliance, Rev. 10.0 or earlier; M-6050/M-8000 Appliances, Rev. 1.6; IntruShield Security Management System Version 4.1.7.5; The Sensor Builds: I-Series Version 4.1.5.27 and M-Series Version 4.1.7.8)

Maintenance Update of McAfee IntruShield Intrusion Prevention System Product Family

Maintenance Report Number: CCEVS-VR-VID10169-2009b

Date of Activity: 3 November 2009

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 McAfee IntruShield, Version 1.43

Documentation Updated: (List all documentation updated)

- Security Target for IntruShield Product Family, Version 1.5

Assurance Continuity Maintenance Report:

The vendor for the IntruShield Intrusion Prevention System, McAfee Incorporated, submitted an Impact Analysis Report (IAR) to CCEVS for approval on October 29, 2009. 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:

The changes to the TOE consisted of minor hardware changes which were implemented to improve signal integrity within the TOE as well as minor changes to manufacturing acceptance tests to maintain manufacturability. Each of these changes were applied to make the TOE or supporting hardware/software function as originally intended while improving reliability. No additional security functionality was added, and no existing security functionality was removed. All seven sensor models described in the Security Target had these hardware changes provided, resulting in an updated revision number for each sensor model.

In addition, the ST has been revised to incorporate the current revision of the I-2700 appliance, which was mistakenly not included in the prior Assurance Continuity update for the TOE. The changes to this appliance model are the same as the other sensor models and do not pose a risk to security functionality.

Each of the updates fall into the categorization of "Minor Changes with Little or No Security Relevance" as they do not alter the TOE components that are responsible for implementing the TOE security functionality.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

The IAR provided by McAfee indicates that the assurance evidence has been updated to reflect the changes, and appropriate testing of the changed TOE has occurred to ensure that the TOE continues to meet the functional requirements. Assurance evidence was updated as necessary, including a new search for potential vulnerabilities.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found it to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.